Expert study on: 'GDPR application in the context of car connectivity'

Final Report

November 2021

This report "**GDPR application in the context of car connectivity**" (the "**Report"**) compiles the findings of an expert study commissioned by the Fédération Internationale de l'Automobile ("**FIA**") and conducted by Ernst & Young Abogados, S.L.P. from July 2021 to November 2021 (the "**Study**").

What is the objective of the Study?

The objective of this Study is (i) to provide an extensive analysis of the EU data protection and privacy legal framework applicable to the processing of data in the context of car connectivity; (ii) to assess whether this framework is accomplishing its purposes from a consumer point of view; (iii) to identify challenges and opportunities; and (iv) to provide policy recommendations, where necessary.

Why is data relevant to the automotive sector?

Connected vehicles collect information from the vehicle and its surroundings and communicate with the outside world through a wireless connection to the internet. Connected vehicles rely heavily on data. Through different input sources they can produce significant amounts of data of different nature.

The number of connected vehicles is expected to increase exponentially, positioning the automotive sector as one of the largest data generators. This is fostering the development of innovative data-enabled solutions and business models which are already disrupting the traditional interaction between car users and service providers. However, despite the undeniable benefits and opportunities brought about by connected vehicles, they raise significant privacy risks and concerns.

How does the EU data protection and privacy regulatory framework apply in the context of the connected vehicle?

When the data collected from the connected vehicle qualifies as personal data under the GDPR, both the e-Privacy Directive and the GDPR apply. The interaction between these two pieces of legislation is not always easy. Notably, there is an open debate on the question of the legal basis applicable to subsequent processing operations involving the information gathered from the connected vehicle. The forthcoming e-Privacy Regulation, currently under discussion, will bring relevant modifications to the legal framework.

What is the level of consumer awareness regarding the processing of data in this context?

The Study has revealed that there is certain degree of awareness about connectivity features of connected vehicles and the fact that vehicles can collect and share information. Nevertheless, there is a shared perception that drivers have no control over the data shared by connected vehicles and certain degree of concern about this lack of control. In addition, a significant lack of information about vehicle data collection and processing at the points of sale has been identified.

What are the current challenges and opportunities brought by car connectivity and vehicle data?

The Study shows that contractual/informative documents relevant to the processing of personal data in the context of connected vehicles often lack transparency and have deficiencies.

On the other hand, if the right to data portability was designed in a way in which consumers could exercise it fully and without significant constrains, this would lead to significant benefits for industry's stakeholders and market growth.

In addition, the current data protection and privacy legal framework and the conditions of the original equipment manufacturers in practice work as an entry barrier for independent service providers in the automotive sector.

How can the current situation be improved?

The following policy recommendations are suggested:

- Sector-specific regulation establishing a technical architecture which promotes local data processing and users' control over vehicle data.
- Soft law or guidelines promoting enhanced privacy information in this ecosystem.
- Updated guidelines on consent, and even specific guidelines for this sector.
- Sector-specific regulation implementing an effective data portability mechanism.

TABLE OF CONTENTS

Executive Summary

This report "**GDPR application in the context of car connectivity**" (the "**Report"**) compiles the findings of an expert study commissioned by the Fédération Internationale de l'Automobile ("**FIA**") and conducted by Ernst & Young Abogados, S.L.P. from July 2021 to November 2021 (the "**Study**").

The objective of this Study is to provide a comprehensive analysis of the data protection and privacy legal framework applicable to the processing of data in the context of car connectivity. Through primary data and desk research, its purpose is to assess whether this framework is achieving the objectives set by the legislator, especially from the point of view of consumers, to identify challenges and opportunities, and to provide, where necessary, policy recommendations.

On this basis, the Report:

- assesses how the personal data protection and privacy legal framework applies in relation to car connectivity;
- presents the findings of two practical exercises: the distribution and analysis of a survey across different EU regions, as well as several mystery shopping experiences at vehicles' point of sales;
- identifies and analyses areas which might present challenges and opportunities to the stakeholders involved in the automotive markets linked to connected vehicles, including (i) the analysis of different types of contractual/informative documents relevant to the processing of personal data in the context of connected vehicles; (ii) the opportunities and benefits for different actors and society derived from an effective implementation of the data portability right; and (iii) whether the conditions under which original equipment manufacturers ("**OEMs**") collect, process and make their data available to third parties might create disadvantages to independent service providers ("**ISPs**"); and
- presents the conclusions of the Study and provides policy recommendations on how to empower consumers through legislation.

Background

Connected vehicles rely heavily on data. Through different input sources such as GPS trackers, telematic boxes, cameras, microphones, or sensors, connected vehicles can produce significant amounts of data of different nature. This can include: operational data (e.g. speed, location, number of passengers, fuel), data pertaining to maintenance aspects (e.g. oil levels, milage due, technical problems), data about the surroundings (e.g. temperature, weather conditions, road marking), user's selected settings and driver's behaviour (e.g. seat and steering wheel position, speed patterns, distances travelled), infotainment data (e.g. phone's information relating to messages, contacts, call history), car users' personal details (e.g. name, contact and financials details provided to the vehicle's operating system, for instance, through a smartphone connected to the vehicle), etc.[1]

[1] Engers, Tom & de Vries, Dennis, *Jusletter-IT privacy-on-wheels*, 2019, p. 4.

The number of connected vehicles is expected to only increase, positioning the automotive sector as one of the largest data generators.[2] This is fostering the development of innovative data-enabled solutions and business models which are already disrupting the traditional interaction between car users and service providers.[3] Such solutions include, among others, predictive repair and maintenance services, remote delivery of fuel or on-demand vehicle washing to where the vehicle is parked, adjustments on insurance rates based on driving behaviour, or receiving information directly from the vehicle about driving conditions ahead, nearby scenic spots, hospitality services, offers, discounts, coupons of commercial establishments based on location, season or other elements.

Much of the data,[4] if not all, that is generated and processed in connected vehicles constitutes personal data because it relates to natural persons that are identified or identifiable. Some of the data collected by connected vehicles can be of sensitive nature for the individuals concerned and its misuse could have severe implications for someone's personal and professional life. For instance, vehicles can collect detailed records of a person's movements and destinations by means of geolocation and can recur to biometric data to allow access to the vehicle or to the user's private settings. Vehicles could record administrative infringements, such as speeding or failing to stop at a red light, or even criminal offences. The quantity and very diverse nature of the data collected by connected vehicles allow for the combination of data in a way that can reveal detailed information about car users' preferences or driving behaviours. In parallel, processing capabilities of large amounts of raw data and data analysis capabilities are developing at a fast pace with the development of big data techniques and artificial intelligence ("**AI**") solutions. As a result, recipients of the data collected from connected vehicles have tools at their disposal for the processing of data in ways that were not conceivable before and which are evolving fast and uninterruptedly.

Therefore, despite the undeniable benefits and opportunities brought about by connected vehicles, they raise significant privacy risks and concerns.

Application of the privacy regulatory framework in the context of car connectivity

This is why the Report starts by conducting an in-depth analysis of the data protection and privacy regulatory framework applicable to the connected vehicle ecosystem: the General Data Protection Regulation ("**GDPR**")[5] and the Directive on Privacy in the electronic communications ("**e-Privacy Directive**")[6]. It continues by presenting the regulation that is set to substitute the e-

[2] Gaspare Fiengo, Giulia Lovaste, *Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform*, Legal Study, 2021.
[3] *Ibid*., p. 3.
[4] See, among others: European Data Protection Board, *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*, version 2.0, 2021, p.6; European Commission and TRL, *Access to In-Vehicle Data and Resources – Final Report*, 2017, p. 124; or European Commission, C-ITS Platform – *Final Report*, 2016, in the context of messages (cooperative awareness messages and decentralized environmental messages) between vehicles and cooperative intelligent transport systems.
[5] Regulation (EU) 2016/679 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.
[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as revised by directive 2009/136/EC.

Privacy Directive (the e-Privacy Regulation Proposal, or "**ePR Proposal**")[7], analyses its legislative status and the different texts that EU political institutions are negotiating. Finally, it analyses the implications that this new regulation could have for vehicle connectivity and data sharing.

In regard to the applicability of the GDPR, the Study has shown that this regulation is fully applicable to data processed in the context of connected vehicles to the extent that the data involved qualifies as "personal data" under Article 4(1) GDPR. Personal data is not limited to identifiers of the people using the vehicle such as a name, surname, national ID, etc., but also includes any information that can be linked to these persons, notably via the vehicle serial number or the vehicle licence plate number. The technical nature of vehicle data does not preclude its legal qualification as personal data, to the extent that it can be related to an identified or identifiable individual.

Unless otherwise anonymised, data from connected vehicles will most likely qualify as personal data in relation to the organizations directly collecting and using the data, as well as organizations indirectly collecting and using the data to the extent that they have the information necessary to identify the person or can lawfully obtain sufficient additional data to link the information to a person and therewith identify that person.

As for the e-Privacy Directive, Article 5(3) is applicable to the collection of data from connected vehicles to the extent that: (i) the vehicle qualifies as "terminal equipment" under Directive 2008/63/CE;[8] (ii) and the data is collected through a publicly available electronic communication service. Article 5(3) e-Privacy Directive takes precedence over Article 6 GDPR with regards to the activity of "storing or gaining access to information" collected in the context of the connected vehicles.

As a general rule pursuant to the Art. 5(3) e-Privacy Directive, prior informed 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. The storing of information or the gaining of access to information that is already stored in the terminal equipment is exempted from the requirement of informed consent if it satisfies one of the following criteria: (i) the storage of information or the gaining access to information already stored is performed for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the storage of information or the gaining access to information already stored is strictly necessary in order for the provider of an information society service[9] explicitly requested by the subscriber or user to provide the service.

---

[7] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.2.2021, 2017/0003(COD), 6087/21.

[8] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance), OJ L 162, 21.6.2008, pp. 20–26.

[9] An information society service is defined in Article (1)(b) of Directive (EU) 2015/1535 as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

Based on the above, to the extent that connected vehicles are terminal equipment transmitting information through public networks, collecting and using information from the vehicle shall primarily rely on consent, unless an exemption exists. This setup rather limits service providers' ability to process data collected from the connected vehicle.

When the data collected from the connected vehicle qualifies as personal data under the GDPR, both the e-Privacy Directive and the GDPR applies. The interaction between these two pieces of legislation is not always easy. Notably, there is an open debate on the question of the legal basis applicable to subsequent processing operations involving the information gathered from the connected vehicle. According to the European Data Protection Board ("**EDPB**"), as a general rule, where consent is necessary pursuant to Article 5(3) e-Privacy Directive, data controllers cannot rely on one of the lawful basis in Article 6 GDPR other than consent for subsequent processing operations, especially in relation to tracking and profiling processing activities. This opinion is not necessarily followed by the industry, especially in the digital advertising ecosystem.

Nonetheless, the EDPB acknowledges that service providers can rely on the performance of a contract as a legal basis as per Article 6(1)(b) GDPR for subsequent processing operations if certain conditions are met. In addition, the EDPB acknowledges that in some cases, and subject to transparency and additional safeguards, tracking and profiling may also be permissible to prevent fraudulent use of the services offered.

The European Data Protection Supervisor ("**EDPS**") and the *Commission nationale de l'informatique et des libertés* ("**CNIL**") have also released specific guidelines on connected vehicles. The three abovementioned authorities identify similar risks to privacy and data protection stemming from this technology and recommend a cautious approach to data processing at the peril of vehicle users' losing control over their personal information. This Report summarizes these guidelines as they are relevant to understand how the data protection and privacy regulatory framework applies to the context of vehicle connectivity.

As for the ePR Proposal, the draft text, currently under negotiation between the European Parliament and the Council of the European Union ("**EU**"), will bring relevant modifications to the legal framework on privacy of electronic communications and therefore to the connected vehicle ecosystem.

Originally, this regulation was intended to be passed together with the GDPR, but EU Member States have not yet been able to agree on the draft legislation and negotiations of the ePR Proposal are still ongoing. Since the publication of the original version proposed by the European Commission on January 2017 ("**EC ePR Proposal**"),[10] shortly followed by the European Parliament's on 20 October 2017 ("**EP ePR Proposal**"),[11] the Council, after four years of internal negotiation and the publication of more than 30 different versions of the file, passing through 8 different presidencies, finally adopted a common position on February 10, 2021 ("**Council ePR Proposal**").[12] At the date of publication of this Report, the Council and the Parliament are negotiating the ePR Proposal at first reading under the ordinary legislative channel.

[10] Version available here: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52017PC0010.
[11] Version available here: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html?redirect.
[12] Version available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=ENn.

Depending on which version of the ePR Proposal we pay attention to – European Commission, European Parliament or Council of the EU – there are significantly different rules, especially with regard to the protection of end-users' terminal equipment. Therefore, the Report focuses on understanding the differences between the three versions of the ePR Proposal.

The EU legislator, especially the Council of the EU, has sought in this proposal to grant service providers with greater flexibility when it comes to processing of data collected from terminal equipment, such as connected vehicles. Most notably, the ePR Proposal, in all of its versions, creates a more flexible landscape for OEMs and ISPs to use the connected vehicle's processing and storage capabilities or the collection of information from the vehicle without the end-user's consent.

This opens the door for numerous services to be provided bypassing consent, which is beneficial for OEMs (e.g., access to data by official repairers, etc.) and, theoretically, for ISPs (e.g., independent repair and maintenance, road assistance, insurance, etc.). However, the enhanced flexibility in what regards to legal bases other than consent is balanced out by an increased complexity of the regulatory framework. This complexity will also derive in increasing difficulties in providing information that is easy to understand for consumers and complete at the same time.

Interestingly, the Council ePR Proposal allows for the processing of data collected from connected vehicles for further/compatible purposes, in line with the GDPR. This will allow OEMs and ISPs for significant flexibility to ascertain situations in which consent is not necessary. Nevertheless, provisions in the ePR Proposal are more stringent than the GDPR.

There is legal uncertainty around consent in the ePR Proposal, as some aspects remain unresolved. Notably, it remains unclear how consent could sufficiently be provided by end-users, for instance, where the end-user of a connected vehicle changes (i.e. car sharing).

All in all, the ePR Proposal could bring higher regulatory exposure to operators in the connected vehicle ecosystem in those cases where Member states decide to bring together supervisory competencies under the GDPR and the e-Privacy into one, unique national supervisory authority.

Finally, the Council ePR Proposal could bring more certainty to justify that the processing necessary for eCall does not require consent, as it specifically includes an exemption to consent or these purposes.

Consumer awareness (survey and mystery shopping exercises)

As part of this Study, two practical exercises have been conducted: the distribution and analysis of a survey across different EU regions as well as several mystery shopping experiences at vehicles' point of sales. The purpose of these exercises was to collect empirical data to assess consumers' sensitivity, awareness and attitudes towards data processing in the context of car connectivity, as well as transparency of information provided to consumers at the vehicle points of sales.

As regard the **survey**, it has been conducted in 3 European regions, i.e.:

- Southern (with respondents in France, Italy and Spain).
- Continental (with respondents in Belgium, Germany, the Netherlands and Switzerland).

- Northern (with respondents in Denmark, Norway and the United Kingdom).

A total of 4,889 answers have been recorded as a result of the survey process. Amongst these respondents, 1,980 declared to have a vehicle manufactured from 2018 onwards, which means that 40% of the total respondents own or regularly drive a vehicle which would likely qualify as a "connected vehicle" based on, at least, the minimum connectivity capabilities provided by the eCall regulation.

The results have been categorized in two groups: (i) awareness, perceptions and attitudes towards data processing in the context of connected vehicles; and (ii) data empowerment: information, consent and rights. Among the results, it is worth highlighting the following:

- Across the jurisdictions included in the Study, there is certain degree of awareness about connectivity features of connected vehicles and the fact that vehicles can collect and share information.
- Among the respondents, the general perception is that the information collected and shared by connected vehicles is both personal and non-personal, and a significant part of the respondents have the perception that this information is solely non-personal.
- Most respondents declared to feel comfortable sharing information from their vehicle with different entities but only to the extent that they could choose with whom, and what type of data to share, and stop doing it at any given time. When asked about the services they would be willing to share information with, the most common preference is early detection of necessary maintenance and repairs, with detailed monitoring and recommendations. Following close, respondents are in favour of receiving information provided by the vehicle about traffic and suggestions about best routes and alerts provided by the vehicle of dangerous driving conditions ahead.
- Generally speaking, there is a shared perception amongst respondents that drivers have no control over the data shared by connected vehicles and show concern about this lack of control.
- Most respondents answered that they have not given consent for the processing of the data collected in the context of vehicle connectivity. Likewise, most of the respondents who have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer declared that they were not informed at all about the fact that information would be collected from the vehicle and the purposes for which the information could be used or about how to control the information collected from the vehicle (e.g. how to make a request or complaint, who to contact, etc.).
- As regards perceptions and awareness about data protection rights, a relevant number of respondents are aware about their right to be informed, as well as about their right to lodge a complaint before a supervisory authority, their right of access, erasure, object to the processing and rectification. Numbers decrease relevantly when asked about awareness of their rights to data portability, and to not to be subject to automated individual decision-making.
- A very limited number of the respondents declared to have ever exercised any of their rights. From those declaring to have exercised one of these rights, most respondents have

declared to have exercised their right to rectification, followed by erasure and access. Only a very limited number declared to have exercised their data portability right. When a right has been exercised, a majority of the respondents declared not to have received a satisfactory result, either because they did not to receive an answer to their request at all, because they received an incomplete answer, because the answer came too late or because the process was too complicated. When a right has not been exercised, the respondents generally share the view that it is because they were not in the need to exercise it.

For the purpose of complementing the research on the degree of consumer awareness with regard to vehicle data, four ***'Mystery shopping'*** ("**MS**") exercises were conducted at different vehicles' point of sales. The ultimate goal of the MS exercises was to evaluate the level and transparency of information provided to consumers at the vehicle points of sales.

Overall, the MS exercises revealed a significant lack of information about vehicle data collection and processing at the point of sales visited.

While some information about vehicle connectivity is provided at the point of sale, this information exclusively concerns the connectivity functionalities available and the related user's experience. However, it does not cover the implications of such functionalities, i.e. the underlying vehicle data processing.

In the best-case scenario, limited information about vehicle data processing aspects was provided but only after inquiring by the person conducting the exercises ("**Mystery Shopper**"). Even in these cases, the sales representatives were reluctant, unwilling or unprepared to provide general information about vehicle data processing or elaborate on any of the questions raised.

No additional information resources (such as privacy policies, privacy notices or references to websites where information in this regard can be obtained) – that could assist consumers in understanding the implications of data processing deriving from connected vehicle functionalities – were provided either, even after showing an interest in these issues.

Challenges and opportunities

The Report analyses three areas which might present challenges and opportunities to the stakeholders involved in the automotive markets linked to connected vehicles. It starts by analysing different types of contractual/informative documents relevant to the processing of personal data in the context of connected vehicles, selected from different OEMs. It continues by identifying the opportunities and benefits for different actors and society derived from an effective implementation of the right to data portability. Finally, it studies whether the current data protection and privacy legal framework and the conditions under which OEMs collect, process and make their data available to third parties, might create disadvantages to ISPs when offering services and developing innovative services for vehicle users.

In relation to the review of contractual/informative documents relevant to the processing of personal data in the context of connected vehicles, the aim was to assess (i) the clarity of the information/conditions and implications on the sharing and processing of vehicle data; and (ii) whether consumer consent is requested in connection to the use of their (personal) data, including third-party use.

Main findings in this area include:

- Some information about the processing of personal data by connected vehicles is not always made available by OEMs to consumers.
- The information provided by OEMs to consumers about the processing of personal data by connected vehicles is often fragmented across different documents.
- The information provided by OEMs sometimes shows deficiencies regarding data sharing aspects.
- In a lot of the documents studied, the information provided by OEMs is incomplete, insufficient and hard to find.
- Sometimes OEMs collect geolocation data "by-default" prior to having obtained consent from the consumer, against GDPR's requirement that consent shall be provided through a clear affirmative act.

The Report explores the impact that the right to data portability could have on the different stakeholders in the connected vehicle ecosystem whether this right was designed in a way in which consumers could exercise it fully and without significant constrains. The aim is to evaluate whether this would create benefits for industry's stakeholders.

An effective, easy-to-implement data portability right would increase innovation in the sector, foster cooperation between stakeholders to find synergies and develop better products and increase competition in the market by lowering switching costs and entry barriers. A context in which data portability was fully implemented and easy to exercise, a greater number of actors could contribute to finding use cases in which data could potentially be used to create new business opportunities and, therefore, make the overall market grow. Such an implementation of the right to data portability would also contribute to have a positive public impact in the realms of development of smart cities, infrastructure improvement, reduction of accidents or emission decrease. It would also foster the empowerment of individuals through increased autonomy by reducing switching costs and greater consumer choice and can also contribute to the enhancement of the products at their disposal and better prices. The increase on data liquidity through data portability would accelerate market maturity and maximize value per vehicle and has the potential to make the automotive market grow through new solutions as players take more advantage from data.

Finally, the Report studies whether the current data protection and privacy legal framework and the conditions under which OEMs collect, process and make their data available to third parties, might create disadvantages to ISPs when offering services and developing innovative services for vehicle users.

In this regard, despite its purpose is the protection of the fundamental rights of individuals, the data protection and privacy legal framework could sometimes constrain the voluntary sharing of data. Further, these constrains or limitations might be leveraged to avoid, limit or control the sharing of personal data and foster data concentration, entrenching an advantageous market position for certain players (i.e. OEMs) based on better, even exclusive access to data and the control over the terms and conditions under which data is shared in the market, with adverse effects on ISPs.

On a related matter, the current legal design of the right to data portability under Article 20 GDPR and uncertainties around its application in practice challenge the ability of this tool to serve as a mechanism to put an end to the current situation where OEMs are gatekeepers of the data collected from connected vehicles, hence proving ineffective for serving as a data empowerment or antitrust tool, to the detriment of ISPs.

Finally, in practice, OEMs conditions can foster limitations to the actual control vehicle users have over their personal data processed, and this can discourage seamless access or transmission of data to ISPs, with a negative effect on them.

Conclusions

The so-called "privacy paradox" illustrates how, in bulk, internet users tend to express much concern in surveys about their privacy and concur on the need and wish to protect it. However, at the same time, they generously share and dispose of their data when consuming digital services, e.g., by accepting cookies. Typically, the paradox points at two possible reasons: either users are not actually concerned about their privacy, although they declare so, or users lack of real and effective means in practice to express their privacy preferences. The Study indicates that, in the context of car connectivity, the reason behind the existence of a privacy paradox is that vehicle users' concern about privacy is not paralleled with mechanisms to allow them to make informed and granular decisions about their privacy and control their privacy preferences.

A glance at the future brings further reasons for concern: in a world that is increasingly connected, the issues found in the present are indicators of dangerous dynamics.

Soon, all vehicles will have connectivity capabilities and will be able to collect growing amounts of very heterogenous data about their users and environment. Recipients of the data collected from connected vehicles will have tools at their disposal for the processing of data in ways that we can barely conceive now. In this future, the contour of individuals' privacy fade; it will be increasingly easier for organizations to identify individuals and combine information to reach insights and conclusions about them with little or no knowledge of the individual.

Lack of adequate information will very quickly turn into users' lack of control over their personal data. Opaque data collection and processing, as well as incomplete or too complex information about the processing of data in the context of connected vehicles will have the effect that consumers will lack the means to understand the impact and risks of such data processing. If not appropriately informed about the rights that privacy and personal data protection regulations grant them in connection to the processing of their personal data, the idea of control will be, more than never, illusory. Lack of control will only deepen and consolidate if the limitations to make use of legal tools for control persist, particularly limitations derived from the current legal design and functioning of the right to data portability.

Furthermore, the future ePrivacy rules will most likely create a more flexible framework to use the connected vehicle's processing and storage capabilities or the collection of information from the vehicle without the end-user's consent, therefore potentially contributing to consumers' loss of control over their personal data. The enhanced flexibility in what regards to legal bases other than consent brings increased complexity to the table, and it will likely derive in increasing difficulties in providing information that is easy to understand for consumers and complete at the same time.

Present issues and future dynamics recommend taking action on the realm of transparency, consent and rights to foster real control of consumers in the context of connected vehicles.

Recommendations

Having regard to the GDPR's manifested objectives and the criteria shared by the main EU data protection regulators, some technical architectures for data sharing between stakeholders provide vehicle users a higher degree of control over personal data and consequently they are significantly better suited to satisfy the legislation's objectives. These architectures are those which primarily rely on local processing within the vehicle rather than the default transfer of personal data outside of it, on the one hand, and which provide vehicle users with real, effective control over the sharing of personal data with third parties, including with OEMs, on the other. Accordingly, the adoption of a sector-specific regulatory solution establishing a technical architecture which promotes local data processing and vehicle users' control over vehicle data is recommended.

In relation to transparency, an effort for increased harmonisation, availability and understandability of the privacy policies and other information touchpoints can be achieved in the form of soft laws or guidelines. Also, intervention at a legislative level is recommended for the provision of standardised icons in order to provide mandatory data protection information in an easily visible, intelligible and clearly legible manner, as well as a meaningful overview of the intended processing in the specific context of car connectivity.

The eventual adoption of the ePR Proposal and the likely innovative elements it will bring to the table, combined with the particularities of the connected vehicle ecosystem will call for updated guidelines on consent and even specific guidelines in the context of car connectivity.

Finally, the specialties of the car connectivity ecosystem and the potential benefits that this right could bring justify the design of a sector-specific regulatory solution establishing the main traits of the right to data portability, the technical requisites for data and service interoperability, standard solutions for safety and security and standard processes for its practical application.

1

Section I: Background & objectives

This section provides the background necessary to understand the conceptual framing of this Study, introduces the reasons behind its performance and lays down its different objectives. It briefly explains car connectivity and the crucial role data plays in it, to later approach the debate concerning privacy in connected vehicles within the context of car connectivity challenges and other open debates which are inextricably linked to privacy, notably governance of data generated in the context of vehicle connectivity. After presenting the reasons justifying the relevance of this Study, this section finally explains the objectives and main purpose underpinning the Study.

I. Background

Global megatrends did not go unnoticed for the mobility industry.

As it happens in most industry sectors, emerging exponential technologies are accelerating and radically changing the automotive and mobility sectors. In this context, car connectivity plays a leading role as it can bring great benefits for users, as well as for society.

Connected vehicles, i.e., vehicles equipped with sensors and connectivity functionalities,[13] collect information from the vehicle and its surroundings and communicate with the outside world through a wireless connection to the internet.[14]

Connectivity does not only allow for new useful functionalities to be offered to car users, but it also supports the development of advanced driver assistance systems underpinning autonomous vehicles.[15] Achievements in road safety and quality, reduction of accidents, congestions and emissions, are among other advantages.

The potential of car connectivity to unlock value to the mobility industry, car users and society as a whole has fostered a policy discussion in the European Union ("**EU**") and within its member States on how to best enable connected driving and to address its opportunities and challenges. From 2015 the Digital Single Market Strategy for Europe[16] provided a wide strategic framework for European citizens to fully benefit from the digital economy, resulting in important political initiatives with relevance in the realm of car connectivity.[17]

Connected vehicles rely heavily on data. Through different input sources such as GPS trackers, telematic boxes, cameras, microphones, or sensors, connected vehicles can produce significant

[13] Connectivity can be established in a number of ways, notably through a built-in SIM card in the vehicle. See: Kerber, Wolfgang and Frank, Jonas, Data Governance Regimes in the Digital Economy: The Example of Connected Cars, 2017, p.18.

[14] In its Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, the European Data Protection Board ("**EDPB**") defines the connected vehicle as "a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle". Along the same lines, the European Data Protection Supervisor ("**EDPS**") that sensors with which cars are equipped "can be built-in (i.e. offered by the connected car internal system) or brought-in (i.e. connected through an external device, such as a smartphone)". See: EDPS TechDispatch on Connected Cars, Issue 3, 2019. This Report takes a similar broad approach to the concept of connected vehicle and considers that data processed in the context of connected vehicles is not only limited to data collected by the vehicle's internal systems but also encompasses data collected from telematic boxes, from the communication with personal devices, for instance, through Apple's CarPlay or Android Auto, as well as through the use of mobile applications where the user manually inputs vehicle or driving information.

[15] Giving rise to the wider concept of Connected and Automated Mobility (CAM).

[16] See EU Commission, A Digital Single Market Strategy for Europe, 6.5.2015, COM(2015) 192 fin.

[17] See EU Commission, A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, 30.11.2016, COM(2016) 766 fin.

amounts of data of different nature. This can include: operational data (e.g. speed, location, number of passengers, fuel), data pertaining to maintenance aspects (e.g. oil levels, milage due, technical problems), data about the surroundings (e.g. temperature, weather conditions, road marking), user's selected settings and driver's behaviour (e.g. seat and steering wheel position, speed patterns, distances travelled), infotainment data (e.g. phone's information relating to messages, contacts, call history), car users' personal details (e.g. name, contact and financials details provided to the vehicle's operating system, for instance, through a smartphone connected to the vehicle), etc.[18] The number of connected vehicles is expected to only increase, positioning the automotive sector as one of the largest data generators.[19] This is fostering the development of innovative data-enabled solutions and business models which are already disrupting the traditional interaction between car users and service providers.[20] Such solutions include, among others, predictive repair and maintenance services, remote delivery of fuel or on-demand vehicle washing to where the vehicle is parked, adjustments on insurance rates based on driving behaviour, or receiving information directly from the vehicle about driving conditions ahead, nearby scenic spots, hospitality services, offers, discounts, coupons of commercial establishments based on location, season or other elements.

European institutions are well aware of the relevant role data plays in the digital economy in general[21] and in the mobility sector, in particular.[22] The political thrust has culminated in several data-related legislative and regulatory initiatives, both of general scope or sector-focused. Hard and soft law has been designed to apply horizontally to all sectors in the realms of data protection and privacy,[23] data governance,[24] non-personal data,[25] open data and re-use of public sector data, [26] and sharing private sector data (business-to-business – B2B – and business to government – B2G).[27] As for legislation specifically designed for the automotive sector, notable areas are those concerning type approval requirements as regards to the deployment of vehicle emergency systems[28] and standardised access to vehicle data.[29]

[18] Engers, Tom & de Vries, Dennis, *Jusletter-IT privacy-on-wheels*, 2019, p. 4.
[19] Gaspare Fiengo, Giulia Lovaste, *Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform*, Legal Study, 2021.
[20] *Ibid*., p. 3.
[21] European Commission, A European strategy for data, 19.2.2020, COM(2020) 66 fin.
[22] See EU Commission, Building a European data economy, 10.1.2017, COM(2017) 9 fin; EU Commission, Towards a common European data space, 25.4.2018, COM(2018) 232 fin.
[23] Including the General Data Protection regulation and the e-Privacy Directive, which are analysed in detail later on.
[24] Proposal for a Regulation of the European Parliament and of The Council on European data governance (Data Governance Act), COM/2020/767 final.
[25] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), PE/53/2018/REV/1, OJ L 303, 28.11.2018, pp. 59–68.
[26] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, pp. 56–83.
[27] EU Commission, 2021, Consultation on a Data Act & amended rules on the legal protection of databases; and Guidance on sharing private sector data.
[28] Regulation (EU) 2015/758 of the European Parliament and of the Council 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, OJ L 123, 19.5.2015, pp. 77–89.
[29] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (Text with EEA relevance), OJ L 171, 29.6.2007, pp. 1–16, as amended by subsequent regulations and as developed by delegated acts.

The EU Communication "On the road to automated mobility: An EU strategy for mobility of the future"[30] offered an overview of some of the crucial challenges ahead of car connectivity, including the following: safety and cybersecurity risks, liability, ethical questions, standardization and interoperability problems, privacy concerns, and the governance of data, especially access to in-vehicle data.

A great deal of attention has been given to the governance of data generated by connected vehicles, i.e. who can access and decide over this data. A long-standing policy discussion has developed around the confronted views defended by vehicle manufacturers (or original equipment manufacturers, "**OEMs**"), on one side, and independent service providers ("**ISPs**"), on the other.[31] The former produce and sell vehicles and have a *de facto* control over the data generated by connected vehicles by means of controlling access to the IT systems of vehicles. OEMs uphold this situation through mainly safety and security arguments giving rise to the "extended vehicle" view, whereby they are in control of the development, implementation and management of connectivity-related software and hardware as *extensions* of the vehicle. This gatekeeper position allows them to generate additional sources of revenue by monetizing the data, as well as put them in a position of control over markets for complementary data-driven services. On the other hand, ISPs represent a myriad of service providers which populate the automotive markets, such as component suppliers, independent repair and maintenance service providers (including spare part producers), insurance companies, rental and car sharing companies, fleet managers, independent automobile dealerships, or, more generally, providers of mobility services for vehicle users (e.g., infotainment, parking, navigation, assistants). ISPs claim that the current situation whereby OEMs are gatekeepers of data can endanger their access to the emergent ecosystems linked to car connectivity, resulting in downward competition and less innovation and user choice.[32]

While these "lock-in" effects have been mitigated to some extent by sector specific regulations,[33] ISPs advocate for the implementation of technical solutions to allow more direct access. This could happen either by putting the data directly under the governance of a neutral entity in charge of granting non-discriminatory access, or solutions based on platforms supporting local storage of data in the vehicle to provide users direct control over their data.[34]

We face a complex multi-stakeholder environment where several actors claim access and use of the data based on their corresponding interests. This situation is not dissimilar to other internet

[30] EU Commission, On the road to automated mobility: An EU strategy for mobility of the future, 17.5.2018, COM(2018) 283 fin.

[31] See Gaspare Fiengo, Giulia Lovaste, *Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform,* Legal Study, 2021, pp. 4-5; and Kerber Wolfgang and Frank Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017, pp. 20-21.

[32] The discussion about access to aftermarkets and the problem of competition within them has been a relevant topic for decades in the repair and maintenance services and several initiatives have been put in place, most notably, the Motor Vehicle Block Exemption Regulation, as composed by Regulation (EU) No 461/2010 - application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector, and Regulation (EU) No 330/2010 to vertical agreements concerning conditions for the purchase, sale or resale of spare parts for motor vehicles, or for the provision of repair and maintenance services for motor vehicles.

[33] Access to in-vehicle data framework, especially the type approval regulation, established in 2007 and further enhanced in 2018 and currently under discussion to include new players along with repair and maintenance services: car sharing, mobility as a service and insurance services.

[34] See Strategy on C-ITS; C-ITS TRL, *Access to In-Vehicle Data and Resources – Final Report* (2017); and Gaspare Fiengo, Giulia Lovaste *, Liabilities of Independent Service Providers*, pp. 6-11.

of things ("**IoT**") ecosystems, situating the discussion of data governance in connected vehicles as an example of the wider discussion concerning data governance in IoT environments.[35]

Privacy in the context of car connectivity is also subject to public discussion as several points remain unresolved.

Much of the data,[36] if not all, that is generated and processed in connected vehicles constitutes personal data because it relates to natural persons that are identified or identifiable. Some of the data collected by connected vehicles can be of sensitive nature for the individuals concerned and its misuse could have severe implications for someone's personal and professional life. For instance, vehicles can collect detailed records of a person's movements and destinations by means of geolocation and can recur to biometric data to allow access to the vehicle or to the user's private settings. Vehicles could record administrative infringements, such as speeding or failing to stop at a red light, or even criminal offences. The quantity and very diverse nature of the data collected by connected vehicles allow for the combination of data in a way that can reveal detailed information about car users' preferences or driving behaviours. In parallel, processing capabilities of large amounts of raw data and data analysis capabilities are developing at a fast pace with the development of big data techniques and artificial intelligence ("**AI**") solutions. As a result, recipients of the data collected from connected vehicles have tools at their disposal for the processing of data in ways that were not conceivable before and which are evolving fast and uninterruptedly.

Therefore, despite the undeniable benefits and opportunities brought about by connected vehicles, they raise significant privacy risks and concerns. Pan-European data protection watchdogs, the European Data Protection Board ("**EDPB**")[37] and the European Data Protection Supervisor ("**EDPS**")[38] concur in identifying the following as the most relevant: lack of control and information asymmetry, excessive data collection and storage, lack of purpose limitation/further processing and security.[39]

It comes as no surprise that privacy represents a real concern. Particularly in the context of connected vehicles, consumers have developed a sensitivity concerning the need for organizations to preserve their privacy and protect their personal data and they have increasing expectations over self-determination regarding personal data choices.[40] Accordingly, it is the aim of data protection and privacy regulations to provide users with control over their personal data.[41]

---

[35] Kerber Wolfgang and Frank Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars,* 2017, p. 4.

[36] See, among others: European Data Protection Board, *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*, version 2.0, 2021, p.6; European Commission and TRL, *Access to In-Vehicle Data and Resources – Final Report*, 2017, p. 124; or European Commission, C-ITS Platform – *Final Report*, 2016, in the context of messages (cooperative awareness messages and decentralized environmental messages) between vehicles and cooperative intelligent transport systems.

[37] *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*, version 2.0, 2021, pp. 11-15.

[38] EDPS, *TechDispatch #3: Connected Cars,* 2019.

[39] Also relevant in this context, International Working Group on Data Protection in Telecommunications, *Report on connected vehicles*, 2018.

[40] See https://mycarmydata.eu.

[41] Félicien Vallet, *The GDPR and Its Application in Connected Vehicles—Compliance and Good Practices*, 2019, p. 249.

At a glance , the relationship between the two pieces of legislation currently in force governing the processing of personal data by connected vehicles is not necessarily seamless, creating several gaps and unresolved issues. The two pieces of legislation are the General Data Protection Regulation ("**GDPR**")[42] and the Directive on privacy in electronic communications ("**e-Privacy Directive**").[43] Hereinunder, we will refer jointly to these regulations as the "**EU Privacy Regulatory Framework**".

To a great extent, the reason behind the discoordination between these legal instruments lies on the fact that the e-Privacy Directive is in force since 2002 while the GDPR since 2018. Despite the efforts of the European legislator to release an updated e-Privacy framework at the time the GDPR was passed, it was not possible to reach an agreement on time. At the date of publication of this Report, the regulatory piece which will replace the e-Privacy Directive (e-Privacy Regulation Proposal; "**ePR Proposal**")[44] is yet under negotiation between the European Parliament and the Council of the European Union. The underlying difficulties with regard to this negotiation are justified in the significant impact this new legislation will have to several economic sectors, including that of connected mobility. The positions of the European legislators are quite far away one from the other and the final effects for connected mobility will be very different depending on whether the final text tends more to the European Parliament's or the Council's position.

The above considerations justify an in-depth analysis of the regulatory framework set up by these laws with the aim of clarifying the rules applicable to the processing of data collected in the context of connected vehicles. In addition, it is worth exploring the status of the legislative process concerning the ePR Proposal to analyse the implications that this new set of rules can have to car connectivity, distinguishing between the positions of the European Parliament and the Council of the European Union.

In a scenario where vehicles are increasingly connected and are able to collect growing amounts of very heterogenous data about their users and environment, where the recipients of that data have processing capabilities developing at a fast speed, lack of adequate information can quickly turn into users' lack of control over their personal data. Opaque data collection and processing, as well as incomplete or too complex information about the processing of data in the context of connected vehicles have the effect that consumers do not have the means to understand the impact and risks of such data processing. Further, if not appropriately informed about the rights privacy and personal data protection regulations grant them in connection to the processing of their personal data, the idea of control becomes unrealistic. Even if consumers could have an idea of the rights that these regulations grant, if they do not understand what happens with their data, control over them is not real. It is worth remembering that the processing of data in the context of connected vehicles involves processing data that can be considered sensitive in

[42] Regulation (EU) 2016/679 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 (General Data Protection Regulation).

[43] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as revised by directive 2009/136/EC.

[44] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.2.2021, 2017/0003(COD), 6087/21.

nature, where information and transparency efforts should be reinforced to ensure consumers understand the implications of their interaction with vehicles.

In a context such as the described, there are reasons to explore whether consumers' control and empowerment is a reality or not. However, little empirical data currently exists to understand the possible shortages, both of a legal or practical nature, in the transparency and consent processes followed by industry players (especially by OEMs, as controlling or influencing access to vehicle data and acting as gatekeepers in most cases), and to determine whether drivers and vehicle users have an actual, effective control over their personal data. This is why this study derives findings from primary data collected from different sources. On the one hand, a survey conducted in different European regions serves to explore consumers' awareness and sensitivities regarding vehicle data processing, as well as the obstacles consumers face when exercising their data protection and privacy rights. On the other hand, several mystery shopping experiences have been conducted and different documentation has been reviewed to analyse how information is presented to consumers, both at point of sales and in sales and purchase agreements and privacy policies. The aim is to understand whether consumers' sensitivity in relation to the processing of vehicle data and their growing expectations regarding data empowerment are currently being met by market practices to provide information and control in relation to data collected from connected vehicles.

The right to data portability represents another key element in the discussion around data subjects' informational self-determination. This topic is in direct connection with the debate around the conditions of access to data generated in the context of the connected vehicle. [45] Although this legal mechanism has the potential to mitigate "lock-in" effects concerning the access to the data generated by connected vehicles and it can serve to foster consumers' control over their personal data, relevant technical and legal issues remain unresolved, challenging its ability to serve as an effective empowerment and antitrust tool. For instance, OEMs could make use of different arguments to limit or delay the exercise of this right, thus constraining the potential of data portability both as an antitrust and a data empowerment mechanism. As an example, OEMs are legally obliged to provide the data in a "commonly used" format pursuant to Article 20(1) GDPR. Nevertheless, the lack of standardization of vehicle data hinders the chance of finding a commonly used format useful for ISPs. Further, it is unclear what data would be within the scope of the right to data portability, as some vehicle data could be considered as "inferred data", data concerning to persons other than the one exercising the right, data potentially revealing trade secrets or anonymised data.[46] From an economic perspective, it is also relevant to look at the transaction costs that car users might face when exercising this right.

Therefore, studying how the exercise of the data portability right is functioning in practice will provide useful insights to assess whether further policy or regulatory action is advisable. An economic approach to the potential impact this right might have on the current *status quo* between OEM and ISPs and its broader potential in mobility can offer the right context to support why seamless, informed data portability should be provided to car users.

[45] See Osborne Clark, *What EU Legislation says about car data - Legal Memorandum on Connected Vehicles and Data, Legal Study Commissioned by FIA Region I in the context of the My Car My Data Campaign*, 2017, pp. 12 -17; Wolfgang Kerber, *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 2019, JIPITEC 310, paras 42-45.

[46] European Data Protection Board, Guidelines on the right to "data portability", 5.4.2017, WP 242 rev.01, pp. 12-14.

The above considerations are relevant from the point of view of consumers. However, the relative position of ISPs in comparison to OEMs in relation to the EU Privacy Regulatory Framework represents also an area generally overlooked by research. In particular, whether this legal framework (and the contractual activity based on it) might create disadvantages on ISPs in comparison to OEMs, can bring a good basis to the general discussion around privacy, but also to the larger policy discussion on "access to in-vehicle data and resources" of connected vehicles.

II. Objectives of the Study

This report "**GDPR application in the context of car connectivity**" (the "**Report"**) compiles the findings of an expert study commissioned by the Fédération Internationale de l'Automobile ("**FIA**") and conducted by Ernst & Young Abogados, S.L.P. from July 2021 to November 2021 (the "**Study**").

The objective of the Study is the assessment of how the EU Privacy Regulatory Framework has been applied in Europe with regards to car connectivity, and to understand the level of consumer awareness in relation to vehicle data, the manner in which consent for the processing of such data is collected and given, as well as the challenges faced by consumers when exercising their rights under the GDPR.

Accordingly, the Report starts by examining the application of the EU Privacy Regulatory Framework in the context of vehicle connectivity, providing an overview of the current framework in force and analysing the potential implications of the future e-Privacy rules for vehicle connectivity and data sharing.

At a second stage, the Report focuses on the level of consumer awareness regarding connected vehicles and their sensitivity regarding sharing vehicle data. For this purpose, the Report analyses: (i) consumer awareness on data protection and privacy rights with regards to car connectivity; (ii) challenges faced by consumers when exercising their rights under the GDPR (e.g., data portability); and (iii) consumer sensitivity on sharing vehicle data. Furthermore, the Report analyses the information consumers receive at the vehicles point of sales.

As regards the challenges and opportunities brought by car connectivity and vehicle data, the Report includes the conclusions reached after analysing consumer vehicle purchase contracts and privacy policies, looking at: (i) the clarity of the conditions and implications on the sharing of vehicle data; and (ii) how the consumer consent is requested concerning the use of their (personal) data, including third party use. In addition, the Report covers the potential of data portability in mobility and its impact on connected vehicles, and assesses the disadvantages posed by the current EU Privacy Regulatory framework and OEMs terms and conditions to ISPs when offering vehicle servicing, repair and maintenance, and innovative services to motorists.

Finally, the Report includes a set of recommendations and proposes action lines for policy makers to adopt rules which empower consumers to gain control over their personal data.

III. Structure of the Report

The Report is structured as follows:

Section II assesses how the personal data protection and privacy legal framework has been applied in relation to car connectivity. This section is divided in two subsections: subsection I analyses the current EU Privacy Regulatory Framework in detail – GDPR, e-Privacy Directive and relevant sector legislation – and how it applies to the connected vehicle, including the view of regulators' positioning in this regard. Subsection II presents the ePR Proposal and analyses the different texts that EU political institutions are negotiating to point at the implications that the ePR Proposal could have for vehicle connectivity and data sharing.

Section III presents the findings of two practical exercises: the distribution and analysis of a survey across different EU regions and mystery shopping experiences at vehicles' point of sales. This section gives an overview of the methodologies followed for these exercises and provides the findings for each of them. Subsection I presents the results of the survey and subsection II presents the findings of the mystery shopping experiences.

Section IV conducts three analyses of areas which might present challenges and opportunities to the stakeholders involved in the automotive markets linked to connected vehicles. Subsection I presents findings resulting from the analysis of different types of contractual/informative documents relevant to the processing of personal data in the context of connected vehicles, selected from different OEMs. Subsection II identifies the opportunities and benefits for different actors and society derived from an effective implementation of the data portability right. Finally, subsection III studies whether the current EU Privacy Regulatory Framework and the conditions under which OEMs collect, process and make their data available to third parties might create disadvantages to ISPs when offering services and developing innovative services for vehicle users.

Section V presents the conclusions of the Study and provides policy recommendations on how to empower consumers through legislation.

Several appendixes support the content within the sections above:

- **Appendix I** includes a table to compare the different versions of the ePR Proposal released by the EU institutions involved in the legislative process.
- **Appendix II** is a fact sheet where the detailed methodology of the survey process is explained.
- **Appendix III** is a fact sheet where the detailed methodology followed during the mystery shopping experiences is elaborated, as well as where each individual experience is explained in detail.
- **Appendix IV** is a fact sheet explaining the methodology followed to review consumer vehicle purchase contracts and privacy policies and presenting the specific findings for each OEM in detail.
- **Appendix V** includes the Report's bibliography.

2

Section II: Application of the EU privacy regulatory framework in the context of vehicle connectivity

This section aims at understanding the regulatory framework applicable to the connected vehicle ecosystem and analysing the implications the ePR Proposal can have for this ecosystem. For this purpose, it starts by analysing the current EU Privacy Regulatory Framework in detail – GDPR, e-Privacy Directive and relevant sector legislation – and how it applies to the connected vehicle, including the view of regulators' positioning in this regard. It continues by presenting the regulation that is set to substitute the e-Privacy Directive, analyses the legislative status and the different texts that EU political institutions are negotiating. Finally, it analyses the implications that this new regulation could have for vehicle connectivity and data sharing.

I. Relevant EU rules and guidelines

In the context of car connectivity, the general personal data protection and privacy rules are laid down in two laws: the GDPR and the e-Privacy Directive.[47] In addition to them, there are sector regulations with certain relevance in the field of privacy, to the extent that they impose certain obligations in this regard and regulate access to data collected from connected vehicles.

In addition, a legislative initiative to update e-Privacy rules is currently under negotiation. For this reason, there is not a definitive text yet but only different versions issued by the European Commission, the European Parliament and the Council of the EU.

The following pages will serve to go through the abovementioned regulations, to understand how they apply to data processed in the context of connected vehicles and to highlight relevant aspects to take into consideration therewith.

A. General Data Protection Regulation

The GDPR, fully applicable since May 25, 2018, provides a comprehensive set of rules for the processing of personal data, aiming at achieving a consistent and high protection of personal data, placing citizens back in control over their data, and providing legal and practical certainty for economic operators, individuals and public authorities through a pan-European unified framework.[48]

The GDPR applies when personal data is processed. Article 4(1) GDPR defines personal data as "any information relating to an identified or identifiable[49] natural person". In relation to data processing in the context of connected vehicles, personal data includes all data that can be associated with any of the individuals using a connected vehicle (owner, driver, passengers).

As analysed later in further detail, any data that can be related to an identified or identifiable individual shall be considered personal data, regardless of its nature. Therefore, personal data is not limited to identifiers of the people using the vehicle such as a name, surname, national ID, etc., but also includes any information that can be linked to these persons, notably via the

[47] A "directive" is an EU legislative act that sets out certain objectives that Member States must achieve. Each country can decide how to implement directives into national laws, by creating or adapting their internal legislation, in order to reach these goals. In contrast, a "regulation" is a binding legislative act, applicable and enforceable in all Member States, without the need of further implementation.

[48] See Recitals 5-7 GDPR.

[49] The Article 29 Data Protection Working Party ("**Data protection WP29**", which is currently the EDPB) considered in its "Opinion 4/2007 on the concept of personal data" (p. 11) that, in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able").

vehicle serial number or the vehicle licence plate number. Likewise, technical data such as oil levels, milage due or technical problems can legally qualify as personal data to the extent that it can be associated with an identified or identifiable person. [50]

Where data has been anonymized (i.e. irreversibly de-identified), it is no longer considered personal data.

This Report understands the definition of connected vehicle as a broad concept.[51] As such, data provided by means of connection via personal devices, such as a mobile phone, or data provided by mobile applications independent of the vehicle and offering driving-related services is considered as data processed *in the context of the connected vehicle*, even if it does not necessarily rely on the vehicle's system or connectivity functionalities for collection and processing.

Virtually any operation performed on personal data qualifies as "**processing**" pursuant to Article 4(2) GDPR,[52] regardless of it being performed by manual or automated means. The person to which the data relates to is called "**data subject**" and the person or organization determining the purposes for which and the means by which personal data is processed is the "**data controller**".

Core principles, rights and main obligations for data controllers

Personal data processing is governed by a series of principles and requirements:

Lawful processing:

Personal data may only be processed if the data controller has a valid lawful basis for processing among those listed by the GDPR.[53] These legal bases are the following: (i) the data subject gives consent for his or her data to be processed for one or more of the specified purposes; (ii) the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (iii) the processing is necessary to comply with a legal obligation; (iv) the processing is necessary to protect the vital interests of the data subject or of another natural person; (v) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; and (vi) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Outside of these cases, any processing shall be considered unlawful and cannot be performed.

It must be highlighted that, when data processing is based on consent, it shall be obtained validly, meaning that it is free, specific, informed and unambiguous.[54] The data controller must

[50] Commission Nationale de l'Informatique et des Libertés (CNIL), *Compliance package for a responsible use of data in connected cars,* 2017, p. 5.
[51] See *Ibidem* and Guidelines 01/2020 on connected vehicles.
[52] Including the 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.
[53] See Article 6 GDPR.
[54] See Article 7, Recitals 32 and 43 GDPR and EDPB "Guidelines 05/2020 on consent under Regulation 2016/679".

be capable of proving that it has obtained consent. Finally, the data subject must be capable of withdrawing consent at any moment, through a channel that ensures withdrawing consent is as easy as it was to give it. Withdrawing consent cannot imply any detriment to the data subject and, specifically, may never imply any cost. This information shall be included when obtaining consent.

Some of the main obligations for data controllers stemming from this principle are:

- Data controllers must have an appropriate legal basis to process personal data.
- Where data controllers process data that can be considered of special sensibility ("special categories of personal data"), data controllers must take additional safeguards to ensure an appropriate protection. [55]
- Data controllers must not share personal data unless they have consent from the data subject or the law expressly allows them to do so. When hiring external services which will have access to the personal data under the responsibility of the data controller, there must be an agreement in place to regulate relevant aspects of the processing and data controllers must only hire entities which are apt to comply with the GDPR.[56]
- Data controllers shall have appropriate legal instruments or rely on exceptional situations to before being able to transfer personal data to third countries.[57]

Transparency:

The main practical implication of this requirement is the obligation to inform data subjects that their personal data is being processed and the obligation to explain to them what is done with the data. The GDPR requires data controllers to give detailed information on how they use and what they do with the data subjects' personal data.[58]

The information must be offered in an easily accessible manner for the data subjects. This means it should be either offered directly to them or it should be placed where it is immediately apparent to them.

The principle of transparency must ultimately be applied considering the data subject's perspective; i.e. consider who the audience is and adapt the language to the average member of that audience. It implies that all efforts necessary for the data subject to know what is being done with his or her data must be taken.

Among the main obligations for data controllers stemming from this principle is the need to to provide data subjects with concise, easily accessible and easy to understand information regarding the processing of their personal data.

Purpose limitation principle:

The GDPR establishes that personal data must be collected for specific and legitimate purposes and that, as a general rule, it must not be used for incompatible purposes. This principle is

[55] See Article 9 GDPR.
[56] See Article 28 GDPR.
[57] See art. 44-49 GDPR.
[58] See Arts. 13 and 14 GDPR, and EDPB "Guidelines on Transparency under Regulation 2016/679" (wp260rev.01).

directly related to the information that must be offered to data subjects, as at the moment data is collected, the purpose for which it will be used must be stated.[59]

The fundamental practical implication of this principle is that the personal data must not be used for purposes other than those explicitly stated to the data subject when the subject was informed about data protection matters. The processing of personal data for purposes other than those for which they have been initially collected must only be allowed when it is compatible with the purposes of their initial collection.

As we will have the opportunity to explore in subsection "GDPR and e-Privacy interplay – the debate around further processing", further processing is an open issue in the context of connected vehicles based on the way the GDPR and the e-Privacy Directive interplay.

The main obligation for data controllers stemming from this principle is that, prior to use personal data with purposes other than those for which the data was collected, they shall perform a compatibility assessment based on the criteria laid down in Article 6(4) GDPR.

Principle of data minimisation

This principle implies that data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means when collecting the data, only personal data necessary to fulfil the purpose for which they were collected shall be requested.[60]

Principle of accuracy

Personal data must be accurate, and therefore must be updated when necessary.[61]

The fundamental requirement arising from this principle consists in implementing measures that allow for the periodic updating of personal data; for example, through periodic communication with the data subjects. This could be good practice in connected vehicles to ensure that, following the sale of a second-hand vehicle, data from the previous owner is deleted and updated with the new owner.

Storage limitation principle

Personal data must not be stored for longer than necessary. The time for which personal data must be stored depends on the purpose for which it was collected; when the data is no longer necessary to fulfil the purpose for which it was collected, the data shall be erased.[62]

This is a challenging principle to comply with in the connected vehicle scenario as the data collected is of very diverse nature, is used for very different purposes and shared with different entities, making it difficult to have an effective control over the retention periods.

Data controllers must be able to control the periods for which they store data and protocol the periodic deletion of personal data.

Integrity and confidentiality principles

[59] See art. 5(1)(b) GDPR.
[60] See art. 5(1)(c) GDPR.
[61] See art. 5(1)(d) GDPR.
[62] See art. 5(1)(e) GDPR.

The GDPR requires that data controllers handle the personal data in a manner which ensures an adequate security of the personal data, applying appropriate technical and organisational measures to protect the data (including against unauthorised or unlawful processing and against accidental loss, destruction or damage).

With this in mind the GDPR introduces a new focus, based on risk, meaning that before selecting the measures to be adopted, data processors must consider the nature, scope, context and purposes of processing, as well as the risk for rights and freedoms of people.[63]

The main obligations for data controllers stemming from this principle are:

- Data controllers must elaborate a record of processing activities to list and keep record of the data processing activities followed in the organization.
- Data controllers must perform, prior to beginning processing, an assessment of the risks the processing activity has on the privacy of the data subjects. To do that, it shall be necessary to perform two distinct risk management procedures, based on the level of foreseeable risk of the activity: (i) if the foreseeable risk is high, a data protection impact assessment ("**DPIA**") must be performed; and (ii) if the risk is not high, a basic risk analysis shall be conducted.[64]
- They also need to put in place procedures to make them capable of dealing effectively with personal data breaches. Where necessary, data controllers have the obligation to notify personal data breaches to a data protection authority or to even communicate the breach to the natural persons affected.[65]

Given the scale and sensitivity of the personal data that can be generated and processed via connected vehicles, it is likely that processing – particularly in situations where personal data is processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals.[66]

Accountability principle

Under this principle, data controllers shall be responsible for, and be able to demonstrate compliance with the previous principles and, in general, with the GDPR. In practical terms, this principle requires organisations to analyse what data they process, for what purpose they are processing it and what type of processing operations are performed. Knowing this, organisations must explicitly determine how they will apply the measures foreseen in the GDPR, ensuring that these measures adequately comply with the Regulation and that they can demonstrate this to data subjects and supervision authorities.

Data subjects' rights

Data subjects have several rights in relation to the processing of their personal data. In particular:[67]

[63] See art. 5(1)(f) GDPR.
[64] See arts. 30, 32, 35 GDPR.
[65] See art. 33-34 GDPR.
[66] EDPB Guidelines 01/2020 on connected cars, p 17.
[67] See arts. 12-22 GDPR.

- Right to information: right to be informed by the data controller about the purposes and other aspects of the processing performed on the data subject's personal data.

  This right is paramount in the context of connected vehicles due to the inherent complexity of the processing linked to them. In line with Recital 39 GDPR, data controllers should ensure consumers are aware of the scope, consequences, and risks of the processing of their data. A basic understanding of the implications linked to the processing activities performed in the context of connected vehicles is key to ensure that data subjects are in a position where they have the means to effectively control their personal data, which is one of the GDPR's declared objectives as per Recital 7.

- Right of access: right to obtain confirmation from the data controller as to whether or not personal data concerning the data subject is being processed, and, where that is the case, right to access to the personal data and the following information: the purposes of processing, the categories of personal data concerned, who the data has been transferred to, how long the data is going to be stored, and the possibility to exercise additional rights, such as the erasure of the data, limitation of the processing or the right to object to commercial communications. Also, to acknowledge the procedure to file any kind of claim before the corresponding authority.

  The right of access is also a key control tool at the disposal of data subjects to be aware of the scope of the processing derived from the use of connected vehicles. The complex set of information that data controllers, such as OEMs, could be processing in the context of connected vehicles recommend that data controllers provide for easily accessible and easy to use mechanisms for data subjects to access their information.

- Right of rectification: right to request the data controller to modify the personal data that is inaccurate without undue delay.

- Right to erasure or right to be forgotten: right to request the data controller for the erasure of personal data that is no longer necessary, under certain circumstances.

  This is also an important right for the connected vehicle environment as it allows car users to request the deletion of the data about them stored in connection to a specific vehicle.

- Right to restriction of processing: right to request the data controller, in certain cases, to stop the processing unless otherwise consented by the data subject or for the establishment, exercise or defence of legal claims.

- Right to portability: right to receive the personal data provided to a data controller, in a structured, commonly used and machine-readable format and to transmit this data to another data controller without obstacles.

- Right to object: right to object, at any time, to the processing of personal data with direct marketing purposes, or to the processing of personal data based on a public interest of the data controller or a legitimate interest of the data controller or a third party.

- Right not to be subject to automated decision-making, including profiling: right not to be subject to a decision based solely on automated processing, including profiling, which

produces legal effects concerning the data subject or similarly significantly affects him or her.

- Right to withdraw consent: right to revoke the consent provided to the data controller at any time.
- Right to file a claim with a control authority: right to lodge a complaint before a data protection authority in order to enforce the data subject's rights or to notify any possible infringement of the GDPR.

The main obligation for data controllers stemming from this principle is to respond to the exercise of rights of the data subjects in a timely manner.

Privacy by design and by default

Privacy by design means ensuring that, from the outset, considerations of privacy are built into every new system, for example in terms of what data is collected, how long it is kept for, how it is stored, and who has access to it. Privacy by default means implementing appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.[68]

This principle affects primarily to OEMs in regard to the design of the means to collect, store and process the data collected through vehicles, as well as to provide a setup which is privacy friendly by default. Privacy by design and by default is an open issue for the industry. At the date of publication of this Report, some automobile manufacturers collect geolocation data by default, unless the car user activates the privacy mode, as we will have the opportunity to see in section IV.I of this Report ("Analysis of the contracts signed by consumers when purchasing a vehicle").

A framework for consumers' control of personal data

It is in the GDPR's declared spirit to put individuals in control of their personal data. For this purpose, this piece of legislation regulates several elements to ensure data subjects can effectively achieve the desired degree of data empowerment. Typically, these elements include the ability for the data subject to consent to the processing, where necessary, the right to be informed, along with the other rights granted to individuals, with especial emphasis on the right to data portability.

When these elements are unified, they compose a framework of control that is also known as the **right to informational self-determination.**[69] In relation to the connected vehicle, the *Commission Nationale de l'Informatique et des Libertés* ("**CNIL**") has expressed that this right shall include: "configurations by default that protect privacy; the option for users to easily modify those configurations, during the entire processing period, especially for the purpose of activating or deactivating services based on consent or on the performance of a contract (e.g. commercial offers personalised on the basis of geolocation or breakdown assistance); where appropriate, the option for users to adjust the level of detail of the data collected to the level of

[68] See art. 25 GDPR.

[69] The CNIL defines this right as the individual's necessary control over their data during the entire processing period. See CNIL, *Compliance package for a responsible use of data in connected cars*, 2017, p. 8.

service requested, e.g. by accessing a map without being geolocated if they do not wish to be guided; and the option for users to access those data easily".[70]

The EDPB defends a similar approach and recommends default limitations to data processing by data controllers, provisions of controls to the data subject to have the possibility to activate or deactivate the data processing for each purpose and to delete the data concerned. Also, data subjects should be able to delete permanently any personal data before the vehicles are put up for sale and should, where feasible, have a direct access to the data generated by these applications.[71]

Debate around the nature of the data processed in the context of connected cars

In its guidelines on connected vehicles, the EDPB has considered that most vehicle generated data qualifies as personal data pursuant to the GDPR, [72] even when the data relates to technical elements of the vehicle and its components.

The EDPB's interpretation assumes that technical data can simultaneously qualify as personal data, thus ruling out interpretations arguing that data generated in the context of connected vehicles cannot be personal and technical data at the same time.[73] Let us not forget that the concept of personal data encompasses *any information,* regardless of its nature. Further, connected vehicle data is normally data *relating to* an identified or identifiable individual to the extent that it is either (i) *about* an individual – "content" element"-; (ii) or can be used/will be used *in order to* evaluate or treat the individual in a certain way – "purpose element"-; or it is *likely to have an impact* on the individual concerned – "result element".[74]

Once accepting that technical data can simultaneously qualify as technical and personal data, the next question is whether the data processed in the context of connected vehicles qualify as personal for all the organizations processing it or only for some of them. As already explained, the determining element for data to qualify as *personal* pursuant to the GDPR is that it relates to an identified or identifiable individual. Accordingly, the question of when a person is identifiable to a specific data controller is paramount to determine whether that specific controller processes personal data or not and, thus, whether the requirements and obligations set by data protection regulations are applicable.

This question confronted two lines of thinking, the "subjective/relative approach" and the "objective/absolute approach".[75] The first one considers that the relevant element to be taken into account is the means *reasonably likely* to be used by the controller to identify the individual concerned. The latter, on the contrary, supports that the "reasonably likely standard" shall be considered not only in relation to the data controller but in relation to any other person, in other words, whether a third party has reasonable means at its disposal to identify the individual, even if this requires additional knowledge exclusively assigned to such third party. It falls from here that almost all data will be considered as personal data if the objective/absolute approach is

[70] *Ibidem*.
[71] EDPB Guidelines 01/2020 on connected vehicles, p. 16.
[72] *Ibid.*, p. 5.
[73] Osborne Clark, *What EU Legislation says about car data says - Legal Memorandum on Connected Vehicles and Data, Legal Study Commissioned by FIA Region I in the context of the My Car My Data Campaign*, 2017.
[74] See Article 4(1) GDPR and Article 29 Working Party, *Opinion on the concept of personal data*, p. 6.
[75] Nadezhda Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology*, 2018.

chosen. As a result, the debate is very relevant to the context of connected vehicles as the nature of the data for the different stakeholders concerned – OEMs and ISPs – can be different depending on the approach selected.[76]

The EDPB points at a "relative approach" to the concept of personal data under the parameters set by the European Court of Justice ("**ECJ**") in its ruling in October 2016.[77] Accordingly, to ascertain the nature of the data, it would be necessary to assess whether or not the specific organization controlling the data is in a position to identify a person behind that data, either because it has the information necessary to identify the person or can lawfully obtain sufficient additional data to link the information to a person and therewith identify that person.

Data from connected vehicles will most likely qualify as personal data in relation to the organizations directly collecting and using the data, especially OEMs which will at least be able to identify vehicle owners with reasonable efforts through information in sales contracts, either between them and the consumer or via their dealership network. Moreover if we take into account that OEMs can access vehicle and vehicle owner data from official vehicle registers for legally defined purposes, such as product recall.[78] Likewise, ISPs deal with personal data in those cases in which agreements are in place with their customers.[79]

B. e-Privacy Directive

The e-Privacy Directive is part of the so-called "Telecoms Package", adopted in 2002 and later revised in 2009), which establishes the regulatory framework for electronic communications in the EU.

The e-Privacy Directive lays down a specific set of rules for the protection of privacy and the processing of personal data in connection with public electronic communication networks and services.

Along with the GDPR, this directive, which came into force in 2002, is the cornerstone of privacy protection in the EU for the digital age and was meant to offer a harmonised framework for EU Member States.[80] Due to the development of the technological landscape and the deep changes that our society has undergone from the year of entry into force of this directive, the EU political institutions have meant to update the e-Privacy rules for several years now. A new up-to-date framework was expected to be adopted at the same time as the GDPR, but the proposal for a new Regulation (ePR Proposal) is yet under negotiation between the European Parliament and the Council of the EU, as we will examine further in subsection II ("Implications of the e-Privacy Regulation Proposal").

In relation to the GDPR, the e-Privacy Directive is *lex specialis*, which means that it particularises and complements the GDPR as regards personal data in the electronic communications sector. All matters not specifically addressed by e-Privacy rules in relation to personal data are, therefore, regulated by the GDPR (for instance, the requirements for a valid legal consent).

---

[76] Osborne Clark, *What EU Legislation says about car data says - Legal Memorandum on Connected Vehicles and Data, Legal Study Commissioned by FIA Region I in the context of the My Car My Data Campaign*, 2017, pp. 4-5.
[77] European Court of Justice, Judgment of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland – C-582/14.
[78] Osborne Clark, *What EU Legislation says about car data says - Legal Memorandum on Connected Vehicles and Data, Legal Study Commissioned by FIA Region I in the context of the My Car My Data Campaign*, 2017, pp. 4-5.
[79] *Ibid.*, p. 10.
[80] See recitals 4-7 e-Privacy Directive.

e-Privacy Directive overview

The e-Privacy Directive lays down a number of harmonized rules with the aim to ensure (i) an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector; and (ii) the free movement of such data and of electronic communication equipment and services in the EU.

The directive, therefore, applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks, and deals with very relevant matters as confidentiality and security of communications, spam or cookies.

The e-Privacy Directive regulates the confidentiality of communications and related traffic data.[81] It expressly prohibits listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data without the consent of the users concerned, unless legally authorised to do so.

On the other hand, it imposes on electronic communications providers the obligation to safeguard the security of their services, by adopting technical and organizational measures which are appropriate in accordance with the risks posed, as well as notification requirements in case of security or personal data breaches.

The directive also regulates the processing of traffic data and location data[82] and establishes a number of requirements relating to certain aspects, such as the presentation and restriction of calling and connected line identification, automatic call forwarding, itemized billing, directories of subscribers and e-marketing.

Finally, the e-Privacy Directive lays down provisions to regulate the conditions under which online tracking can take place through the use of cookies and other tracking technologies.

Relevant rules in the context of car connectivity

Most of the e-Privacy Directive provisions only apply to providers of publicly available electronic communications services and networks (i.e. telecommunication operators). Consequently, these provisions are not relevant for the purposes of the Study.

By contrast, Article 5(3) e-Privacy Directive is a general provision which applies to anyone (including both private and public entities) which stores or gains access to information already stored in a "terminal equipment" of a subscriber or user,[83] regardless of the nature of the data to be accessed or stored. Terminal equipment is defined as either "(a) equipment directly or indirectly connected to the interface of a public telecommunications network to send, process

[81] According to Article 2(b) e-Privacy Directive "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

[82] According to Article 2(c) e-Privacy Directive "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

[83] Pursuant to Article 2(a) e-Privacy Directive "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service. "Subscriber" is not defined in the e-Privacy Directive. The Information Commissioner's Office defines it as "a person who is party to a contract with a provider of public electronic communications services for the supply of such services".

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; or(b) satellite earth station equipment".[84] Typical examples of terminal equipment can be computers, smartphones and, more recently, smart TVs, tablets or other devices connected to the internet, such as refrigerators, vacuums or vehicles. Typically, storing information on an end-user's terminal equipment, or gaining access to information already stored, happens through the use of "cookies" and other tracking technologies.[85]

Article 5(3) e-Privacy Directive sets a general rule and two exemptions to it:

As a general 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. Subscribers or users must be provided with clear and comprehensive information about the processing. Rules on consent and information requirements are those of the GDPR.

The storing of information or the gaining of access to information that is already stored in the terminal equipment is exempted from the requirement of informed consent, if it satisfies one of the following criteria: (i) the storage of information or the gaining access to information already stored is performed for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the storage of information or the gaining access to information already stored is strictly necessary in order for the provider of an information society service[86] explicitly requested by the subscriber or user to provide the service.

For the purposes of this Study, the EDPB has stated that when connected vehicles (and devices connected to them) meet the criteria of the definition of terminal equipment, they must be considered as such and provisions of Article 5(3) e-Privacy Directive must apply where relevant.[87]

GDPR and e-Privacy interplay – the debate around further processing

If information stored or gained accessed to constitutes personal data, Article 5(3) e-Privacy Directive shall take precedence over Article 6 GDPR[88] with regards to the activity of *storing or*

[84] See Article 1(a) Directive 2008/63/CE of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance), OJ L 162, 21.6.2008, pp. 20–26.
[85] A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions. Other tracking technologies can refer to local shared objects, pixel tags, web beacons, device fingerprinting, etc.
[86] An information society service is defined in Article (1)(b) of Directive (EU) 2015/1535 as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.
[87] EDPB Guidelines 01/2020 on connected vehicles, p. 7.
[88] Article 6 GDPR lists the cases in which the processing of personal data is lawful (see page 27 of this Report for further information), most notably: (i) the data subject gives **consent**; (ii) processing is necessary for the **performance of a contract**; (iii) the processing is necessary to comply with a **legal obligation**; (iv) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party.

gaining access to this information, as confirmed by the EDPB.[89] Processing operations of personal data subsequent to *storing or gaining access to this information*, must *additionally* have a legal basis under Article 6 GDPR in order to be lawful.[90]

For instance, an OEM retrieves location data from a connected vehicle in order to identify nearby affiliated petrol stations and offer discounts on petrol to the driver. For this purpose, when the data is collected through a publicly available electronic communication service (for instance, the vehicle's SIM card) Article 5(3) e-Privacy Directive would apply and the OEM will have to request consent for (i) the accessing information stored in the user's device, pursuant to Article 5(3) e-Privacy Directive; and (ii) to process this information to know the user's location so as to offer discounts based in nearby affiliated petrol stations, pursuant to Article 6 GDPR.

In other cases, consent might not be necessary if the storing or gaining access is exempted under Article 5(3) e-Privacy Directive and an additional legal basis different than consent is adequate pursuant to Article 6 GDPR. This could be the case where the storing of information is strictly necessary to provide a service explicitly requested by the end-user and the subsequent processing operations are necessary for the performance of a contract with an information society service. This would the case, for instance, of a company that puts in contact owners of parking spaces with interested drivers through its platform and which entails the transmission of the vehicle's location to the company to receive messages or alerts relating to the possible available parking spots.[91] In this example,[92] consent pursuant to Article 5(3) e-Privacy Directive would be exempted to the extent that the accessing to information stored in the user's terminal equipment – location data – is necessary for the provision of an information society service explicitly requested by the user.[93] Likewise, to the extent that the data processed qualify as personal data, in this case, by means of linking location data with the identity of a client, the GDPR also applies. Nonetheless, consent pursuant to the GDPR would not be required as the processing is necessary for the performance of a contract in which the driver/data subject is part, pursuant to Article 6(1)(b) GDPR.

In practical terms, when both the GDPR and the e-Privacy Directive apply, there are several obligations that data controllers/service providers must comply with at this point which overlap with each other: (i) to inform about the purposes of the processing; (ii) to obtain informed consent for the purpose of storing information or accessing information stored, when appropriate pursuant to Article 5(3) e-Privacy Directive; and (iii) to have an adequate legal basis for subsequent processing activities under Article 6 GDPR. In these cases, the data controller/service provider shall inform data subjects/end-users of all the purposes of the processing, i.e. the storing and/or access and any subsequent processing. When consent is

[89] 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,12.3.2019, p. 14; and EDPB Guidelines 01/2020 on connected vehicles.

[90] *Ibidem*.

[91] See use case "Renting and booking a parking space" in the EDPB Guidelines 01/2020 on connected vehicles cars, p. 29.

[92] Assuming that the e-Privacy Directive apply because: (i) the data is collected through a publicly available service; and (ii) the connected vehicle qualifies as terminal equipment.

[93] Note that the exemption operates on the basis that the service provider is an "information society service". A service provider not qualifying as such, for instance, a company offering roadside assistance in the event of a breakdown and processing location data to receive alerts about possible problems, would not qualify as such and would therefore need to obtain consent pursuant to Article 5(3) e-Privacy Directive. See, for instance, the "usage-based insurance" use case in the EDPB Guidelines 01/2020 on connected vehicles cars, p. 27.

necessary both under Article 5(3) e-Privacy Directive and Article 6 GDPR, consent for each purpose involved can be collected at the same time, although the consent for each purpose shall not be bundled with each other to ensure the consent is specific and, therefore, valid.

The EDPB invites to read the relationship between Article 5(3) e-Privacy Directive and Article 6 GDPR in the wider context of GDPR's principle of fairness. Whether the e-Privacy rules provide for consent as the appropriate base for processing, "when assessing compliance with Article 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".[94] The EDPB understands that consent in these cases will likely constitute the legal basis both for (i) the storing and gaining of access to information already stored and (ii) the processing of personal data following the aforementioned processing operations. The EDPB concludes that Article 6 GDPR "cannot be relied upon by controllers in order to lower the additional protection provided by Article 5(3) e-Privacy Directive".[95] In practice, this interpretation means that, in most cases where consent is necessary pursuant to Article 5(3) e-Privacy Directive, data controllers cannot rely on one of the lawful bases in Article 6 GDPR other than consent for subsequent processing operations involving the information gained accessing the end-user's device.[96]

It is worth noting that the EDPB has confirmed that service providers other than information society services that have collected personal data via Article 5(3) e-Privacy Directive, can rely on the performance of a contract as a legal basis as per Article 6(1)(b) GDPR for subsequent processing operations to the storing or accessing the data if certain conditions are met. These are: (i) the processing needs to take place in the context of a valid contract between the service provider and the data subject; and (ii) the processing shall be *objectively* necessary for the performance of the contract, i.e., without the processing the contract could not be performed. In this case the EDPB understands that the level of additional protection provided by Article 5(3) e-Privacy Directive would not be lowered by Article 6(1)(b) GDPR, therefore allowing its use.[97] For instance, this would be the case in the context of the provision of usage-based insurance services to car drivers, whereby the insurance company needs to track the driver's mileage and habits to reward "good" drivers with lower premiums.

The EDPB has also clarified some cases in which it understands consent for subsequent processing operations is necessary in all or a majority of cases. For instance, where personal data obtained via the storing or accessing of information from the terminal equipment is used for purposes such as analysing or predicting personal preferences, behaviour and attitudes of individuals, with this subsequently informing measures or decisions taken about them, consent is likely to be required otherwise this further use cannot be considered compatible.[98] Likewise, consent would be required for data processing like, for instance, tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based

[94] Guidelines 01/2020 on connected car, p. 7.
[95] *Ibid.,* p. 8.
[96] This interpretation is followed by other data protection authorities. See for example the ICO guidelines on "How do the cookie rules relate to the GDPR?" available at: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/#GDPR3.
[97] Guidelines 01/2020 on connected car, p. 27.
[98] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2013, p. 46.

advertising or tracking-based digital market research due to the nature of the processing operations and the risks posed to individuals.[99]

This interpretation is not necessarily shared by industry players, especially in the digital advertising ecosystem.[100] Contrary, they argue that there is a clear separation between processing activities, one being the (i) storing information or accessing information stored on the end-user's device, and the other (ii) the purposes for which the data accessed will be used. For instance, the use of the information obtained via cookies about an individual's preferred films could be used to build a profile and send personalized marketing communications of films matching that profile. The EDPB's criteria understands that consent is necessary not only for the accessing to the information of the cookie, but also for building the profile and send personalized communications based on that profile. The reasons are that an activity such as profiling and sending commercial communications in this context can be intrusive and easily unknown to the user. By contrast, the digital media industry and adtech ecosystem is relying systematically on legitimate interest as a legal basis for processing personal data obtained from the use of cookies and other tracking technologies for purposes such as profiling or personalized marketing, even in programmatic advertising environments,[101] where the data will likely be shared with numerous actors.[102]

Despite the above is the general rule, based on the considerations made by the EDPB in their guidelines on purpose limitation, in some cases it could be possible to use data collected via consent or through an exemption of Article 5(3) e-Privacy Directive for further compatible processing activities, specifically mentioning that, "in some cases, and subject to transparency and additional safeguards, tracking and profiling may also be permissible to prevent fraudulent use of the services offered".[103]

In the context of connected vehicles, following the example offered above, an insurance company providing pay-as-you drive insurance services, might be able, after conducting the assessment prescribed in Article 6(4) GDPR for further processing, use personal data collected in the context of the provision of the usage-based insurance service for the detection of fraudulent activity by the users.

---

[99] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014, p. 18.

[100] Proof of this can be seen in that a majority of the consent management platforms used to obtain consent from cookies are currently obtaining information through legitimate interest.

[101] According to IAB UK, programmatic advertising refers to the buying and selling of online ad inventory through automated methods rather than human actions.

[102] At the date of publication of this Report, main consent management platforms (CMP) for web, app and other environments offer publishers the option to process data collected through cookies and other tracking technologies on the basis of legitimate interest in the context of IAB's Europe Transparency and Consent Framework 2.0. Leading media organizations are currently taking advantage of this option (see, for instance, in Spain, www.elmundo.es or www.abc.es, or in the UK, www.theguardian.com, www.bbc.com, or www.dailypost.co.uk). Despite its wide adoption, the use of legitimate interest as a basis for processing data collected from cookies and other tracking technologies for advertising-related purposes has been questioned by regulators (for instance, the 29WP in its Guidelines on consent, profiling or legitimate interest, or the ICO in its general guidelines on legitimate interest and the report into adtech and RTB) and by literature, see for instance Matte, Célestin & Santos, Cristiana & Bielova, Nataliia, *Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?*, 2020; or Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P. Markatos, *User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users*, 2021.

[103] Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation*, p. 46.

This debate is relevant to the connected vehicle because Article 5(3) e-Privacy Directive is fully applicable to this context. As a result, OEMs and service providers relying on data stored in the vehicle need to assess what is the appropriate legal basis for subsequent processing operations and, if appropriate, obtain the necessary consent. As explained, the decision can only be based on the specific circumstances of each case, on account of the nature of the processing and the risks posed for the data subject/end-user.

Finally, even where criteria for the exceptions of Article 5(3) e-Privacy Directive are met, the processing of personal data, including personal data obtained by accessing information in the terminal equipment, shall be based on one of the legal bases as provided by the GDPR.

C. What regulators say?

EDPB - Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications

These guidelines laid the groundwork for privacy in the context of connected cars. In essence, the Guidelines are structured in three main sections: (1) presentation of the subject matter and scope of application, including an explanation of the applicable regulations, the aspects and definitions to be considered and the basic principles of data protection that must also be taken into account in the context of processing ; (2) recommendations that may be taken into account as a result of the collection and subsequent processing of personal data; and (3) illustrative case studies.

The Guidelines focus on the processing of personal data in the context of connected vehicles by different vehicle users, including, but not only, drivers, passengers and vehicle owners. It also brings mobility apps related to driving under scope, even if there are not integrated within the vehicle.

Throughout the Guidelines, the EDPB explores the definition of personal data in the context of connected vehicles, arriving at the conclusions explained in subsection I.A (“General Data Protection Regulation”).

As regards the lawful basis to process personal data, the EDPB recalls that the e-Privacy Directive must be taken into account along with the GDPR. Article 5(3) e-Privacy Directive applies to the storage or access to the information in the connected vehicle. For further analysis on Article 5(3) and the interplay with the GDPR, please consult subsection I.B (“e-Privacy Directive”).

The EDPB identifies the following main risks in relation to personal data processing in the context of connected vehicles:

Lack of control and information asymmetry between the different subjects concerned

There is a risk that the drivers and passengers of the vehicle are not adequately informed about the processing of personal data, for instance, the information could be provided only to the vehicle’s owner, who may not be the driver, and could not be provided in a timely manner by not taking into account that a vehicle may belong to different owners over time, or might be a shared or rented vehicle.

In all these cases it may happen that the person from whom the data is collected does not have access to information about the processing at hand and cannot object or exercise their rights. In

addition, communication in the vehicle can be activated without the individual being aware, a risk that must be avoided.

Quality of user consent

Under certain circumstances, it can be difficult to obtain the consent of drivers or passengers. This is the case, for instance, in regard to vehicle users who are not the owner of the vehicle or in cases of used cars, rental cars or car sharing.

Use of data for any further processing

The consent provided for a specific purpose, and so explained to the data subject, will never legitimize subsequent processing activities. The validity of consent demands consent is free, specific and informed. This would not be the case for instance, if data initially collected for maintenance is used by insurance companies to enrich the profile of drivers, or by traffic authorities to monitor compliance with traffic regulations, such as speed limits.

Excessive collection of personal data

The increase in the number of sensors used in connected vehicles increases the risk of excessive data collection, beyond what is strictly necessary to comply with the specific processing.

Data security and confidentiality

The diversity of functionalities, services and interfaces offered by connected vehicles increase the exposure to attacks and therefore the potential vulnerabilities through which personal data can be compromised. Connected vehicles are critical systems where a security breach can endanger the lives of its users and the people around them.

On account of their higher risks to data subject's personal life, special attention should be paid to location data, biometric data and data related to fines and traffic-related offenses and provides some specific aspects that must be supervised in this respect, including the implementation of data protection by default, to ensure the processing is set in the most privacy-friendly way from the outset.

The EDPB provides several recommendations to mitigate these risks, including:

- Information regarding the main aspects of the processing must be provided in a clear, simple and easily accessible way. In case the information was not collected directly from a vehicle user, he or she needs to be informed as soon as possible, for example, when the data is collected by the OEM and the latter provides the data to offer roadside assistance services.
- Data controllers must ensure that its purposes are specific, explicit and legitimate.
- Given the potential sensitivity of vehicle's usage data (journeys made, driving style, etc.), the EDPB recommends obtaining consent from the data subject before transferring the data to third parties. Special attention should be paid to data transferred to countries outside the EU.
- With regard to data subjects' rights, the EDPB understands that specific and easy mechanisms must be provided to allow data subjects to effectively exercise the data protection rights in the GDPR. The EDPB recommends that a profile management system is

implemented in the vehicle to save the preferences of each vehicle user to allow them to provide individual consents and information. In cases where the connected vehicle changes ownership, a procedure to erase any personal data of the previous owner could be provided.

- The solutions must be designed to comply with the principle of minimization and limit the data needed for processing to what is strictly necessary, provide data protection mechanisms by default and ensure that data subjects are well informed and can change the settings associated with their personal data.
- The EDPB recommends carrying out DPIAs, even in cases where these are not strictly required by the GDPR.
- Anonymization and pseudonymisation of data should be put in practice to the extent possible, thus minimizing the risks of identification when directly identifying data is not necessary.
- Another interesting recommendation strives on carrying out the processing of this data locally – not leaving the vehicle's internal system-, whenever possible, so that the user has direct control over the processing carried out.

In order to illustrate the previous recommendations, the EDPB presents different interesting case studies, some of which were mentioned above in subsection I.B ("e-Privacy Directive"). In particular, the use cases studied are: (i) provision of a service by a third party, including, insurance "pay as you drive" and rental and reservation of parking spaces; (ii) emergency call ("**eCall**"); (iii) accidentology studies; and (iv) auto theft.

In each of the cases, the EDPB analyses the applicable legal basis, the data collected, the retention period, the information and rights of data subjects, the data sharing and security aspects and provides *ad-hoc* recommendations for each of them.

EDPS – TechDispatch on Connected Cars

The EDPS released this report with the aim of explaining what connected cars are and the privacy and data protection risks associated with the processing of personal data in relation to them.

The EDPS describes the connected vehicle as a "computer on wheels" and highlights both the multiple applications connected vehicles have as well as the risks they pose. The connected vehicle encompasses a variety of technologies, including built-in (provided by the vehicle's internal system) or brought-in (connected through external devices) sensors which can measure data concerning driving behaviour (e.g. accelerometer, cameras, microphones, global navigation satellite systems).

The growth of vehicle network capabilities[104] as well as connectivity technologies is fostering the processing of increasing amounts of data outside the vehicle in detriment of local, in-vehicle, processing.

[104] The options to connect are multiple and still growing: from vehicle-to-manufacturer, to vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-any other entity (V2X). This is also illustrated by connected vehicles increasingly becoming a part of the cooperative intelligent transport systems (C-ITS), which allow the communication between car users and traffic managers.

The EDPS highlights the following data protection issues as the most relevant:

Lack of transparency

The complex processing operations involved in the context of connected vehicles (e.g. different technologies, including new technologies), the variety and large amount of data collected (e.g. driving habits, emergency related data, infotainment, vehicle-related data) and the different actors that can be involved (OEMs, insurers, law enforcement authorities and any other ISP), providing concise, transparent, intelligible and easily accessible information can be very challenging.

Excessive data collection

The development of new technologies for the collection and processing of data and its increasing application on the connected vehicle context increases the risk of excessive data collection and calls for the reinforcement of the principle of data protection by design and by default and especially, that of data minimisation.

Data retention

The risk of personal data storage beyond the minimum necessary for the explicit purposes for which the data was collected for, is highly increased by the complex ecosystem of actors involved of connected vehicles.

The EDPS recommends the adoption of retention policies to prevent indefinite storage and the risks linked to it, such as unauthorised disclosure or reuse.

Lack of control

In a context such as the described, there are numerous risks of data subjects not being fully aware of the processing activities happening via their vehicles. This creates a scenario where controlling one's data might be of extreme difficulty.

The EDPS recommends that connected vehicles should offer specific controls enabling the update and deletion of the data as well as means to withdraw consent easily, where appropriate.

Lack of purpose limitation

Provided the very diverse data that might be collected from a vehicle and the multiple actors with interests in it, it is easy that data is collected from purposes other than those for which the data was collected for, without an appropriate legal basis. The EDPS notes that privacy policies governing the processing of personal data in the context of connected vehicles sometimes bundle purposes even when they might be non-compatible with each other, e.g. providing requested services, credit and behaviour scoring and operating and expanding business activities.

Collection or inference of sensitive information

Data collected may reveal sensitive information of vehicle users. For instance, analysing location data can reveal, based on the locations visited by the vehicle, users' hobbies, home address, their cult, sexual orientation, etc.

Data controllers need to pay attention to the nature of the data in regard to how sensitive it can be for data subjects and allocate special resources and reinforce the protection in place.

Security and access control

The EDPS reminds that maintaining the security of information systems in connected vehicles is essential because the dangers associated with vehicles go beyond the individuals and affect other drivers, passengers and pedestrians. Increased connectivity and available touchpoints create new opportunities for cyber-attacks, which are more probable the more connected vehicles there are. The connected vehicle interconnects with other vehicles and systems, so any attack may have even more serious consequences if it is not fully ready to deal with it.

CNIL - Compliance package for connected vehicles

The CNIL released a compliance package for connected vehicles[105] compelling stakeholders to adopt a privacy by design approach. In practice, it implies privacy settings that can be easily modified, so as to empower users and give them control over their data.

In these guidelines, the CNIL describes three possible architectures for data processing in the context of connected vehicles, entailing different data flows:

- "In–In" data flow: the data collected is not transmitted outside the vehicle, remaining under the sole control of the user. To give an example, eco-driving solution displaying real-time advice to the driver or preventive maintenance alerting the driver to the condition of his vehicle.
- "In–Out" data flow: the data collected in the vehicle is transmitted externally to provide a service to the data subject. For instance, "Pay as you drive" insurance contract, anti-theft device allowing the location of the vehicle or automatic eCall.
- "In–Out–In" data flow: the data collected in the vehicle is transmitted to the outside world to trigger an automatic action in the vehicle. By way of illustration, dynamic traffic navigation system, remote modification of the charging capacities of the battery of an electric vehicle or reception of over-the-air technical updates.[106]

On the basis of these scenarios, the CNIL provides a theoretical framework to analyse data processing in the context of connected vehicles, based on the theoretical risks that each scenario raise, from the "In-In" scenario of minimum risk to the "In-Out-In" scenario, of maximum. The guidelines provide an analysis of different use cases or purposes in each scenario and provides recommendations for each use case.

"In-In" scenario analysis

In the "In-In" scenario we can find the following non-exhaustive use cases or purposes: (i) improving the driving experience and onboard life ("infotainment"); (ii) improving driving from a road safety perspective and preventive maintenance; (iii) automated driving assistance; (iv) and unlocking, starting, and activating certain vehicle commands using the driver's biometric data.

[105] CNIL, *Compliance package for a responsible use of data in connected cars*, 2017.
[106] Félicien Vallet, *The GDPR and Its Application in Connected Vehicles—Compliance and Good Practices*, 2019, p. 252.

The CNIL notes that in this scenario users have full control over their data and the CNIL recommends relevant stakeholders to recur to the "In-In" scenario to the extent possible in order to guarantee data privacy at a maximum and keep users in control of their data, whereby user control shall mean:

- That personal data is not transmitted to the service provider.
- The deactivation by default of the local storage of data relating to geolocation of the vehicle and relating to offences, except for real-time data-processing.
- The possibility to deactivate the functionalities at any time, except for functionalities that are strictly needed for the vehicle to function.
- In the absence of real-time processing, the option to easily access and delete usage-data (e.g., using a button inside the vehicle or using one's smartphone or using the onboard computer).
- Informing users regarding data that are likely to be stored locally, as well as the data-deletion options.

"In-Out" scenario analysis

In the "In-Out" scenario we can find the following non-exhaustive use cases or purposes: (i) model optimisation and product improvement; (ii) accidentology studies; (iii) commercial use of the vehicle's data; (iv) eCall; and (v) fighting theft.

In this scenario, where the risks to privacy and data protection are dramatically augmented by the fact that data leaves the vehicle, the CNIL places special emphasis on geolocation processing activities, as they are very common in this scenario and particularly sensitive for vehicle users. In this regard, the CNIL provides the following recommendations when collecting geolocation data for purposes other than for compliance with legal obligations:

- "Obtaining specific consent that is distinct from the general conditions of sale or use, e.g., on the onboard computer;
- adequate configuration of the detail of geolocation 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);
- the option to deactivate geolocation at any time;
- 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);
- providing accurate information on the purpose of processing (e.g., is geolocation history stored? If so, what is its purpose?);
- defining a limited storage period."[107]

[107] CNIL, *Compliance package for a responsible use of data in connected cars*, p. 25.

"In-Out-In" scenario analysis

In the "In-Out-In" scenario we can find the following non-exhaustive use cases or purposes: (i) remote maintenance; and (ii) improving the driving experience.

Based on the higher risks entailed in this scenario, the CNIL proposes reinforced measures to ensure data subjects stay in control of their data, placing special emphasis on providing adequate information, strong security measures, such as encryption and authentication people and devices involved in the processing, conducting DPIAs and the development of products and services which incorporate, form the outset, privacy and personal data protection considerations.

D. Other relevant regulations

For the purposes of this Study, it is worth mentioning other regulations in the mobility sector with provisions with relevance to the processing of personal data in the context of connected vehicles.

> *Regulation (EU) 2015/758 of the European Parliament and of the Council 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*

This regulation establishes the general requirements for the EC type-approval of vehicles in respect of the 112-based eCall in-vehicle systems, its components and separate technical units. eCall means an in-vehicle emergency call to 112, made either automatically by the activation of in-vehicle sensors or manually, which carries a minimum set of data and establishes an audio channel between the vehicle and the eCall public safety answering point via public mobile wireless communications networks.

Article 6 of this regulation regulates the conditions under which the processing of personal data in the context of the eCall system shall take place. This provision starts by limiting the purpose of the processing to the handling of emergency situations and also refers to the storing of data, which shall not be retained longer than necessary for the purpose of handling the emergency situations and shall be fully deleted as soon as it is no longer necessary for that purpose.

Article 6 also establishes several obligations to be complied with by OEMs, in particular:

- Purpose and storage limitation: the personal data processed shall only be used for the purpose of handling the emergency situation and retained no longer than necessary for this purpose.
- Non traceability: OEMs shall ensure that the 112-based eCall in-vehicle system is not traceable and is not subject to any constant tracking.
- Data minimization: OEMs shall ensure that in the internal memory of the 112-based eCall in-vehicle system data is automatically and continuously removed and that only the last three locations of the vehicle shall be stored to the extent that they are necessary to specify the location and direction of travel at the time of the event and that the data sent in the

case of an event is the minimum information possible, as referred to the applicable standard.[108]

- Unavailability: the data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
- Transparency: OEMs shall provide clear and comprehensive information in the owner's manual about the processing of data carried out through the 112-based eCall in-vehicle system.
- Data isolation: OEMs shall ensure that there is not an exchange of information between the eCall in-vehicle system and any additional systems in the vehicle, for instance, those providing added-value services.

Type approval regulations, delegated acts and Commission regulations regulating access to vehicle on-board diagnostics information and repair and maintenance information[109]

The type approval framework provides common technical requirements for the type approval of motor vehicles and replacement parts.

As part of the requirements that this framework has imposed on OEMs, several are addressed at providing access to vehicle repair and maintenance information ("**RMI**") to ISPs so as to provide easy, restriction-free, and standardised access to information on the repair and maintenance of vehicles and prevent discrimination with respect to authorised dealers and repair workshops as well as access to vehicle on-board diagnostics information ("**OBD**").

Regulation (EU) 2018/858, which regulates access to OBD and RMI information, in its Recital 62 call OEMs for complying with the GDPR and "implement all measures necessary to comply with the rules on processing and transmission of personal data that are generated while the vehicle is used".

It is worth mentioning that the provisions concerning the access to vehicle information are currently under review by the European Commission in order to evaluate whether to widening the scope of the obligation of access to vehicle's information to new players, including car sharing, mobility as a service and insurance.[110]

Also worth mentioning is the Scheme for accreditation, approval and authorization to access security-related RMI which is the basis for independent operators requiring access to security-related vehicle RMI and services.[111]

---

[108] EN 15722:2011 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)'.

[109] Most notably: Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJ L 171, 29.6.2007, pp. 1–16; and its implementing acts; and Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, PE/73/2017/REV/1,OJ L 151, 14.6.2018, p. 1–218; and its implementing acts.

[110] See In-vehicle generated data – EU rules for services based on access to car data (europa.eu).

[111] SERMI operations group, Scheme for accreditation, approval and authorization to Access Security-related Repair and Maintenance Information (RMI), 2016. Available at: https://circabc.europa.eu/sd/a/55ec9ba6-ca74-4439-864a-b5104704f828/SERMI_EA-validated_2016_05_19.pdf. Last accessed: 30/11/2021.

In parallel, cybersecurity aspects take into account UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.

> *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*[112]

This Directive establishes a framework in support of the coordinated and coherent deployment and use of Intelligent Transport Systems ("**ITS**") within the EU, in particular, across the borders between the Member States, and sets out the general conditions necessary for that purpose.

The deployment and use of ITS applications and services entail the processing of personal data, reason why the directive mandates that all personal data processing is carried out in accordance with the EU Privacy Regulatory Framework.

In particular, Article 10 establishes the rules on privacy, security and re-use of information, prompting Member States to comply with the EU Privacy Regulatory Framework. This provision regulates general programmatic guidelines for Member States to ensure that specific aspects are taken into account when regulating, mainly, protection against the misuse of information, the limitation of the processing to the necessary for the performance of the ITS applications and services and appropriate dealing with special categories of personal data, when included.

> *Regulation (EU) 2019/2144 on type approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road user*[113]

This Regulation requires OEMs to equip vehicles with a series of advanced vehicle systems: (i) intelligent speed assistance; (ii) alcohol interlock installation facilitation; (iii) driver drowsiness and attention warning; (iv) advanced driver distraction warning; (v) emergency stop signal; (vi) reversing detection; and (vii) event data recorder.[114]

Recital 14 clarifies that any processing of personal data, such as information about the driver processed in event data recorders or information about the driver's drowsiness and attention or the driver's distraction, should be carried out in accordance with Union data protection law.

---

[112] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance, OJ L 207, 6.8.2010, pp. 1–13.

[113] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, PE/82/2019/REV/1, OJ L 325, 16.12.2019, p. 1–40.

[114] Event data recorders are devices capable of recording and storing critical crash-related parameters and information shortly before, during and immediately after a collision and make this data available to national authorities for research and analysis.

Article 6 put in place several safeguards with relevance in the context of personal data protection, starting by mandating that they shall operate in closed-loop systems. Article 6(3) determines that the driver drowsiness and attention warning or advanced driver distraction warning should not continuously record nor retain any data other than what is necessary in relation to the purposes for which they were collected or otherwise processed within the closed-loop system. Furthermore, those data shall not be accessible or made available to third parties at any time and shall be immediately deleted after processing.

Article 6(4) provides that event data recorders shall operate in a way that should not allow the vehicle or holder to be identified and they shall be able to make the data recorded available to national authorities through a standardised interface for the purpose of accident research and analysis, in compliance with the GDPR.[115]

> *Regulation (EU) 2019/631 of the European Parliament and of the Council of 17 April 2019 setting CO2 emission performance standards for new passenger cars and for new light commercial vehicles*[116]

This Regulation lays down obligations for OEMs to control the emissions of their vehicles. For this purpose, OEMs shall regularly made available, either by transfer or through direct transfer from vehicles, information about their vehicles' fuel or energy consumption. Along with the information about consumption and other parameters, OEMs are mandated to share the vehicle identification number with the Commission, as per Article 12(2). The European Commission shall process this data to create anonymised and aggregated datasets.

Linking the information with the vehicle identification number can make this personal, especially if shared with a public authority. This is why the same Article mandates that the Commission shall use the vehicle identification numbers only for the purpose of that data processing and shall not be retained longer than needed for that purpose.

[115] Event data recorders are devices capable of recording and storing critical crash-related parameters and information shortly before, during and immediately after a collision and make this data available to national authorities for research and analysis.

[116] Regulation (EU) 2019/631 of the European Parliament and of the Council of 17 April 2019 setting CO2 emission performance standards for new passenger cars and for new light commercial vehicles, and repealing Regulations (EC) No 443/2009 and (EU) No 510/2011, (OJ L 111 25.4.2019, p. 13).

II. Implications of the e-Privacy Regulation Proposal

A. Overview of the ePR Proposal

The ePR Proposal is meant to update the ePrivacy regulatory framework. Originally, this regulation was intended to be passed together with the GDPR, but EU Member States have not yet been able to agree on the draft legislation and negotiations of the ePR Proposal are still ongoing. Since the publication of the original version proposed by the European Commission on January 2017 ("**EC ePR Proposal**"),[117] shortly followed by the European Parliament's on 20 October 2017 ("**EP ePR Proposal**"),[118] the Council, after four years of internal negotiation and the publication of more than 30 different versions of the file, passing through 8 different presidencies, finally adopted a common position on February 10, 2021 ("**Council ePR Proposal**").[119] At the date of publication of this Report, the Council and the Parliament are negotiating the ePR Proposal at first reading under the ordinary legislative channel.

This regulation is meant to culminate the modernization of the EU Privacy Regulatory Framework in order to keep track with the fast-evolving pace of IT-based services.[120] The new regulation will replace the current e-Privacy Directive, introducing and updated framework on privacy and data protection in the electronic communications sector.

For this purpose, the ePR Proposal brings a number of changes to the table, starting by pivoting to a regulation, instead of a directive, in order to ensure limited local margin to implement the new rules, thus achieving a higher level of harmonization across Member States.

The ePR Proposal regulates the following main areas:

In the first place, Chapter II of the proposal regulates the protection of end-users' electronic communications data,[121] specifically regulating the confidentiality of two types of electronic communications data: "content data"[122] and "metadata".[123] It includes rules on storage and erasure of this data. It also regulates the integrity of end-users' terminal equipment under the framework described below. In total, this chapter sets a number of legal bases for the lawful processing of the different data in scope (i.e., electronic communications data – including its content and metadata – and data collected or emitted by terminal equipment) and establishes specific conditions for each category of data.

In the second place, Chapter III lays down specific obligations for number-based interpersonal communications services, which scope has been extended further than traditional telecoms operators to include over-the-top ("**OTT**") services. These obligations are related to the

[117] See https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52017PC0010.
[118] See https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html?redirect.
[119] See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=ENn.
[120] See https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.
[121] Pursuant to Article 4 ePR Proposal, "electronic communications data" means electronic communications content and electronic communications metadata.
[122] Pursuant to Article 4 ePR Proposal, "electronic communications content" means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound.
[123] Pursuant to Article 4 ePR Proposal, "electronic communications metadata" means data processed by means of electronic communications services for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication.

identification of the calling line, the prevention of unwanted calls and publicly available directories. Additionally, it establishes rules to prevent unsolicited direct marketing, unless the end-user has consented or when such communications happen in the context of a purchase of a product or a service.

On the other hand, Chapter IV allows EU Member States to designate one or more competent authorities for the enforcement of the abovementioned rules. Contrary to the EC ePR Proposal where the authorities in charge of enforcement would be those in charge of data protection rules at a national level, under the Council ePR Proposal, these authorities can include authorities different than data protection authorities, for instance National Regulatory Authorities ("**NRAs**") responsible for supervising compliance with and enforcement of telecoms regulation. In the Council ePR Proposal, the EDPB is entrusted to "contribute to" the ePR's consistent application (as opposed to "ensure" in the original EC ePR Proposal), establishing only a general duty to cooperate between the competent authorities not subject to the GDPR's consistency mechanism.[124]

Finally, Chapter V provides for remedies, liability and penalties, setting out administrative fines for infringements of specific provisions up to EURO 20M or 4% of total worldwide annual turnover. Fines can apply concurrently to GDPR penalties.

Some of the most relevant areas of change in contrast to the e-Privacy Directive are:

- Bringing some OTT services, such as voice over IP, instant messaging (e.g., WhatsApp, Telegram, Facebook Messenger, Skype), or web-based email services into the EU electronic communications regulatory framework to ensure they guarantee the same level of confidentiality of communications as traditional telecommunication operators.
- Putting an end to application gaps in regard to transfer of data and information between devices, applications or IoT systems (machine-to-machine or "**M2M**" communication), whose regulatory framework is unclear under the current e-Privacy provisions.[125]
- Prohibiting any interference, whether human or through the intervention of automated processing by machines, of electronic communications, including their content and associated metadata, unless the parties involved in the communication provide their consent or if other permitted circumstances apply. New consent requirements compared to the e-Privacy Directive are set out for the processing of content and metadata by service providers so as to allow them to offer new services, enhance their current services and innovate.
- Fostering the obtention of consent for online tracking through cookies and similar technologies via the use of browser settings as an easy way to accept or refuse tracking cookies and other identifiers The ePR Proposal also clarifies that no consent is needed for non-privacy intrusive cookies that improve internet experience, such as cookies to remember shopping-cart history or to count the number of website visitors.

[124] The Council's positioning has been contested by the EDPB; see: European Data Protection Board, statement 03/2021 on the ePrivacy Regulation, 9.3.2021,p. 4.

[125] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC; COMMISSION STAFF WORKING DOCUMENT, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC.

- Strengthening protection against spam by mandating marketing callers to display their phone number or use a special prefix that indicates a marketing call.
- Establishing stronger enforcement measures by making data protection authorities, already in charge of the rules under the GDPR, or telecommunication authorities responsible of overseeing enforcement of confidentiality rules.

ePR Proposal-GDPR interplay

The ePR Proposal has a similar interplay with the GDPR as the e-Privacy Directive. In that regards, the provisions of the ePR Proposal will take precedence over those of the GDPR. When no specific rule exists within the ePR Proposal for the processing of personal data, then the GDPR will apply to that processing.

Likewise, the provisions of the ePR set forth rules regarding the protection of the rights of both natural persons and legal persons, in contrast to the GDPR which is limited to natural persons.

Finally, the ePR Proposal includes a level of sanctions consistent with the GDPR, establishing fines of up to EUR 20 000 000 or 4% of the total annual turnover.

Relevant rules in the context of car connectivity

With regard to M2M, initial versions of the ePR Proposal could have led to the interpretation that entities manufacturing IoT devices (including OEMs) would have qualified as electronic communication service providers. Indeed, the EC ePR Proposal included language that suggested that all transmission of data from one machine to another would have been considered as the provision of an electronic communications service and, therefore, IoT manufacturers would in fact be providing electronic communications services and, therefore, subject to the application of the ePR Proposal. The Council ePR Proposal later clarified this interpretation was not correct by amending Recital 12 the current wording of which now distinguishes between: (i) the application-layer of M2M communication; (ii) and the underlying transmission-layer for the conveyance of signals via an electronic communications network. Only the latter layer would constitute an electronic communications service.

Similar to what happens with the e-Privacy Directive, for the purposes of this Study the most relevant rules are those related to the protection of the confidentiality of end-users' terminal equipment in regard to the information which can be collected or emitted by them. As a matter of fact, Recital 21 of the Council ePR Proposal specifically mentions automated and connected vehicles as an example of "terminal equipment". In this regard, the relevant provisions of the ePR Proposal for the purposes of this Study are Article 8 (*Protection of end-users' terminal equipment information*) and Recitals 20 to 25 (all related to the protection of end-users' terminal equipment information).

In addition, the ePR Proposal includes specific provisions on consent which might be applicable in the context of connected vehicles. While these provisions are contained in Article 10 of the EC ePR Proposal and EP ePR Proposal, they are regulated in Article 4 of Council ePR Proposal.

Finally, the development of new in-vehicle touchpoints with car users, such as direct communication through the vehicle's on-board screen or similar, will allow for the sending of direct marketing communications directly through the car, which would be subject to the

relevant rules on unsolicited communications. This Report, nevertheless, does not explore such rules as they are not scope and purpose of the Study.

B. Differences between versions

As a preliminary note, some relevant terms and expressions have been modified in the ePR Proposal in respect of the e-Privacy Directive:

- The concept of "user or subscriber" is modified by the all-encompassing term "end-user".
- The expression "the storing of information, or the gaining of access to information already stored in the terminal equipment" becomes "the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment". As in the previous case, the new wording responds to the intention of widening the scope of the provision, in this case by pivoting from the simple *storing* of information to the *use* of storing and processing capabilities of the device. Likewise, now the rules cover the collection of any information and not merely the accessing to information already stored in the device. With this change, the ePR Proposal moves away from the cookie use case, where data is stored in devices, and extends to any information collected from the device thus bringing IoT-related data processing under scope of the rules of confidentiality in relation to data processing in the context of end-user's terminal equipment.
- The ePR Proposal has separated rules pertaining to information "collected from" (Article 8(1)) and "emitted by" (Article 8(2)) the end-users' terminal equipment.
- The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment expressly extends to the terminal equipment's software and hardware.

As explained, the most relevant provisions for data processing in the context of connected vehicles are the following:

- Rules on consent, as regulated by Article 4 in the Council ePR Proposal and Article 10 in the EC ePR Proposal and the EP ePR Proposal.
- Rules on the protection of end-users' terminal equipment, as regulated in Article 8 and Recitals 20 to 25.

Depending on which version of the ePR Proposal we pay attention to – European Commission, European Parliament or Council of the EU – there are significantly different rules, especially with regard to the protection of end-users' terminal equipment. Therefore, this section of the Report focuses on understanding the differences between the different versions of the ePR Proposal. For a detailed comparison between the relevant provisions in the three versions, please refer to **Appendix I.**

Differences in relation to consent

The ePR Proposal regulates the possibility that consent is provided via the implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings. Where available and technically feasible, an end-user may therefore grant, through software settings, consent to a specific

provider for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider.

The main difference between the EU institutions texts in regard to consent is that both the European Commission and the Council included the obligation to renew the consent at periodic intervals of 6 and 12 months respectively. The European Parliament did not set any specific interval to renew consent.

In addition, the Council eRP Proposal provides for the possibility to demonstrate the obtention of consent through a technical protocol showing that consent was given from the terminal equipment of an end-user who the provider is not able to identify.

Differences in relation to the protection of end-users' terminal equipment

As commented, Article 8 regulates the protection of end-users' terminal equipment information. This Article is paramount to connected vehicles because connected vehicles can qualify as "terminal equipment" of the end-user if certain conditions are met. Whether this is the case, the processing of data, both *collected from* the connected vehicle and *emitted by* it, will be subject, first, to the rules of Article 8 ePR Proposal and, if the processing involves personal data, all the requirements laid down in the GDPR and explored in subsection I.A ("General Data Protection Regulation").

In the first place, contrary to the provisions of the e-Privacy Directive, which were limited to the protection against the storing of information or the accessing to information already stored in the end-users' terminal equipment, the versions of the ePR Proposal of the three EU institutions regulate two situations in which end-users' terminal equipment shall be protected: (i) in relation to data collected from the terminal equipment, regulated in Article 8(1); and (ii) in relation to data emitted by the terminal equipment, regulated in Article 8(2).

Article 8(1) regulates a general prohibition regarding the use of the processing and storage capabilities of a terminal equipment and the collection of information from end-users' terminal equipment, including its software and hardware, by parties different from the end-user unless one exemption applies. These exemptions are different in the different versions of the ePR Proposal.

While the European Commission regulates four total exemptions, the European Parliament and the Council regulate five and eight exemptions, respectively.

With minor changes amongst them, the versions of the three institutions regulate the following exemptions:[126]

- The processing is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network.
- The end-user has given his or her consent.
- The processing is necessary for providing an information society service requested by the end-user.

[126] See Article 8(1) letters (a), (b) and (c) in the versions of the three institutions.

- The processing is necessary for audience measuring.

In all cases, the most relevant differences strive in the fact that the European Parliament uses a wording which is aimed at ensuring the highest level of protection of end-users and includes specific safeguards with this purpose. The Council, on the other hand, tends to widen the scope laid down by the European Commission and uses a language that is less protective or consumer-focused.

In addition to the abovementioned, the European Parliament and the Council regulate that the processing shall also be permitted if necessary to ensure security of the end-users' terminal equipment or for software updates, if certain conditions are met.[127] The Council widens the scope of this provision by permitting also the processing necessary to ensure the security of an information society service and processing activities necessary to prevent fraud or detect technical faults.

The European Parliament provides for an exception not included by any other institution related to the employment context, when the processing is strictly necessary for the execution of an employee's task.

The Council regulates two additional exemptions: (i) when the processing is necessary to locate terminal equipment when an end-user makes an emergency communication to an emergency number; and (ii) when the processing is compatible with the purposes for which the information was collected, if certain conditions are met.

These two exemptions are of great relevancy for the connected vehicle ecosystem: the former because is specifically allowing the use of the eCall functionality without the need of the end-user's consent; and the latter because it sheds light about the rules applying to further processing for compatible purposes, which are today unclear, as explained in subsection I.B ("GDPR and e-Privacy interplay – the debate around further processing"). In order to be able to rely on this exemption, service providers/data controllers will have to firstly assess the compatibility of the new purpose through a compatibility test similar to the one regulated in Article 6(4) GDPR, and meet the following conditions: (i) the information is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, (ii) the processing is limited to information that is pseudonymised, and (iii) the information is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user. The information collected for compatible purposes cannot be shared with third parties unless a data processing agreement is in place, pursuant the conditions laid down in Article 28 GDPR.[128]

Article 8(2) regulates the collection of data emitted by end-users' terminal equipment. The use case refers to the data that is necessary to access, discover or maintain a connection with an electronic communication network, such as connecting to a 5G mobile network or a WiFi network in a shopping centre or airport. Among the data necessary for this purpose, unique identifiers of the terminal equipment are processed under the current standards of communication, such as MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI, the WiFi signal etc. This data is then used for the provision of services, such as providing data on the number of people waiting in line, ascertaining the number of people in a specific area (referred to as statistical counting). This information could be also used for more

[127] See Article 8(1)(da) EP ePR Proposal and Article 8(1), letters (da) and (e) Council ePR Proposal.
[128] See Article 8(1), letters (g), (h) and (i) Council ePR Proposal.

intrusive services such as to send commercial messages with personalized offers to end-users, for example, when they enter stores. While some of these functionalities do not entail high privacy risks, others certainly do; for example, those involving the tracking of individuals over time, including repeated visits to specified locations.[129]

As with Article 8(1), the Council version regulates more cases than the other institutions in which processing is allowed without consent.

As the Council ePR Proposal shows,[130] this Article can be relevant to the connected vehicle ecosystem to the extent that it applies also to the information emitted by a device to connect to another device.

Different competent authorities

The EC ePR Proposal allocates the responsibility over enforcement on the same supervisory authorities in charge of the enforcement of data protection rules. The European Parliament and the Council have not followed this line and have left open for EU Member States the decision about which supervisory authority shall be in charge.

In all cases, the EDPB is appointed as the pan-European supervisory authority, although the rules on cooperation and consistency laid down by the EC ePR Proposal are very different from the Council ePR Proposal, the latter being dissimilar to the GDPR.[131]

C. Implications for car connectivity and data sharing

The ePR Proposal introduces relevant modifications to the current framework, some of which will surely have effects on the connected and automated vehicle ecosystem and, more generally, on the IoT industry.

When looking at possible implications, the fact that rapidly evolving digital technologies such as M2M communications and IoT environments are included within scope makes it likely that some of the implications the ePR Proposal will have are to a great extent unknown or difficult to predict.

As a starting point, depending on which version of the ePR Proposal we pay attention to, the implications will likely be very different. In general terms, the EC ePR Proposal serves as a starting point or basic outline, lately enriched by the often-contrasting visions of the European Parliament and the Council of the EU. Accordingly, for the analysis of possible implications we will primarily focus on the implications which stem from these latter versions, analysing possible implications in relation to the both of them and keeping in mind that the final text will likely include parts of both.

Implication 1 – Increased flexibility to process data without consent, at a cost

By and large, in the context of vehicle connectivity, the ePR Proposal, in any of its versions, creates a more flexible landscape for OEMs and ISPs to use the connected vehicle's processing and storage capabilities or the collection of information from the vehicle without the end-user's consent. The versions of the three institutions provide for a continuum where the EC ePR

[129] For further reference please consult recital 25 of the ePR Proposal.
[130] See recital 25(a) of the Council ePR Proposal.
[131] EDPB statement ePR 2021.

Proposal sets the lower level of flexibility and the Council ePR Proposal the higher, as it counts with up to eight exemptions to consent.

The enhanced flexibility in what regards to legal bases other than consent is balanced out by an increased complexity of the regulatory framework. The different options available for organizations processing the data translate into higher compliance costs derived from the need to assess the types of information available and select the most appropriate legal base to process it among the different possible options. Moreover, where the data processed qualifies as personal data, the interplay with the GDPR creates an extra burden for actors involved in the processing.

This complexity will also derive in increasing difficulties in providing information that is easy to understand for consumers and complete at the same time. In cases where consent is not necessary, providing timely and appropriate information will be discouraged by the complexity of the processing operations and the inherent difficulties of informing in connected vehicle contexts.

In practice, actors collecting data from connected vehicles will have to provide larger amounts or more complex information from the outset in relation to the implications of data processing. With regard to connected vehicles, the EDPB recommends that when processing personal data is based on consent or a contract, information about data portability aspects must be clearly stated, including the difference between this right and the right to access personal data.[132]

Implication 2 – *Any* kind of service provider, not just information society services, will be able to process data collected in the context of the connected vehicle without consent, if requested by end-users

All the versions of the ePR Proposal allow service providers other than information society services to process data generated in the context of the connected vehicle without consent when requested by the end-user. Contrary to the e-Privacy Directive, it is not necessary that the service requested by the end-user qualifies as an information society service for the exemption to apply.

This opens the door for numerous services to be provided bypassing consent, which is beneficial for OEMs (e.g., access to data by official repairers, etc.) and, theoretically, for ISPs (e.g., independent repair and maintenance, road assistance, insurance, etc.).

Implication 3 – Rules on further/compatible processing allow for significant flexibility to ascertain situations in which consent is not necessary, in line with the GDPR, although these rules are more stringent than the GDPR

The Council ePR Proposal allows service providers to carry out the processing necessary to ascertain whether a processing for another purpose is compatible with the purpose for which the electronic communications data was initially collected.

These rules shed light about the rules applying to further processing for compatible purposes and align the ePR Proposal rules with the GDPR's risk-based approach and accountability principles. In spite of this, very strict rules apply for this processing, thus risking its future effectiveness. In order to be able to rely on this exemption, service providers will have to firstly

[132] EDPB, *Guidelines 01/2020 on connected cars*, 2020, p. 23.

assess the compatibility of the new purpose through a compatibility test similar to the one regulated in Article 6(4) GDPR, and meet the following conditions: (i) the information is erased or made anonymous as soon as it is no longer needed to fulfil the purpose; (ii) the processing is limited to information that is pseudonymised; and (ii) the information is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.

The information collected for compatible purposes cannot be shared with third parties unless a data processing agreement is in place, pursuant the conditions laid down in Article 28 GDPR.

Implication 4 – Still legal uncertainty around consent

It remains unclear how that consent could sufficiently be provided by end-users, especially where the end-user -of, for instance, a connected vehicle- changes. The Council ePR Proposal has sought to alleviate this question, at least partially, by allowing service providers to demonstrate the valid obtention of a consent by presenting the technical protocol showing that consent was given from the terminal equipment.

In a context of rapidly evolving technologies, such as in an IoT environment, the quality of consent is not easily achieved, especially if the end-user has little awareness about the implications of the data processing, e.g., in the context of the connected vehicles.

The abovementioned considerations could justify the need to periodically renew consent. The EC ePR Proposal and the Counsil ePR Proposal lay down the obligation to renew consent after 6 and 12 months, respectively. It is not clear whether this requisite will go through to the final text and, if so, which will be the required periodicity.

Implication 5 – Higher regulatory exposure

It is likely that organizations located in a Member State where the responsibility over enforcement is allocated on the same supervisory authority in charge of the enforcement of data protection rules, will assume higher regulatory exposure than the case in which authorities are different. This is so to the extent that combined investigations based on GDPR and ePR infringements will be more probable than in cases where the competences are distributed between the different authorities.

Additional exposure stems from the updating of the ePrivacy fines to GDPR standards.

Implication 6 – The Council ePR Proposal regulate that the processing necessary for eCall does not require consent

By contracts with the other versions, the Council ePR Proposal regulates that service providers shall not obtain consent when the processing is necessary to locate terminal equipment when an end-user makes an emergency communication to an emergency number.

3

Section III: Consumer Awareness

This section aims at assessing (i) consumer awareness, sensitivity and attitudes towards data sharing and processing in the context of vehicle connectivity; (ii) consumer awareness on data protection and privacy rights in this context and the difficulties consumers might face when exercising their data protection rights; and (iii) the level and transparency of information provided to consumers at the vehicle points of sales. In order to collect empirical data to assess these parameters, as part of this Study, two practical exercises have been conducted: the distribution and analysis of a survey across different EU regions, as well as several mystery shopping experiences at vehicles' point of sales. This section gives an overview of the methodologies followed for these exercises and provides the findings for each of them.

I. Awareness on connected vehicles and sensitivity regarding sharing vehicle data (survey)

A. Introduction and methodology overview

As a part of this Study, a survey has been conducted in several EU regions for the purpose of getting an understanding on consumer awareness, sensitivity and attitudes towards data sharing and processing in the context of vehicle connectivity, as well as awareness on data protection and privacy rights in this context.

In particular, the survey aimed at assessing: (i) which challenges consumer face when exercising their rights under the GDPR (e.g., data portability); (ii) what are the consumer sensitivity on sharing vehicle data; and (iii) what is the degree of consumer awareness with regard to vehicle data.

The survey has been conducted in 3 European regions, i.e.:

- **Southern** (with respondents in France, Italy and Spain).
- **Continental** (with respondents in Belgium, Germany, the Netherlands and Switzerland).
- **Northern** (with respondents in Denmark, Norway and the United Kingdom).

Participation was open to any kind of respondent profile and not only to drivers, on the believe that non-drivers can also provide valuable insights on awareness, sensitivity and attitudes towards data sharing and processing in the context of vehicle connectivity.

Please refer to **Appendix II** for further information about the methodology followed for this survey process.

B. Findings

A total of 4,889 answers have been recorded as a result of the survey process. Amongst these respondents, 1,980 declared to have a vehicle manufactured from 2018 onwards, which means that 40% of the total respondents own or regularly drive a vehicle which would likely qualify as a "connected vehicle" based on, at least, the minimum connectivity capabilities provided by the eCall regulation.

By region, the results are as follows:

- **Southern region** (France, Italy and Spain): out of 721 respondents, 303 declared to have a vehicle manufactured from 2018 onwards, i.e., a 42% of the total respondents.

- **Continental region** (Belgium, Germany, Netherlands and Switzerland): out of 1,292 respondents, 379 declared to have a vehicle manufactured from 2018 onwards, i.e., a 29% of the total respondents.
- **Northern region** (Denmark, Norway and UK): out of 2,876 respondents, 1,298 declared to have a vehicle manufactured from 2018 onwards, i.e., a 45% of the total respondents.

A summary of the main findings is explained below. Please refer to **Appendix II** for the detail of the results.

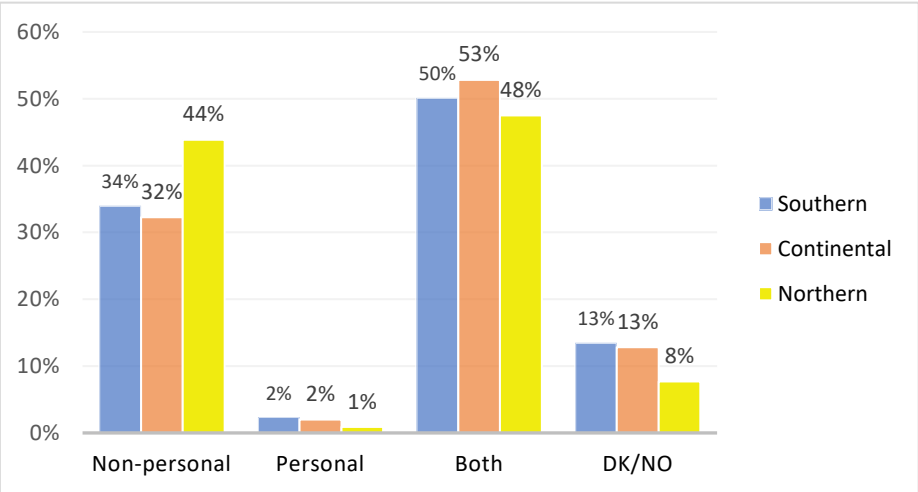
Awareness, perceptions and attitudes towards data processing in the context of connected vehicles

The results show that, across the jurisdictions included in the Study, there is certain degree of awareness about connectivity features of connected vehicles and the fact that vehicles can collect and share information. 77% of the respondents declared to know that vehicles are equipped with sensors and connectivity features (including its own SIM card and Internet connection) which allow them to connect with other cars, devices, infrastructure, services, etc. Similarly, 73% declared to know that connected vehicles (vehicles equipped with sensors and connectivity features) can collect information from the vehicle and share this information with different entities.

Among the respondents, the general perception is that the information collected and shared by connected vehicles is both personal and non-personal, with 50% of the responses answering in this line. 36% of the respondents have the perception that this information is solely non-personal, reaching up to 44% of the respondents in the Northern region. Only 2% think that the information is solely personal. Contrary to the criteria supported by data protection regulators as regards the nature of the data collected in the context of vehicle connectivity, as based on the legal definition of personal data, there is a general perception among respondents, especially in the Northern region of the EU, that the data collected and shared by connected vehicles is not personal in nature.

Respondents generally share the perception that data collected in the context of vehicle connectivity is shared with OEMs, with a 26% of the respondents supporting this option. 17% think the data is shared with repair and maintenance services, 13% with insurance companies and 13% with emergency services. In a lower level, 8% think that the data is shared with public authorities, 5% with entertainment services, 4% with parking providers and

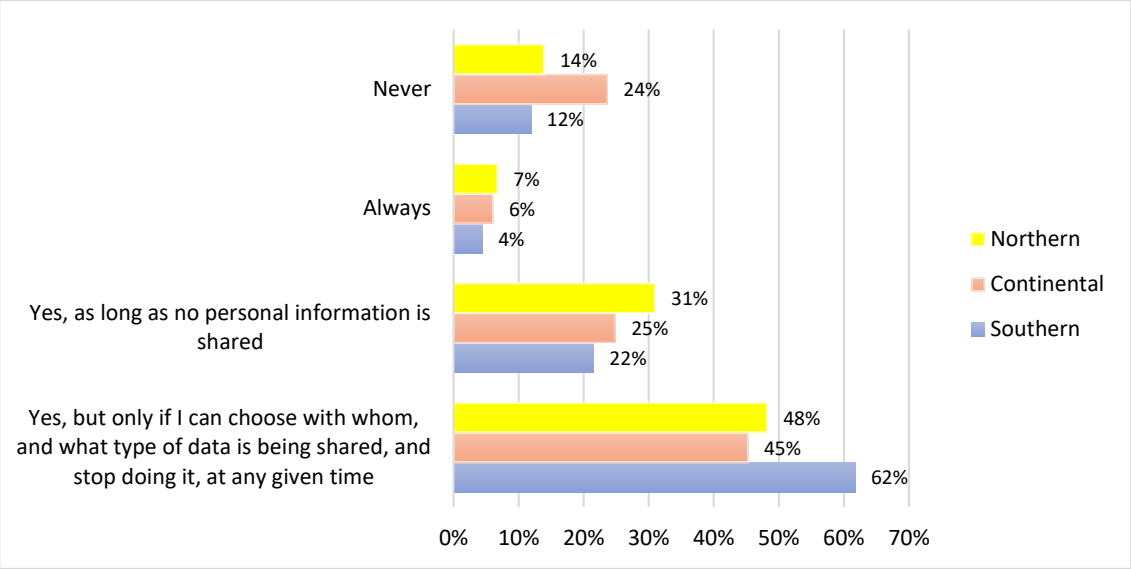
Q4: What type of information do you think is being collected and shared?



3% with gas stations.

51% of the respondents declared to feel comfortable sharing information from their vehicle with different entities but only to the extent that they could choose with whom, and what type of data to share, and stop doing it at any given time. 26% declared to be comfortable sharing information collected from the vehicle but only to the extent that no personal information is shared with the receiving entities. Only 6% declared to be comfortable sharing their data with different entities in all cases and up to 17% declared not to be comfortable sharing this data in any case. In comparison with the other regions, respondents in the Northern region showed especially uncomfortable with data sharing (up to 24% of the answers within this region), with German respondents taking the lead with up to 33% of the respondents supporting this option.

Q6: Would you be comfortable sharing information from your vehicle with these entities in exchange of services or functionalities that could benefit your driving experience or safety?



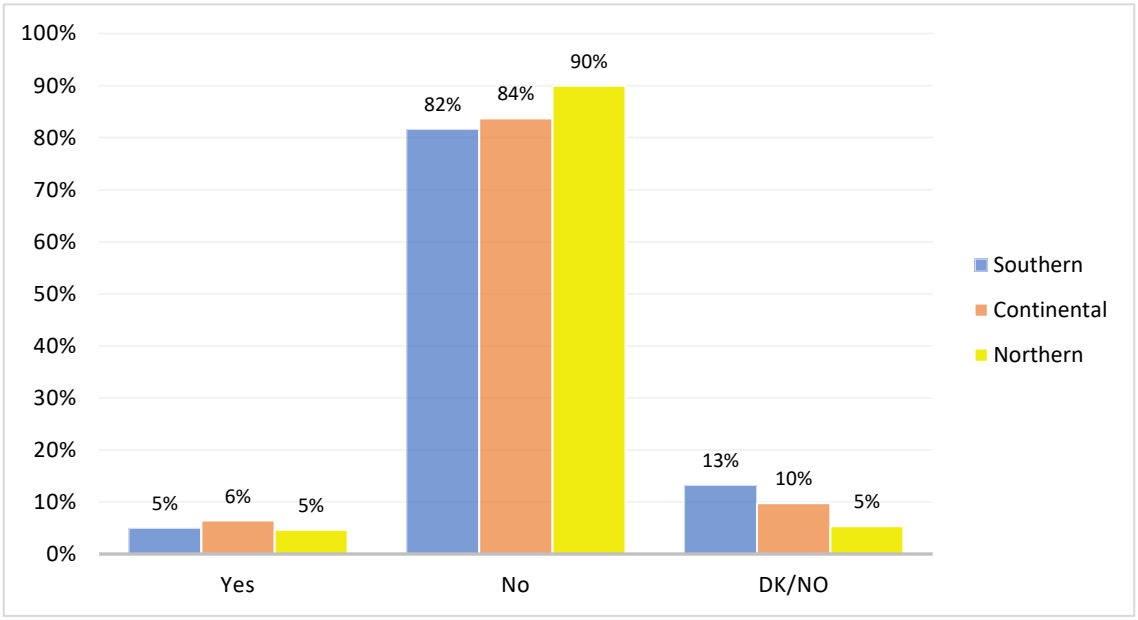
The number of respondents who declared to know that OEMs receive an economic compensation out of the data collected from connected vehicles were in general lines similar to respondents declaring not to know (52% declared not to know and 48% to know).

When asked about the services respondents would be willing to share information with, the most common preference is early detection of necessary maintenance and repairs, with detailed monitoring and recommendations (20%). Following close, respondents are in favour of receiving information provided by the vehicle about traffic and suggestions about best routes (19%) and alerts provided by the vehicle of dangerous driving conditions ahead (18%). Receiving suggestions from the vehicle about nearby parking locations, repair and maintenance garages, charging spots or petrol stations is shared by 12% of respondents and receiving adjustments on insurance rates, based on the driving behaviour showed by the vehicle 9% of the total answers. Other options received less support, such as fuel consumption monitoring for recommendations and discounts in petrol stations (8%) or to receive information from the vehicle about nearby scenic spots, restaurants, tourist attractions, stores or hospitality services (5%).

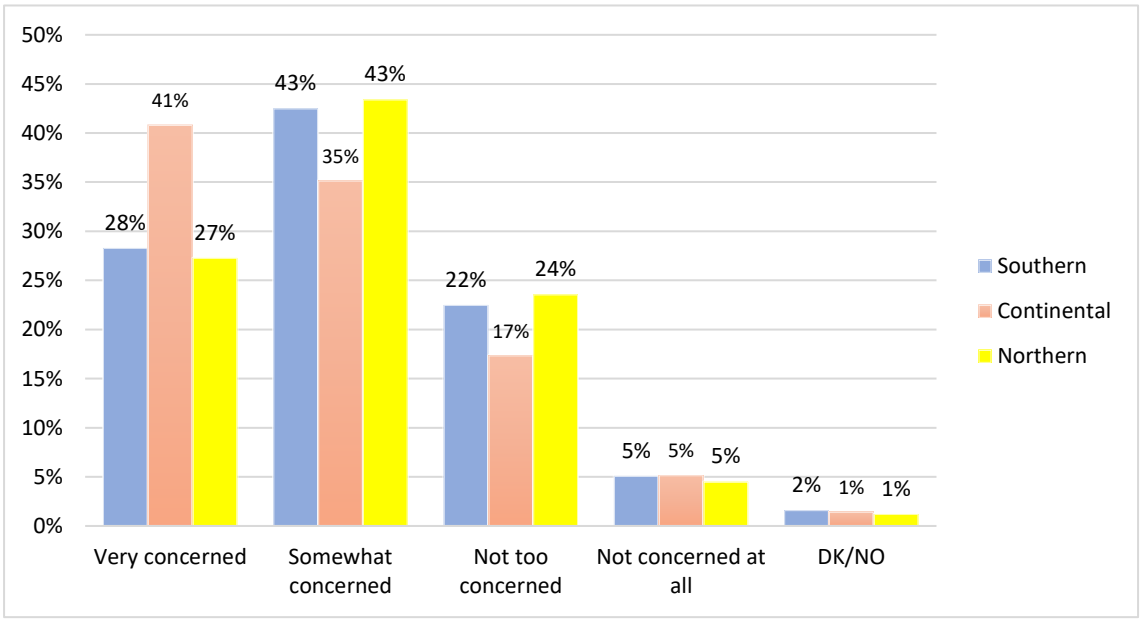
Generally speaking, there is a shared perception amongst respondents that drivers have no control over the data shared by connected vehicles, with 85% of the total respondents sharing this opinion. Only 6% perceive to have control over this data. Amongst the respondents that

declared that drivers have no control, 73% are concerned (i.e., either "very concerned" or "somewhat concerned") about this lack of control. 26% expressed moderate or no concern in this case.

Q9: Do you think drivers have control over the information collected and shared by their vehicles?



Q10: How concerned are you about drivers not having control over the information collected and shared by vehicles?



Data empowerment: information, consent and rights

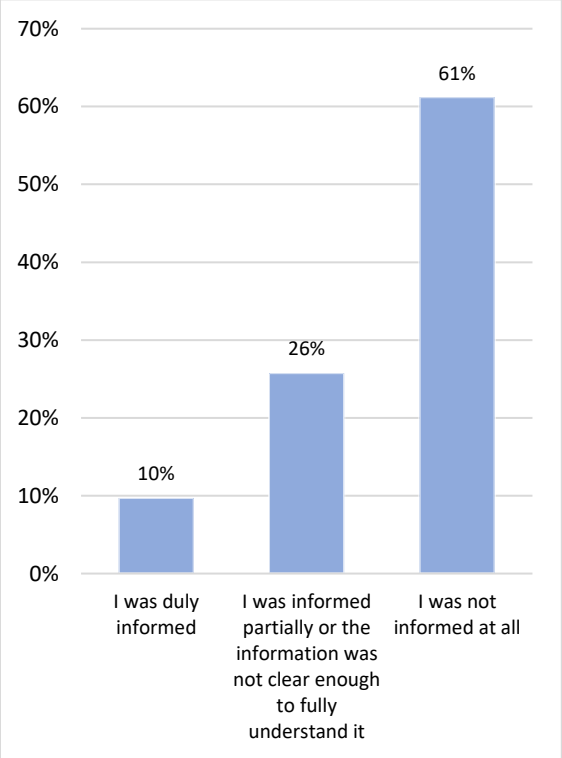
78% of the respondents answered that they have not given consent for the processing of the data collected in the context of vehicle connectivity.

Within the respondents that declared to have provided consent, 58% declared having provided it via a check box and 22% through a signed document. Only 5% declared to have given a verbal authorization as means to provide consent.

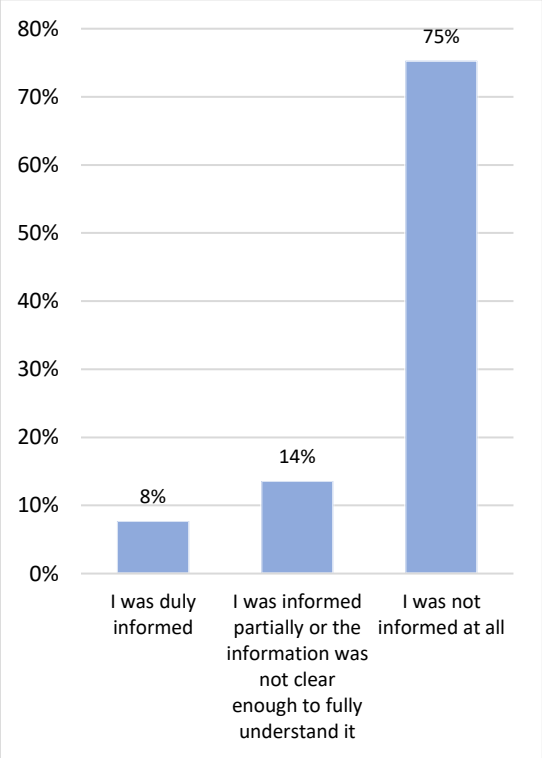
Up to 61% of the respondents who have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer declared that they were not informed at all about the fact that information would be collected from the vehicle and the purposes for which the information could be used. 26% declared to have received partial information or information that was not clear enough to fully understand it. Only 10% perceived that the information they received was adequate.

Up to 75% of the respondents who have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer answered that they did not receive any information regarding how to control the information collected from the vehicle (e.g., how to make a request or complaint, who to contact, etc.). 14% declared to have received partial information or information that was not clear enough to fully understand it. Only 8% perceived that the information they received was adequate.

Q13: If you have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer, were you informed about the fact that information would be collected from the vehicle and the purposes for which the information could be used?



Q14: If you have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer, were you informed about how to control the information collected from the vehicle (e.g., how to make a request or complaint, who to contact, etc.)?

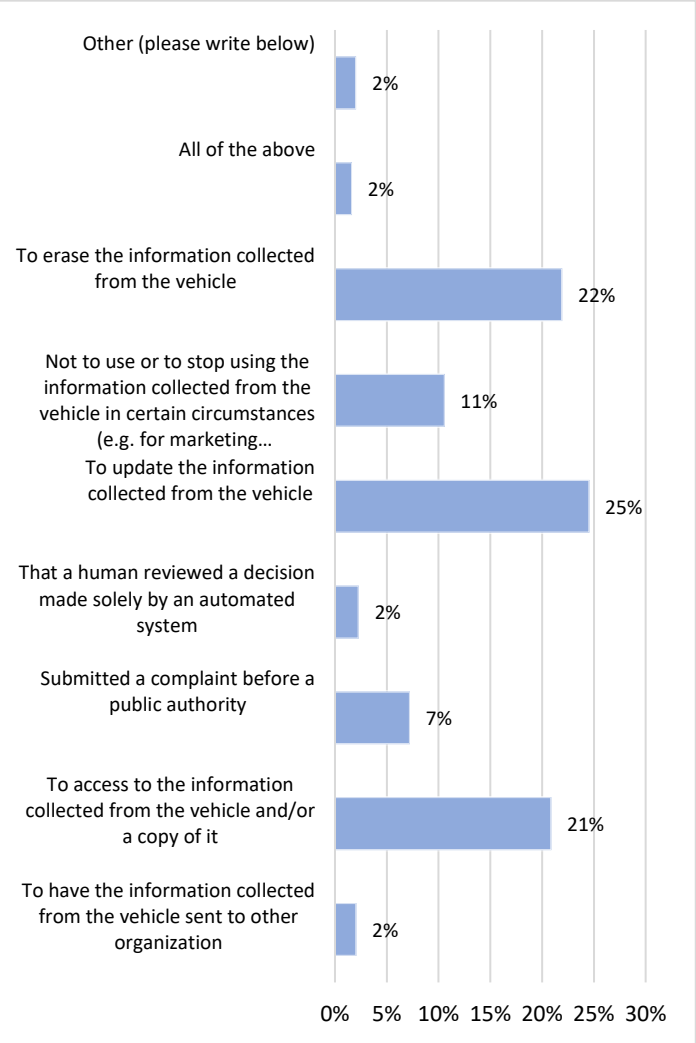


As regards perceptions and awareness about data protection rights:

- Respondents consider that drivers are entitled to request to be informed about who will use the information collected from the vehicle and how it will be used (right to be informed), with 43% of the answers.

- 39% think drivers are entitled to lodge a complaint before a public authority if there is something wrong with the way the information is used or shared (right to lodge a complaint).
- 38% think drivers are entitled to request access to the information provided to the entities receiving the data collected from the vehicle or to request a copy of this information (right of access), as well as to request the erasure of information when it is no longer necessary (right to erasure).
- 36% think drivers are entitled to request the entities receiving the data not to use or to stop using the information in certain circumstances (e.g., for marketing communications) (right to object).
- 33% think drivers are entitled to request that information is updated when inaccurate (right to rectification).
- 24% declared that drivers are entitled to request to have the information sent to other organizations at their request (right to data portability).
- 23% think drivers can request that an employee review a decision made by an automated system without any human intervention (right to not to be subject to automated individual decision-making).

Q18: Which request did you make?



A very limited number of the respondents declared to have ever exercised some of the actions laid down above. The percentage of the respondents who have exercised this right never goes up than 12% (in Germany), and is generally below 5% of the respondents, resulting in a total average of only 3% out of all the respondents declaring to have exercised some of the rights recognized by the data protection and privacy regulations.

From those declaring to have exercised one of these rights, most respondents have declared to have exercised their right to rectification (25%), followed by erasure (22%) and access (21%). 11% declared to have exercised their right to object, 7% to have lodged a complaint before a data

protection authority and 2% only to have exercised portability or not to be subject to automated individual decision-making.

When a right has been exercised, a majority of the respondents declared not to have received a satisfactory result, with 24% of the respondents declaring not to have received an answer to their request at all, 14% declared to have received an incomplete answer, up to 12% declared the answer came too late, 11% that the process was too complicated and 9% of the respondents declared not to have achieved at all the results they were looking for when making the request. Only 23% of the respondents who declared to have made a right request declared to have achieved the results they were looking for when exercising the request.

When a right has not been exercised, the respondents generally share the view that it is because they were not in the need to exercise it (49%). 18% declared they would have liked to but did not know how to, and 13% that they would have liked to but did not know that they could make any of those requests.

II. Analysis of the information that consumers receive at point of sales (Mystery Shopping)

A. Introduction and methodology overview

For the purpose of complementing the research on the degree of consumer awareness with regard to vehicle data, four *'Mystery shopping'* ("**MS**") exercises were conducted at different vehicles' point of sales. The ultimate goal of the MS exercises was to evaluate the level and transparency of information provided to consumers at the vehicle points of sales.

For further details about the methodology followed for the MS exercises and of each of the exercises performed, please refer to **Appendix III**.

B. Findings

Overall, the MS exercises revealed a significant lack of information about vehicle data collection and processing at the point of sales visited.

While some information about vehicle connectivity is provided at the point of sale, this information exclusively concerns the connectivity functionalities available and the related user's experience. However, it does not cover the implications of such functionalities, i.e., the underlying vehicle data processing.

In the best-case scenario, limited information about vehicle data processing aspects was provided but only after inquiring by the person conducting the exercises ("**Mystery Shopper**"). Even in these cases, the sales representatives were reluctant, unwilling or unprepared to provide general information about vehicle data processing or elaborate on any of the questions raised.

No additional information resources (such as privacy policies, privacy notices or references to websites where information in this regard can be obtained) – that could assist consumers in understanding the implications of data processing deriving from connected vehicle functionalities – were provided either, even after showing an interest in these issues.

Consequently, the MS exercises suggest that the level and transparency and clarity of the information provided on vehicle data processing at the points of sales is quite deficient and could clearly be improved in many instances.

More in particular, the MS exercises showed:

Reluctancy or deliberate avoidance to elaborate the implications of connected vehicles in terms of data processing

Information related to vehicle connectivity provided at point of sales is exclusively limited to practical aspects, i.e., the functionalities available and the related benefits and usefulness for vehicle drivers/users.

In none of the exercises the sales representatives tackled *motu proprio* implications of the data processing linked to vehicle connectivity functionalities.

In some cases, the sales representatives took a reactive approach and only tackled these points if specifically inquired by the Mystery Shopper. In other cases, the sales representatives circumvented or directly refused going through aspects relating to data processing.

Lack of general knowledge and expertise to explain data processing aspects

Even when the sales representatives were open to discuss about vehicle data processing, the information was either unclear, incomplete, imprecise or misguiding.

In several cases, the sales representatives directly manifested not to be in a position to answer questions regarding these points or deliberately avoided answering them.

Incomplete, imprecise and misleading information

In none of the MS exercises conducted it was possible to get a clear understanding of the nature of the data collected, the subsequent processing of vehicle data, the rights of vehicle drivers/users and the relevant consent requirements.

In most cases, the sales representatives gave a limited view about the nature of the data that is collected in the context of connected vehicle, stating that only geolocation data is collected. In those cases where the sales representatives stated that other types of data are collected, the nature of the data and the extent of the collection by vehicle manufacturers were unclear.

In all the MS exercises the sales representatives stated that the data collected is not shared with third parties and explained that the purposes of processing are limited to provide app-related services and mandatory functionalities such as the eCall and bCall.[133]

In no case the sales representatives mentioned that data could potentially be used for other purposes.

In most cases, it was unclear whether data processing happens in connection with the app made available by the vehicle manufacturers only, or also in case the app is not downloaded/used.

Likewise, the information provided in relation to the data subjects' rights (such as deletion or portability) and consent was in all cases linked to app use which led to the conclusion that data processing and, therefore, any applicable rights or consent requirements, was app related.

No additional information resources on data processing are offered

In spite of the fact that in all MS exercises the Mystery Shopper expressed interest on data processing implications relating to vehicle connectivity, in no case the sales representatives offered or provided other information resources (such as privacy policies, notices or websites) where further information in this regard could be obtained.

[133] The bCall functionality refers to a service which allows car users to call local road assistance in case of a breakdown.

4

Section IV: Challenges & Opportunities

This section conducts three analyses of areas which might present challenges and opportunities to the stakeholders involved in the automotive markets linked to connected vehicles. It starts by analysing different types of contractual/informative documents relevant to the processing of personal data in the context of connected vehicles, selected from different OEMs. It continues by identifying the opportunities and benefits for different actors and society derived from the effective implementation of an effective, easy-to-exercise right to data portability. Finally, it studies whether the current EU Privacy Regulatory Framework and the conditions under which OEMs collect, process and make their data available to third parties, might create disadvantages to ISPs when offering services and developing innovative services for vehicle users.

I. Analysis of the contracts signed by consumers when purchasing a vehicle

A. Introduction and methodology overview

Several consumer vehicle purchase contracts and privacy policies have been reviewed for the purpose of assessing (i) the clarity of the information/conditions and implications on the sharing and processing of vehicle data; and (ii) whether consumer consent is requested in connection to the use of their (personal) data, including third-party use.

This process consisted on the review and analysis of different types of OEMs' contractual/informative documents relevant to the processing of personal data in the context of connected vehicles. In particular, we have reviewed (i) purchase and sale agreements from dealers in Spain; (ii) general website privacy policies of different vehicle brands applicable in certain EU/UK jurisdictions; (iii) privacy policies in relation to data processing for the connected vehicle for different brands applicable in certain EU/UK jurisdictions; (iv) app privacy policies for vehicle connectivity services; and (v) other documentation which could be useful to understand the data processing in the context of connected vehicles (e.g. installation orders for vehicle connectivity, privacy policies of related automotive services).

Please refer to **Appendix IV** for further information about the process and specific findings for each brand analysed.

B. Findings

Based on the documentation reviewed, several findings have been drawn which we have outlined below.

Information is not always available

In general terms, the documentation analysed shows a clear pattern by which privacy aspects regarding the connected vehicle are not dealt with in the sales and purchase agreements. These documents have a data protection section or annex, but it does not cover the processing relating to connectivity functionalities but instead refers to the fulfilment of the purchase order, marketing activities, etc.

It was verified that the data processing relating to the eCall functionality is not mentioned in app privacy policies (except in some cases where emergency value-added services are offered) that have been reviewed. Accordingly, this suggests that information in this regard should be provided either in the sales and purchase agreement, or in the vehicle owner's manual. Taking into account that the reviewed sales and purchase agreements do not include any information

on this functionality, it seems that the information about this processing is not being made available to consumers, at least, before purchasing the vehicle.

Likewise, whether other connectivity functionalities involving data processing were available and activated without the need to download the app, the information about these processing would not be available for users, at least, before the purchase of the vehicle.

It is also very exceptional for OEMs to make this information available on the sections of their websites which are dedicated to present the vehicles and their connectivity functionalities. Contrary, most of the brands examined provide information about data processing aspects in the context of vehicle connectivity at the moment when the vehicle user downloads the brand's app. In practice, this situation means that, in a majority of cases, information on data processing aspects in the context of connected vehicles is not made available in the moments where this information might be of relevance to consumers, e.g., during the consideration stage in the purchase process.

Information is often fragmented across different documents

Several brands (three out of seven) have the information about data processing in the context of connected vehicles scattered across several documents. This entails that the information on the framework applicable to data processing is fragmented and result in an additional complexity for consumers to understand the implications that the use of connectivity functionalities might have in relation to their personal data. This situation can also contribute to information fatigue.

Recurrent deficiencies on data sharing aspects

A significant number of the documents reviewed showed some deficiencies on data sharing. This is normally due to providing unclear or insufficient information for the average consumer to understand who the recipients of the information shared are. These deficiencies affect five out of the seven brands analysed.

It is also common that the information concerning the sharing of data does not explain whether the consumer needs to consent to the data sharing or whether the transfer is articulated by means of a legal basis different than consent. We had the opportunity to observe that sometimes the legitimate interest of the data controller is relied upon as the basis for the transfer of data to third parties, without granting opt-out mechanisms to reinforce the consumer's control over their data. This situation, in which there is no information available to determine whether consent is the appropriate legal basis, or where opt-out mechanisms are not made available to consumers, can result in consumers not having any means of control over the personal data that is shared by the connected vehicle.

Information incomplete, insufficient and hard to find

In three out of the seven cases studied, the documentation reviewed has revealed incomplete or insufficient for the average consumer to be in conditions to determine the scope and consequences of the processing. In one of the cases studied, the relevant information is not easily available to users along their customer journey but require extensive browsing in order to be able to find it. In other occasions, the documentation reviewed showed that information

which is made available to consumers in regard to the processing of personal data in the context of connected vehicles is unclear in some respects.

Informative shortages detract from consumers' control over their personal data

Fragmented, unclear, incomplete and hardly accessible information can make it difficult for consumers to understand the implications of data processing in the context of connected vehicles. In especial, unclear and incomplete information in regard to types of data processed and the rights granted on how to exercise these rights prevents the average user to be able to exercise their rights effectively, therefore creating an illusion of control on paper which is not corresponded in reality.

Save for one exception, OEMs do not provide information which is intelligible and not discouraging to the average consumer, for instance, by using visual aids to support the explanation and explain the processing and its implications. Moreover, as a general rule (all cases except for one, which has a data protection information web portal), information on data processing in the context of vehicle connectivity seems to be hidden from consumers in the OEMs website environments. Only one brand provides practical information, further to what is prescribed by law, to provide consumers with actual knowledge about aspects that can be very relevant to them. This is the case, for instance, in relation to information about what happens with the personal data stored in the vehicle once it is sold to a third party. From the analyses, only one brand warns consumers to reset all their information before selling their vehicles and explain the risks if not deleted.

Shortages regarding consent

In one case, the documentation reviewed revealed that one of the OEMs studied is processing geolocation data "by-default" prior to having obtained consent from the consumer, i.e., collection happens once the app is running unless deactivated by the user.

In other case, several processing activities are supported on OEM's legitimate interests in a context in which is likely that consumers cannot find the relevant information and do not have actual means at their disposal to opt-out for these processing activities. This situation makes consumers not being aware of the existence of these processing activities, or, if aware, not able to easily object to them. Therefore, this legitimate interest setup can turn into a way to bypass consent.

In sum, the analysis carried out presents a scenario somewhat discouraging in what regard to information to consumers and personal data control. The inherent complexity of the processing linked to connected vehicles should require, in line with Recital 39 GDPR, an extra effort on the side of data controllers to ensure consumers are aware of the scope, consequences and risks of the processing. A basic understanding of the implications linked to the processing activities performed in the context of connected vehicles is paramount to ensure that data subjects are in a position where they have the means to effectively control their personal data, which is one of the GDPR's declared objectives as per Recital 7. Nonetheless, the sometimes incomplete, insufficient, unclear, unavailable or fragmented information about data processing, sharing and rights available for consumers, along with questionable data processing practices and limited provisions of tools for easy privacy management, is likely to result in a significant lack of control for consumers regarding their personal data.

II. Explore the potential of data portability in mobility and its impact on connected vehicles

This subsection analyses the potential that an effective, easy-to-implement data portability right might have in mobility and its impact on connected vehicles.

A. Overview of data portability and general benefits

Data subjects (i.e., vehicle users) have the right under the GDPR to have their personal data directly transferred from data-holding OEMs to other service providers such as ISPs.[134] Thus, the GDPR could serve as a viable route for consumers to make data from a smart device available to other service providers where certain conditions are met.

As later explained in section III, subsection IV ("Assess disadvantages for ISPs posed by the current regulatory framework and OEMs conditions"), the current legal design of the right to data portability under Article 20 GDPR and uncertainties around its application in practice challenge the ability of this tool to serve as a mechanism to put an end to the current situation where OEMs are gatekeepers of the data collected from connected vehicles.

It is worth exploring the impact of the right to data portability on the different stakeholders in the connected vehicle ecosystem whether this right was designed in a way in which consumers could exercise it fully and without significant constrains. The aim is to evaluate whether this would create benefits for all the industry's stakeholders: data-holders, third parties facing obstacles or who do not have access to data, consumers, public institutions, and society as a whole. In the following sections we will be covering in detail how data portability can impact each of them.

To start, the right to data portability could allow new companies to become data holders, arising new opportunities to other stakeholders in the connected vehicle ecosystem. This data transfer would allow collaboration in the creation of products between different agents, drive innovation, reduce market barriers and help to offer a service or product more in line with the user needs. The main advantages this new context would bring are:

- **Increased innovation in the sector**:[135] the right to data portability allows different players in the industry to use data in different ways to generate new innovative services and products. OEMs can choose to introduce new external data sources to complement their internal data pools, while third party companies can use data they would never have been able to access before, therefore allowing innovation with new products, services, business models, infrastructures, etc.

- **Products with an improved result due to several parties working together on it**: data portability could serve to foster cooperation between different companies to find synergies and offer consumers enhanced products to those available in the market.

- **Creation of products and services better suited to the needs of end-users**: through a full implementation of the data portability right, companies can better understand consumers'

[134] See for this debate and the following policy options C-ITS Platform, *Final Report 2016*, 72-90; TRL, *Access to In-Vehicle Data and Resources – Final Report 2017*.
[135] McMurren, Juliet and Verhulst, Stefaan G., *Data to Go: The Value of Data Portability as a Means to Data Liquidity*, 2021.

needs and make data-driven decisions and thus generate products and services with a customer-oriented approach.

- **Increase the number of data players in the market**: thanks to data portability, current barriers to market entry -that prevent third party companies from benefiting from the personal data generated in connected vehicles- can be reduced. The fact that users can freely transfer their data encourages fair competition and the entry of new companies in the industry.

B. New business opportunities

An effective, easy-to-implement right to data portability can lead to a great variety of new business opportunities for existing and new market players while creating value for consumers. Currently there are many stakeholders in the automotive and mobility industries with whom the consumer already interacts (among others, repair and maintenance and insurance services) and that could offer very direct benefits if they had further data from the connected vehicle. At the same time, the aggregated data that companies could have from the sum of each individual person could lead to further improvements and help companies make data-driven decisions.

A context in which data portability was fully implemented and easy to exercise, a greater number of actors could contribute to finding use cases in which the data could potentially be used to create new business opportunities and, therefore, make the overall market grow. In general, commercial use cases are motivated either by generating revenue or reducing costs. Players in the same, related, complementary, or even non-transport/mobility related industries may be interested in using connected vehicles and vehicle data to create new use cases for one or both purposes. Access to more data through the data portability right could allow actors in the ecosystem to:

- On the one hand, achieve increased revenue companies can use data from a single client or analyse aggregated data to provide insights into driver behaviour and vehicle health to generate direct monetization through the sale of products, benefits or services to the consumer, as well as generate personalized advertising to drive individual offers to customers.

- On the other hand, reduce R&D and material costs by collecting field data from products to improve their development, analyse usage patterns to reduce repair cost and inactivity time and improve customer satisfaction through better adaptation of products/services to customer needs.

Widening the scope of actors with access to data from connected vehicles through an effective, easy-to-implement right to data portability can lead to several improvements, both for the consumer and the industry, such as improve the driving experience, increase comfort for the driver and optimize products. Depending on the type or origin of the data generated by the connected vehicle, different use cases have been identified in which new or existing actors could enter to create new business opportunities:[136]

[136] European Commission, *Digital Transformation Monitor – The race for automotive data*, 2017.

- **Driver Data** is produced by people using services offered in connected vehicles. This type of data includes identification data, direct communications from the vehicle, preferences, and vehicle usage. This can generate use cases like the following: (i) innovative insurance, where new services can range from usage-based insurance ("pay-as-you drive", "pay-when-you-drive"), monitor driver behaviour and help in accident reconstruction; (ii) driver insights, such as listening habits, location, vehicle usage, etc. which could help companies to better target advertisements and campaigns, products, and personalized offers, etc. The connected vehicle is also expected to become the next ecommerce platform as vehicle users will take advantage of their driving time to shop and the vehicle will be able to offer discounts based on the user's needs; or parking solutions**,** mainly focused on parking space detection and automated payment based on the staying time.
- **Vehicle communication** can generate services based on the data generated between the vehicle and the environment, as well as aggregated external data collected in the vehicle (weather conditions, traffic…). This can generate use cases like the following:
    - **Mobility as a service:** vehicle location generates opportunities for carsharing services (carpooling, P2P sharing, on-demand mobility services, subscription, etc.).
    - **Energy & Eco:** data can help optimize vehicles consumption with driving style suggestions, monitor the recharging times and plan efficient trips.
    - **Safety Solutions:** actions such as airbag triggering, hard braking and speed data can help improve response times in case of accidents and contact emergency services if needed.
    - **Mapping and planning solutions:** capturing information about the location and environment of connected vehicles can help to successfully develop and constantly update high-definition (HD) maps.
    - **Smart home:** integrating data from home and the vehicle in a connected dashboard will enable remote control of the house systems and devices.
- **Vehicle Data** is information generated by the technical status of the vehicle such as sensor-generated data. Companies are developing a variety of services that can aid in the safety and management of the vehicle itself, like the following:
    - **Predictive maintenance**: historical data and sensor-data can help anticipate technical issues through software applications.
    - **Remote diagnosis:** data allows to monitor the health status of the vehicle in real time in remote (through alerts, indicators, etc.).
    - **Fleet management:** new data embedded in the fleet can help companies operate much more effectively with real-time location, diagnostics, fuel management... as well enhance driver safety.

C. Public Social Benefits

An extensive use of the right to data portability by consumers will generate a set of aggregated anonymized data which can be very useful both for private and public corporations. Only with part of consumer's data, companies can already convert it into valuable information to improve

current products and services and create new ones. In this sense, facilitating the free flow of data through effective and easy-to-implement data portability can be used to respond to social problems which will positively impact both public institutions and society as a whole. Vehicle data use cases with socio-economic benefits are:

- **Smart cities**:[137] individuals can help reduce pollution, traffic, and increase safety for citizens by giving access to their data to other public entities and private companies. With the availability of this data, congestion management, route optimization, emissions management, parking management, etc. can be made more efficient.
- **Infrastructure improvement**: for instance, the data generated in the vehicle from the tire contact with the road can give a lot of information about the road condition and therefore help infrastructure operators ensure proper maintenance.
- **Reduction of accidents**:[138] the exchange of data between vehicles and their surroundings can reduce the number of accidents through detecting density of roads, the speed, etc..
- **Sustainability**:[139] emissions can be decreased as a result of the use of the data generated by the vehicles. Main drivers contributing to emission reductions include:
    - Vehicle performance due to early maintenance.
    - Optimized energy consumption.
    - Efficient routing.
    - Digital speed limits.

D. Consumer Benefits

Besides benefiting companies, an effective implementation of the right to data portability can have a positive impact on consumers choice, as it gives them control over their personal information. The right will facilitate consumers the access to more competitive products and services and provide convenience in their relationship with companies. The individual benefits of data portability include:[140]

- **Increased autonomy and power to the user**: the right to data portability generates greater user confidence, as control over their data is transferred to them. In addition, users opt for the ability to decide with whom they want to share their data and what data they want to share. In turn, greater autonomy and control is expected to boost transparency and trust in the relationship between data holders and consumers.
- **Easiness**: when switching providers or services, the portability right allows users to keep and migrate their information.
- **Security**: The right to data portability allows individuals to carry out actions related to the protection of their data such as backing up, recovering data from obsolete servers, etc.

[137] See, for instance, https://otonomo.io/use-cases/smart-cities-car-data/.
[138] See, for instance, https://roadsafetyfacts.eu/how-can-automated-and-connected-vehicles-improve-road-safety/.
[139] See, for instance, https://www.bnpparibascardif.com/en/article/-/article/big-data-drives-environmentally-friendly-and-sustainable-transport.
[140] McMurren, Juliet and Verhulst, Stefaan G., *Data to Go: The Value of Data Portability as a Means to Data Liquidity*, 2021.

Therefore, it increases the security of the user's activities, as they can recover their data if needed in case of theft or loss.

- **Broad new portfolio of products and services**: data portability promotes innovation across sectors. This is achieved because more organizations have access to data and therefore data sources can be combined to lead to the creation of new goods.
- **Better offers and more competitive prices**: thanks to data access, more customizable goods can be generated, switching costs are reduced, more companies enter the market with new products, and industry players are more informed about the needs of individuals.

Some of the benefits to consumers can be illustrated by the example of the energy sector following the adoption of the Electricity Directive in 2019.[141] In this Directive electricity companies are compelled to share customer data through a data portability right. The typology of data they must share with other electricity suppliers are metering data, consumption, and the data necessary for a customer to switch companies. This data, in turn, is personal data related to a customer's energy profile, so there is an overlap with the GDPR's right of portability.

Thanks to the circulation of data, the customer does not have to pay any additional cost when requesting the portability of their data. Moreover, it is possible to stimulate innovation and encourage competition between the different companies in the sector.[142]

The Directive places the consumer at the centre. All consumers will have the possibility to actively engage in the energy market by adjusting their energy consumption in response to market conditions. In this way, consumers will be able to benefit from lower electricity prices or other incentives. In addition, to be able to take advantage of new developments in the energy market, consumers will have access to intelligent energy systems and dynamically priced electricity supply agreements linked to the spot market.[143]

E. Market maturity

Data portability brings the opportunity to reach out and facilitate the transfer of personal information to other stakeholders within or outside the automotive industry. As a result, this right leverages the potential value of existing, mature, and emerging use cases.

Data is intended to be the primary driving force behind service design, setup, and optimization within the automotive industry. Otonomo, a data aggregator or car data services platform, has developed OtoGraph,[144] which displays the maturity of the connected vehicle market.

The OtoGraph is developed by assessing two axes:

- Market maturity per use case: measured in terms of the maturity of industry players to leverage data to create new offerings.

---

[141] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (Text with EEA relevance.) OJ L 158, 14.6.2019, p. 125–199.

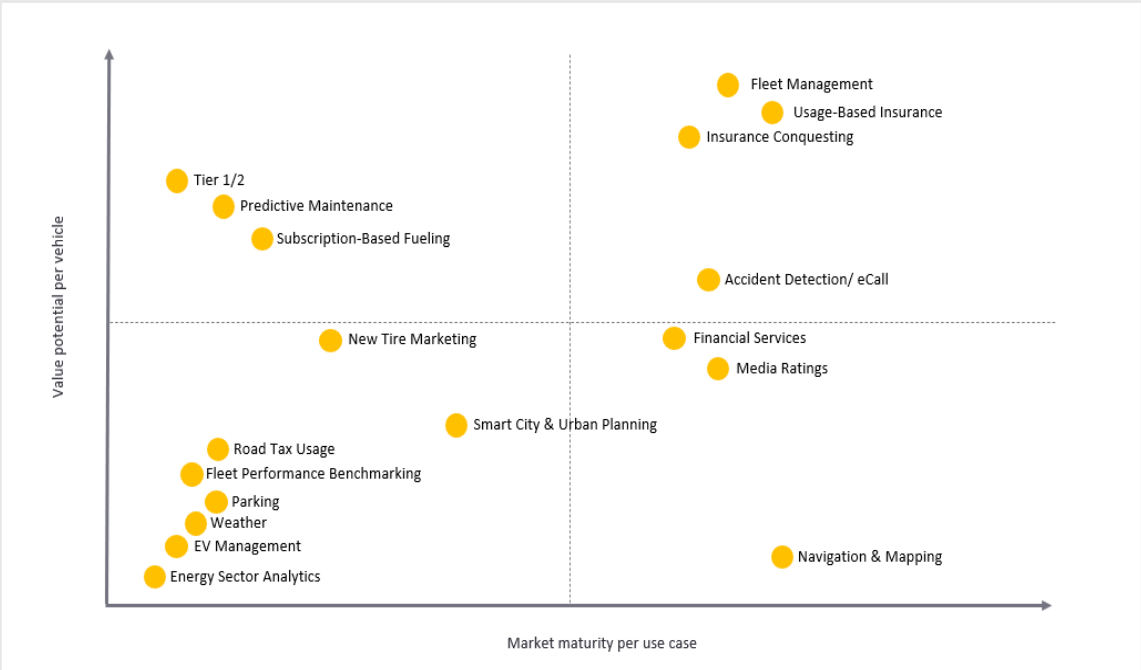
[142] Cerre, *Making data portability more effective for the digital economy*, 2020.

[143] See http://www.eubelius.com/en/news/the-new-electricity-directive-preparing-the-european-energy-market-for-the-future.

[144] Otonomo, *The Automotive Connectivity Ecosystem: Car Data and Emerging Market*, 2019, available at: https://otonomo.io/blog/the-automotive-connectivity-ecosystem-car-data-and-emerging-markets/.

- Value potential per vehicle: evaluated on the type of data use cases employ, especially in terms of the degree of personalization vs. data aggregation giving more broad services. The idea that lays behind is that more personalized use cases will need user agreement and will therefore be more complex and expensive to implement.

OtoGraph (Source: Otonomo)



The results show how some use cases currently have higher market potential than others.

It is anticipated that in the coming years all the use cases will shift to the right in the graph as market maturity grows in terms of leveraging vehicle-generated data and the delivery of services to drivers gets more sophisticated. This, in the end, shows that data has the potential to make the automotive market grow through new solutions as players take more advantage from data.

As it can be seen in the chart above, the automobile market is more mature for the mapping and navigation use case, as the application of data from multiple sources to create a clear and usable image for drivers is highly robust. The insurance industry is another sector that is also quite advanced in its utilization of vehicle data. Insurance firms are already well-versed in the collection of data on driver behaviour. They are analysing automobile data from telematics devices in order to develop usage-based insurance programs, such as pay-as-you-drive or pay-how-you-drive.

Even though both are established industries, the insurance use case offers a larger potential for generating value per vehicle than the mapping use case. Insurance firms modify driver-specific data to provide tailored services. Map firms, on the other hand, utilize aggregated data based on anonymized automobile data attributes to provide more broad services to customers.

However, this does not imply that the use case is less valuable. Use cases that are more valuable per vehicle also need driver agreement to share data, which may be more difficult to get. Consequently, services that rely on the aggregation of data from thousands of vehicles, such as data from the external environment, the mechanical condition of the vehicle, and its use, are

the data categories where customers are most willing to provide information and, as a result, are the most cost-effective as a whole.

In contrast, emerging sectors such as electric vehicle management, subscription-based fuelling, in-vehicle delivery and parking applications are still in their early stages in terms of data utilization.

The OtoGraph can show how, as more personal information from consumers is shared within companies, new use cases can be put in place, which means that products and services can be generated for the market to consume. Accordingly, data portability can contribute to a strong market growth through the generation of new value.

F. Market growth value

Such an implementation of the right to data portability will become an important tool that will contribute to the free flow of personal data and thus promote competition between data controllers. As previously mentioned, when companies have access to the data of their customers through the data portability right, it allows them to know their needs and therefore adapt their value proposition or generate new ones. On the consumers' side, it allows them to easily switch between different service providers and thus promote the development of new services in the context of data generated in the connected vehicle.

Therefore, the data portability right is nowadays a key driver for the generation of new business opportunities and therefore for the growth of the automotive market.

In this section, two studies have been analysed. On the one hand, a study by the Organisation for Economic Co-operation and Development (OECD)[145] that provides a rough estimate of the economic impact of the free flow of data on the global private and public sector. On the other hand, a study conducted by Statista, a leading statistics portal, that estimates the expected growth of the connected vehicle market due to data access and sharing.

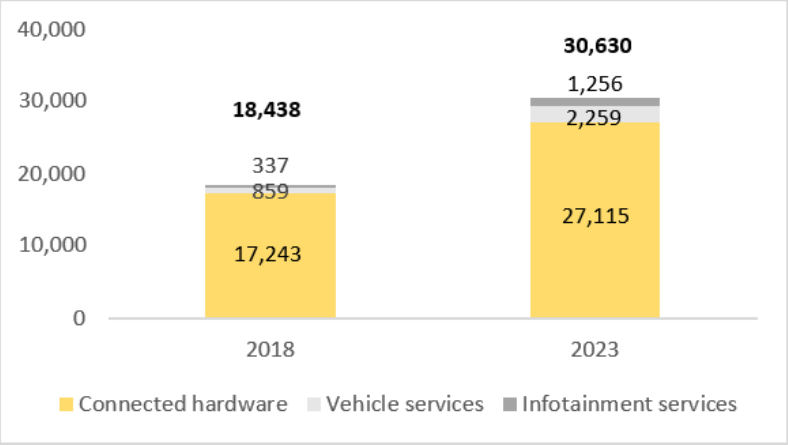
The OECD study indicates that the free flow of personal data would stimulate innovation, as data would be freed from its existing silos and a much larger set of stakeholders would have access to it. The OECD, in 2019, noted that data access and sharing is estimated to generate social and economic benefits worth between **0.1-1.5% of the world's GDP** in the case of public-sector data and between **1.0-2.5% of the world's GDP** if private-sector data is included.

The Statista Digital Market Outlook report[146] forecasts the revenue generated from connected vehicle data grouped into 3 categories: connected hardware, vehicle services and infotainment services. The scope of the study includes 150 countries. It estimates that the overall market will grow until 2023 at an average growth rate per year ("**CAGR**") of 11%, going from 18,438 million US$ in 2018 **to 30.630 million US$ in 2023**. Within Europe, the market is expected to grow from 5,600 million US$ in 2018 to 9,100 million US$, with an annual growth rate of 10,3%.

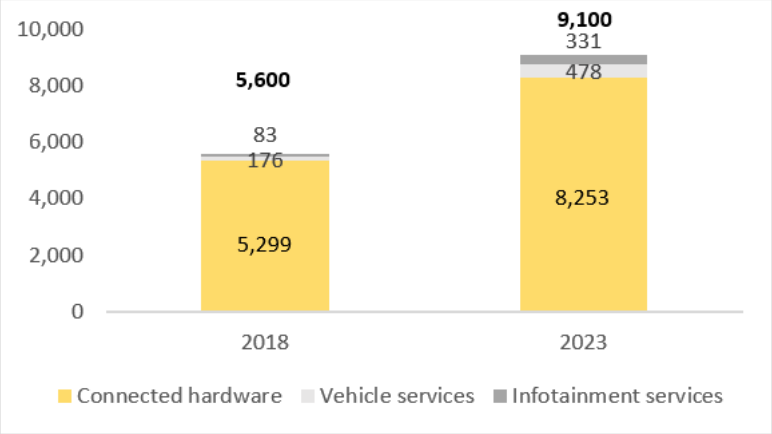
[145] OECD, *Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies*, 2019.
[146] Statista Digital Market Outlook – Market Report, *Connected Car Report 2019*, 2018.

Per category segment, connected hardware is what currently has more weight in the overall market revenue, and is estimated to grow at a CAGR of 9.5%, generating an incremental market revenue of 9,872 million US$ in the period 2018-2023. The vehicle services category is expected to grow at a CAGR of 21,3%, generating a market value of 1,400 million US$ in the same period of study. Last, the infotainment service segment is expected to grow at a CAGR of 30,1% and generate an incremental market revenue of 919 million US$.

Connected Car Revenues Worldwide (USD millions) (Source Statista Market Report, Connected Car Report 2019, 2018)



Connected Car Revenues in Europe (USD millions) (Source Statista Market Report, Connected Car Report 2019, 2018)



III. Assess disadvantages for ISPs posed by current regulatory framework as well as OEMs conditions

A. Introduction and methodology overview

Based on the analysis carried out and findings reached in previous sections of this Report, this section studies whether the current EU Privacy Regulatory Framework and the conditions under which OEMs collect, process and make their data available to third parties, might create disadvantages to ISPs when offering services and developing innovative services for vehicle users.

The process to reach findings in this section consisted, in the first place, on the review and analysis of the regulations studied and the conclusions reached in relation to the application of the EU Privacy Regulatory Framework (as studied in section II), to understand how current regulations might create disadvantages to the offering and developing of services by ISPs.

On the other hand, the conditions under which OEMs collect, process and share personal data with third parties are analysed to arrive at conclusions. For the purposes of this Study, the reference to "OEMs conditions" takes a broad approach as it not only considers the actual conditions in sales and purchase agreements but also the privacy policies (as studied in section IV, subsection I, "Analysis of the contracts signed by consumers when purchasing a vehicle") and, to a lesser extent, the information data subjects receive at point of sales, as explained in detail in section III, subsection II, "Analysis of the information receive at point of sales". A broad understanding of the conditions under which OEMs process personal data (whether contractual – conditions in sales and purchase agreements – or pseudo contractual/informative – privacy policies and information at point of sales), provides an idea on how this data is shared with third parties and, hence, how ISPs could be receiving this data (if the case may be) and whether current conditions pose disadvantages to them.

Therefore, this section shall be read in the light of the abovementioned sections, including the methodologies followed for these purposes, which are also relevant to this analysis.

B. Findings

Based on their private incentives and subject to the applicable legal framework, organizations reach private data governance arrangements based upon contracts, including those related to the exchange and sharing of data.

Thus, there is a two-layered approach to data governance regimes for the exchange and sharing of personal data (distinguishing between a *Level I* data governance regime composed by the legal and regulatory framework for markets, and a *Level II* regime composed by the private data governance arrangements based upon contracts and privacy policies) can be useful to understand how the current framework, as well as OEMs conditions can negatively affect ISPs.[147]

In the first place, this section examines how, despite being a framework for the protection of the fundamental rights of individuals, the data protection and privacy legal framework also

[147] This two-layered framework for data governance regime analysis is developed in Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017. Although built for economic analysis of data governance regimes in complex multi-stakeholder situations, particularly IoT scenarios, it serves well to conceptually frame this analysis from a data protection and privacy perspective.

creates limitations constraining the voluntary sharing of data. Further, these limitations might be leveraged to avoid, limit or control the sharing of personal data and foster data concentration, entrenching an advantageous market position for certain player based on better, even exclusive access to data and the control over the terms and conditions under which data is shared in the market, with adverse effects on ISPs.

Also in the realm of the *Level I data governance regime* (legal and regulatory framework), the current legal design of the right to data portability under Article 20 GDPR and uncertainties around its application in practice challenge the ability of this tool to serve as a mechanism to put an end to the current situation where OEMs are gatekeepers of the data collected from connected vehicles, hence proving ineffective for serving as a data empowerment or antitrust tool, to the detriment of ISPs.

On a second part, as regards the level II data governance regime (contracts and privacy policies), this section studies how there are limitations in practice to the actual control that vehicle users have over their personal data processed, and how this can discourage seamless access or transmission of data to ISPs, with a negative effect on them.

Disadvantages posed by the current EU Privacy Regulatory Framework

As analysed in section II ("Application of the EU Privacy Regulatory Framework in the context of vehicle connectivity"), in the context of vehicle connectivity, the general personal data protection and privacy rules are laid down in two laws: the GDPR and the e-Privacy Directive. Also, some sector regulations include certain relevant aspects in the field of privacy, including legal data access regimes.

Our research points at two potential sources of disadvantages that the current EU Privacy Regulatory Framework poses to ISPs: (i) potential disadvantages based on the general deterrents to data sharing of the legal framework and the consolidation of "lock-in" effects; and (ii) potential disadvantages based on the current design of the right to data portability.

Potential disadvantages based on the general deterrents to data sharing of the legal framework and the consolidation of "lock-in" effects

Level I data governance regime defines the "rules of the game" for the exchange and sharing of personal data in markets, shaping private incentives and the contractual arrangements that organizations can arrive at through contracts (Level II data governance regime).

The data protection and privacy legal framework limits the extent to which personal data can be shared due to the application of the stringent rules laid down in the GDPR and the e-Privacy Directive.

Indeed, the GDPR and e-Privacy connected provisions are, in the first place, a system of protection of natural persons in order to safeguard their fundamental right to privacy and data protection.[148] As such, they impose strict obligations regarding the collection, processing, storage, use and sharing of personal data, limiting data controllers' ability to share personal data. This Report has explored the different requirements that shall be complied with if intending to share personal data, which will normally require contractual arrangements

[148] "The protection of natural persons in relation to the processing of personal data is a fundamental right" - Recital 1 GDPR.

between the parties wishing to share the data (e.g., a data processing agreement or a joint controllership agreement) and/or obtaining prior informed consent from individuals. Compliant options to share personal data are limited under these regulations and come only at a cost, illustrated by the cost of designing and implementing mechanisms to share data in accordance with the applicable legal framework, as well as the legal uncertainty when applying the latter that could lead to an inadequate design/implementation and the corresponding regulatory risk. As a result, in order to share personal data, the economic agents' incentive to exchange or to share data with third parties must be higher than the costs of compliance with these regulations and the legal uncertainty assumed.

Under ordinary market conditions, where all actors have similar means to access data, ISPs would not be affected by the general limitations to data sharing posed by data protection and privacy regulations, or they would be affected in a similar manner to other market players, particularly OEMs. But under the current data bottleneck, OEMs enjoy an advantageous position which data protection and privacy regulations contribute to consolidate, to the detriment of ISPs. There are strong private incentives (i.e., controlling access to secondary markets for automotive and mobility services) justifying the use of the existing legal limitations as pretexts to avoid, limit or control the sharing of personal data with possible competitors.

This is particularly important, as in IoT environments, if we take into account that these services are based on data coming from connected vehicles which are not substitutable by nature. Buying a connected vehicle increasingly transcends the purchase of a product and resembles the subscription of a long-term service with the OEM, subject to maintenance and updates and with a complex pricing structure, which does not only include a fixed price for the vehicle itself, but also the provision of data in exchange for services. It can be argued that this data has economic value to the extent that it is profitable for OEMs, for instance, if used for the improvement of their own products, for innovation and/or for amplifying their revenues through providing access to this data.[149] Connected vehicles are valuable durable products demanding a permanent communication with a system currently under OEMs' control, including the necessary updates of the vehicle's system.

In this context, there are strong private incentives for OEMs justifying the use of the existing legal limitations as pretexts to avoid, limit or keep control over the conditions under which data is shared with possible competitors. This does not mean that personal data will not be shared by OEMs; sharing will take place but only to the extent authorized by OEMs (when there is an adequate legal basis for the sharing, such as consent), with selected partners to fuel a *pseudo*-closed environment where entrance is sanctioned and subject to OEM's terms and conditions. In other words, exchange and sharing of data collected from connected vehicles will only take place where OEMs have an incentive higher than the compliance costs assumed, and only provided that their advantageous position is not challenged.

In a context where data access is completely dependant on OEMs, the general deterrents to exchange and sharing data provided by data protection and privacy regulations become more acute, as ISPs are in a "take it or leave it" situation and may be forced to accept terms of access which they would not accept under conditions of equal access to data. While ISPs face a "take it or leave it" situation, OEMs can claim adherence to data protection and privacy regulations as a

[149] Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017, p. 27.

ground to refuse the supply of data to potential competitors, including through exclusivity agreements.[150] The anticompetitive effects of data concentration to the detriment of ISPs and consumers have been widely discussed and well-proved.[151]

Leaving apart competition aspects,[152] limitations to data sharing in data protection and privacy regulations are twofold: while they serve a protective purpose, it can be argued that they can also serve to foster concentrations in data and data related markets, potentially strengthening large data controllers, to the detriment of competition –ISPs– and, ultimately, the consumer.[153] *De facto* control by OEMs of not replicable, not substitutable data collected from connected vehicles in the context of long-term contractual relationships, means ISPs do not have alternative means to access the data and are negatively affected by the general limitations to sharing personal data imposed by data protection and privacy regulations, to the extent that they foster data concentration, and are either forced to accept the terms and conditions proposed by OEMs or excluded from the market. The analysis of contractual arrangements between OEMs and ISPs for data access, including their privacy terms, could bring interesting light into this discussion.

Potential disadvantages based on the current design of the right to data portability

The effectiveness of the right to data portability to serve, under its current regulated design, as a data empowerment mechanism in the digital economy has been widely challenged.[154] Similar doubts have arisen in relation to whether this right can serve as a capable tool to mitigate "lock-in" effects in the automotive aftermarkets, based on its legal design and the uncertainties, both technical and practical, that its application and implementation bring to the table. The resulting shortages to serve as an empowerment and antitrust tool favours the *status quo,* where OEMs have exclusive control over the data collected from connected vehicles, therefore posing a disadvantage to ISPs.

---

[150] EDPS, Preliminary Opinion of the European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, 2014, p. 31.

[151] See, for instance, European Commission, *Competition policy for the digital era*, 2019; Michal S Gal, Oshrit Aviv, *The Competitive Effects of the GDPR, Journal of Competition Law & Economics*, 2020*;* or Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017.

[152] The interaction between privacy and competition law has been widely studied, especially after the Facebook decision of the German Federal Cartel Office in February 2019, first decision of a competition authority in which the protection of privacy has been explicitly taken into account in a competition law decision. See, for these purposes, Kerber, Wolfgang and Zolna, Karsten K., *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, 2020.

[153] It was precisely the lack of private incentives and insufficient public measures which justified the elaboration of ad hoc data access regimes in the automotive sector, such as the different regulations providing for access to vehicle on-board diagnostics information and repair and maintenance information that we had the opportunity to explore in this Report. The extent to which current regulations can solve the negative effects on competition, innovation and consumer choice on these markets is still under public debate and there is an open legislative process to assess whether or not to widening the scope of the mandatory access regime to new players, including car sharing, mobility as a service and insurance. See: *In-vehicle generated data – EU rules for services based on access to car data* (europa.eu).

[154] For instance, Centre on Regulation in Europe ("cerre"), *Making data Portability More Effective for The Digital Economy*, 2020; Gill, Daniel and Kerber, Wolfgang, *Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data*; or Graef, Inge and Husovec, Martin and van den Boom, Jasper, Spill-Overs in Data Governance: *The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, 2019.

From a general perspective, this right requires that each data subject actively requests the transfer of their data to another entity or delegates this exercise to a third party through prior valid authorization to exercise the right on their behalf. In any of the cases, ISPs would need to go through data subjects and to create sufficient incentives and easy mechanisms for them to exercise this right before OEMs, either directly or by delegation. As a result, a successful exercise of the right depends on data subjects' knowledge of the right, in the first place, and in their willingness to exercise it. This poses a double challenge for ISPs: firstly, current general awareness levels about the existence of this right are very low, as shown during the survey process. Taking into account that OEMs control the information that is provided to data subjects about personal data processing in the context of vehicle connectivity, assuming that OEMs do not have an incentive in raising further awareness about this right, ISPs have a huge challenge ahead in raising awareness among a collective they do not have a direct relationship with. Secondly, ISPs would need to create a sufficiently strong incentive for data subjects to be willing to assume the transaction costs associated with a data protection right request, which require, at a minimum, an investment of their time.[155]

The fact that each transfer must be actively requested or delegated illustrates how the right to data portability has not been designed for the transfer of large quantities of data, neither for a systematic or recurrent transfer, certainly not for the transfer of whole datasets. Instead, the GDPR creates a "one-off" mechanism. This crucially limits ISPs ability to use this tool as a data access tool and, where access is successfully achieved, it would prevent them from enjoying economies of scale.[156]

Other relevant technical and legal issues limit the effectiveness of this right to serve as a tool to grant access to ISPs to data held in OEMs systems, as explained below.[157] Therefore, OEMs can take advantage of this issues to limit or delay the exercise of this right, thus constraining the potential of data portability both as an antitrust and a data empowerment mechanism.

For instance, OEMs are legally obliged to provide the data in a "commonly used" format pursuant to Article 20(1) GDPR. The lack of standardization of vehicle data hinders the possibility of finding a commonly used format useful for ISPs. Many different standards and formats exist, and OEMs can choose between them following a portability request as well as to change at will between them. The right has not been designed to request technical compatibility between two or more services used by the data subject but to allow granting control through a transfer of data in machine readable format.[158]

Similar uncertainties affect the process of exercising the right: as a one-off mechanism, its recurrent exercise before the same data controller could be challenged on the grounds of it being "excessive" based on its "repetitive character", and therefore subject to a fee or directly declined, on the grounds of Article 12(5) GDPR.[159] This restricts the use cases for which data

[155] Gill, Daniel and Kerber, Wolfgang, *Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data,* pp. 6-7.
[156] Michal S Gal, Oshrit Aviv, *The Competitive Effects of the GDPR, Journal of Competition Law & Economics*, Volume 16, Issue 3, 2020, pp. 349–391.
[157] For a general approach to the limitations of this right, Article 29 Data Protection Working Party, *Guidelines on the right to "data portability"*, 2017, WP 242 rev.01. Guidelines endorsed by the EDPB.
[158] Cerre, *Making data Portability More Effective for The Digital Economy*, 2020, p. 20.
[159] Graef, Inge and Husovec, Martin and van den Boom, Jasper, *Spill-Overs in Data Governance*: *The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, 2019. TILEC Discussion Paper No. DP 2019-005, p. 20.

subjects could exercise the right in case that, for instance, they would like to provide regular access to their data in exchange of services, for instance, a recurrent transfer of data to an insurance company for the calculation of usage-based insurance rates.

Uncertain conditions in regard to standards, formats and process make difficult and costly to offer interfaces and effective processes to import data, and therefore limits ISPs ability to offer seamless, attractive data portability mechanisms to individuals discouraging the switch to a new provider.[160]

Further, the scope of the right to data portability is unclear. Article 20(1) GDPR mentions that data subjects have the right to request personal data they have provided to the data controller. The EDPB is of the opinion that personal data *provided by* the data subject includes data which has been actively and knowingly provided by the data subject (e.g., email address, postal address, user name, password, age, etc.) –"volunteered data"– as well as "observed data" provided by the data subject by virtue of the use of the service or device (e.g., search history, traffic data and location data, etc.). By contrast, it does not include "inferred data", i.e., data created by the data controller as derived from the data provided by the data subject. According to the EDPB, the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. Where in doubt, the EDPB argues for a broad interpretation of the concept of "data provided by the data subject".[161]

Despite EDPB's guidelines, the edges of the concept of "data provided by" the data subject are unclear in practice and very prone to discussion if analysed on a case-by-case basis. For instance, following a data portability request for the transfer of information about general driving habits of the driver to an insurance company, OEMs could delay or refuse the transfer of data alleging that this information entails inferred data. While in some cases OEM's allegations could be true (e.g., profiling drivers into different driving styles), this cannot prevent them from transferring raw data in most cases, so as to allow the insurer to reach its own conclusions.

Similarly, uncertainties arise when the request can affect data concerning to an individual other than the one exercising the right, which is a situation that regularly takes place recurrently in the context of connected vehicles, or in cases where the right could affect data covered by intellectual property rights and trade secrets. Article 20(4) of the GDPR is meant to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects. The limits and cases in which the transfer would adversely affect the rights and freedoms of other data subjects is a concept which leaves ample room for interpretation and, therefore, open to discussion. Furthermore, whether the transfer could affect the rights and freedoms of other data subjects the question arises as to whether the transfer should then be declined or limited or whether the data controller must offer to port at least the portion of the data that does not affect data rights of other subjects.

[160] For a detailed elaboration of the different technical complexities of exercising data portability, see Cerre, *Making data Portability More Effective for The Digital Economy*, 2020, pp. 38-49.

[161] Article 29 Data Protection Working Party, *Guidelines on the right to "data portability"*, 2017, WP 242 rev.01. Guidelines endorsed by the EDPB, pp. 9-11.

For instance, following a portability request of location data by an infotainment company, an OEM could delay the transfer of the data on the grounds that it concerns persons other than the driver or that the data is a trade secret of the OEM.

These uncertainties around the scope of the right to data portability can result in a disadvantage for ISPs, as they can be leveraged by OEMs to significantly limit or hinder the scope of the requests made by individuals and therefore limit or directly override the potential benefits that this right could have for ISPs business models and also for consumers.

Finally, as a side note, the survey process indicates that GDPR's right to data portability is not well-known and very rarely used by individuals in the context of connected vehicles. Without well-entrenched use cases around data portability for consumers to exercise it, it is reasonable to think that consumer unawareness about this right and practical uncertainties around its scope and use will remain. We face a typical chicken-and-egg problem, which will be difficult to overcome without OEMs' cooperation, which seems difficult, given the current market conditions, or without amending the current regulatory framework to address these issues.

Disadvantages posed by OEMs conditions

Placing citizens back in control over their personal data is one of the GDPR's manifested flagships. Nevertheless, in the context of connected vehicles, there are limitations in practice to the actual control that vehicle users can have over their personal data, as studied throughout this Report.

As a way of summary, deficiencies start at point of sale, where users are only informed about data processing aspects in case they actively request this information and, if information is provided, it proves to be in an incomplete and inaccurate manner. It is particularly difficult to understand the type of processing that will take place, with whom the data will be shared and the mechanisms at users' disposal to control the processing of their data. Sales and purchase agreements do not include full information about data processing aspects relating to vehicle connectivity, which users need to find by themselves in complex-to-find and complex-in-content privacy policies. According to the study conducted, OEMs generally do not recur to consent as a basis to process personal data, which means that users have less control to decide whether their data shall be processed. Other control methods, such as opting-out mechanisms, are not generally provided to users. This has been confirmed in the survey process, that has showed that respondents tend to think that data processed in the context of connected vehicles is not personal in nature, and that they do not have control over this data. Knowledge about data protection rights, particularly data portability, is rather small among those who participated in the survey.

We have identified a general root issue during this Study: information to vehicle users tends to be insufficient, incomplete, difficult to find or not provided in a timely manner.[162] The survey process confirmed that vehicle users perceive not to have received adequate information about the processing of their personal data when they purchased their connected vehicle. Information

[162] The results could bring some light into the discussion about the existence and effect of privacy-related market failures in the vehicle market, particularly in relation to privacy shortages in contracts between vehicle owners and OEMs, as well as informative asymmetries and lack of transparency. For a deeper dive into the competition's law perspective around this possible market failures, see Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017.

is at the core of the control users can have over their personal data as it contextualizes the processing and indicates how users can control it. Without timely, useful information, there are reasons to believe that vehicle users lack the means to understand the nature of the information they are sharing in the context of vehicle connectivity, the purposes behind this processing and the mechanisms at their disposal to control data processing, as suggested by the survey results.

Empirical information collected during this Study indicates that vehicle users are not capable of making meaningful individual decisions about their privacy in regard to the processing of their data in the context of vehicle connectivity, despite their manifested concern about not being in a position to control their data or decide the agents with which it is shared. This Study indicates that, in the context of car connectivity, the reason behind the existence of a "privacy paradox"[163] is that vehicle users' concern about privacy are not paralleled with mechanisms to allow them to make informed and granular decisions about their privacy and control their privacy preferences.

The EU Privacy Regulatory Framework proposes a balance of power[164] between data subjects and data controllers, whereby data controllers' necessary *de facto* control over data subjects' personal data shall be offset by legal requirements and tools at the individual's disposal.[165]

Where data subjects' control over their personal data is undermined in practice by a lack of relevant information and control mechanisms, the balance of power is broken, and data controllers gain excessive control over the personal data they held. In such a context, data protection and privacy endeavours by data controllers become a void exercise, an illusion of control for individuals, to the peril that data protection and privacy regulations may become nothing more than wishful thinking. Control is in practice retained by OEMs and not in vehicle users, despite they are the rightful owners of their personal data. Because the current *status quo* places OEMs as gatekeepers of the data, this situation turns into a disadvantage for ISPs, as it favours OEMs' perpetuation of control over the data and forecloses the chance of recurring to legal tools, particularly the right to data portability, to overcome the data bottleneck.

[163] The privacy paradox illustrates how internet users in bulk tend to express much concern in surveys about their privacy and coincide in the need and wish to protect it but at the same time generously share and dispose of their data when consuming digital services, e.g., by accepting cookies. Typically, the paradox points at two possible reasons: either users are not actually concerned about their privacy, although they declare so, or users lack real and effective means in practice to express their privacy preferences.

[164] "Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data" – Recital 11 GDPR.

[165] Michal S Gal, Oshrit Aviv, *The Competitive Effects of the GDPR*, *Journal of Competition Law & Economics*, 2020.

5

Section V:
Epilogue: conclusions and recommendations

This section presents the conclusions of the Study and provides policy recommendations on how to empower consumers through legislation.

I. Conclusions

A. Overall conclusion

The so-called "privacy paradox" illustrates how, in bulk, internet users tend to express much concern in surveys about their privacy and coincide in the need and wish to protect. However, at the same time they generously share and dispose of their data when consuming digital services, e.g., by accepting cookies.[166] Typically, the paradox points at two possible reasons: either users are not actually concerned about their privacy, although they declare so, or users lack real and effective means in practice to express their privacy preferences. The Study indicates that, in the context of car connectivity, the reason behind the existence of a privacy paradox is that vehicle users' concern about privacy is not paralleled with mechanisms to allow them to make informed and granular decisions about their privacy and control their privacy preferences.

An "as is - to be" approach serves well to illustrate this hypothesis and the relevant implications it has. Whereas the "as is" scenario describes the situation in which the car connectivity ecosystem finds itself in relation to the data protection and privacy legal framework, the "to be" scenario projects the reality into the future and estimates the issues that current conditions could bring years from now.

Starting with the "as is" approach, from a data protection and privacy point of view, the current scenario is suboptimal in many aspects. Data protection and privacy rules aim to protect individuals' fundamental rights and freedoms by establishing the conditions under which personal data might be processed and the limits in the digital environment to safeguard privacy. Most notably, these rules create tools for individuals to be in control over their personal data.

While individuals' empowerment with regard to their personal data is a cornerstone of the legal framework, the findings of this Study point at deficiencies impeding consumers from having an actual control over it. There are reasons for concern if we take into account that much of the data, if not all, that is generated and processed in connected vehicles constitutes personal data because it relates to natural persons that are identified or identifiable, regardless of whether the data might pertain to technical aspects of the vehicle. In short, shortages start at point of sale, where users are only informed about data processing aspects in case they actively request this information and, if information is provided, it proves to be in an incomplete and inaccurate manner. Sales and purchase agreements do not include full information about data processing aspects relating to vehicle connectivity, which users need to find in complex-to-find and complex-in-content privacy policies, often fragmented across different documents. Certain information is not always made available by OEMs to consumers. In a lot of the cases studied, information provided by OEMs is incomplete, insufficient and hard to find and in some of the cases studied, OEMs collect consent by default, against GDPR's requirement that consent shall be provided through a clear affirmative act. The survey process confirmed some of these aspects: most notably, vehicle users perceive not to have received adequate information about the processing of their personal data when they purchased their connected vehicle. This is in

[166] Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017, p. 15.

line with the fact that knowledge about data protection rights, particularly data portability, is rather small among those who participated in the survey.

Information is at the core of the control that users can have over their personal data as it contextualizes the processing and indicates how users can control it. Without timely, useful information, there are reasons to believe that vehicle users lack the means to understand the nature of the information they are sharing in the context of vehicle connectivity, the purposes behind this processing and the mechanisms at their disposal to control data processing, as suggested by the survey results.

Other tools that could serve for the empowerment of individuals, particularly the right to data portability, show little application in practice, based on limitations in its current legal design and functioning.

Information shortages, limited ability of the available legal tools places individuals in a situation of lack of control over their personal data. This reality is perceived and widely shared by the respondents of the survey.

A glance in the future brings further reasons for concern: in a world that is increasingly connected, the abovementioned issues are indicators of dangerous dynamics. The "to be" scenario places us in a context where all vehicles will have connectivity capabilities and are able to collect growing amounts of very heterogenous data about their users and environment. Where the recipients of the data collected from connected vehicles will have tools at their disposal for the processing of data in ways that we can barely conceive now, through the use of exponential technologies, especially artificial intelligence. The processing of data in the context of connected vehicles will increasingly involve the processing of data that is sensitive in nature.

In a context such as the described, the contour of one's privacy fades; it will be increasingly easier for organizations to identify individuals and combine information to reach insights and conclusions about them with little or no knowledge of the individual. The reason behind the wide concept of personal data in the GDPR is that increasing connectivity and enhanced processing capabilities will make individuals identifiable and prone to being subjects of the knowledge of third parties, to extents maybe unknown or unconceivable for the individual at this stage. The protection to individuals shall be able to tackle this situation and real control over their personal data is paramount for this objective.

However, in this context, lack of adequate information will very quickly turn into users' lack of control over their personal data. Opaque data collection and processing, as well as incomplete or too complex information about the processing of data in the context of connected vehicles will have the effect that consumers will lack the means to understand the impact and risks of such data processing. If not appropriately informed about the rights privacy and personal data protection regulations grant them in connection to the processing of their personal data, the idea of control will be, more than always, only theoretical. Lack of control will only deepen and consolidate if the limitations to make use of legal tools for control persist, particularly limitations derived from the current legal design and functioning of the right to data portability.

Furthermore, the future ePrivacy rules will most likely create a more flexible framework to use the connected vehicle's processing and storage capabilities or the collection of information from the vehicle without the end-user's consent, therefore potentially contributing to consumers' loss of control over their personal data. The enhanced flexibility in what regards to legal bases

other than consent brings increased complexity to the table, and it will likely derive in increasing difficulties in providing information that is easy to understand for consumers and complete at the same time.

Present issues and future dynamics recommend taking action on the realm of transparency, consent and rights to foster real control of consumers in the context of connected vehicles.

B. Conclusions from the study of the regulatory framework

The GDPR is fully applicable to data processed in the context of connected vehicles to the extent that the data involved qualifies as "personal data" under Article 4 (1) GDPR. Personal data is not limited to identifiers of the people using the vehicle such as a name, surname, national ID, etc., but also includes any information that can be linked to these persons, notably via the vehicle serial number or the vehicle licence plate number. The technical nature of vehicle data does not preclude its legal qualification as personal data, to the extent that it can be related to an identified or identifiable individual.

Unless otherwise anonymised, data from connected vehicles will most likely qualify as personal data in relation to the organizations directly collecting and using the data, as well as organizations indirectly collecting and using the data to the extent that they have the information necessary to identify the person or can lawfully obtain sufficient additional data to link the information to a person and therewith identify that person.

As for the e-Privacy Directive, Article 5(3) is applicable to the collection of data from connected vehicles to the extent that: (i) the vehicle qualifies as "terminal equipment" under Directive 2008/63/CE; (ii) and the data is collected through a publicly available electronic communication service. Article 5(3) e-Privacy Directive shall take precedence over Article 6 GDPR with regards to the activity of "storing or gaining access to information" collected in the context of the connected vehicles.

There is an open debate on the question of the legal basis applicable to subsequent processing operations involving the information gathered accessing the end-user's device. According to the European Data Protection Board ("**EDPB**"), as a general rule, where consent is necessary pursuant to Article 5(3) e-Privacy Directive, for subsequent processing operations, data controllers cannot rely on one of the lawful basis in Article 6 GDPR other than consent, especially in relation to tracking and profiling processing activities. This opinion is not necessarily followed by the industry, especially in the advertising ecosystem.

Nonetheless, the EDPB acknowledges that service providers can rely on the performance of a contract as a legal basis as per Article 6(1)(b) GDPR for subsequent processing operations if certain conditions are met. In addition, the EDPB acknowledges that in some cases, and subject to transparency and additional safeguards, tracking and profiling may also be permissible to prevent fraudulent use of the services offered.

As for the ePR Proposal, the draft text, currently under negotiation between the European Parliament and the Council of the EU, will bring relevant modifications to the legal framework on privacy of electronic communications and therefore to the connected car ecosystem.

Generally, in the context of vehicle connectivity, the ePR Proposal, in any of its versions, creates a more flexible landscape for OEMs and ISPs to use the connected vehicle's processing and

storage capabilities or the collection of information from the vehicle without the end-user's consent. However, the enhanced flexibility in what regards to legal bases other than consent is balanced out by an increased complexity of the regulatory framework. This complexity will also derive in increasing difficulties in providing information that is easy to understand by consumers and complete at the same time.

C. Conclusions related to consumer awareness and challenges and opportunities

Placing citizens back in control over their personal data is one of the GDPR's manifested flagships. However, findings derived from the research conducted point at deficiencies impeding consumers from having an actual control over their personal data. Empirical evidence from the MS exercises and the review of contracts and privacy policies points that recommendations by regulators regarding data processing in connected vehicles are, to a large extent, being not well accommodated in the process of acquiring a vehicle.

On the one hand, the MS exercises suggest that the level and transparency and clarity of the information about vehicle data processing provided at the points of sales can clearly be improved in many instances.

Overall, the MS exercises revealed a significant lack of information about vehicle data collection and processing at the point of sales visited.

While some information about vehicle connectivity is provided at the point of sale, this information exclusively concerns the connectivity functionalities available and the related user's experience. However, it does not cover the implications of such functionalities, i.e. the underlying vehicle data processing.

In the best-case scenario, limited information about vehicle data processing aspects was provided but only after inquiring by the Mystery Shopper. Even in these cases, the sales representatives were reluctant, unwilling or unprepared to provide general information about vehicle data processing or elaborate on any of the questions raised.

No additional information resources (such as privacy policies, privacy notices or references to websites where information in this regard can be obtained) – that could assist consumers in understanding the implications of data processing deriving from connected vehicle functionalities – were provided either, even after showing an interest in these issues.

In relation to the review of contractual/informative documents relevant to the processing of personal data in the context of connected vehicles, some of the findings in this area include:

- Information about the processing of personal data by connected vehicles is not always made available by OEMs to consumers.
- Information provided by OEMs to consumers the processing of personal data by connected vehicles is often fragmented across different documents.
- The information provided by OEMs show sometimes deficiencies regarding data sharing aspects.
- In a lot of the cases studied, information provided by OEMs is incomplete, insufficient and hard to find.

- In some of the cases studied, OEMs collect consent by default, against GDPR's requirement that consent shall be provided through a clear affirmative act.

Results of the survey process confirmed some of the findings reached in the MS exercises and the review of the contracts and data protection policies. Most respondents answered that they have not given consent for the processing of the data collected in the context of vehicle connectivity. Likewise, most of the respondents who have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer declared that they were not informed at all about the fact that information would be collected from the vehicle and the purposes for which the information could be used or about how to control the information collected from the vehicle (e.g. how to make a request or complaint, who to contact, etc.).

The lack of information, which has been identified as a shortage during the vehicle acquisition process, can accrue to the general little awareness about data protection rights is never shared by more than half the respondents. While respondents are generally aware that they have information rights and the right to lodge a complaint, but numbers decrease relevantly when asked about awareness of their right to data portability to not to be subject to automated individual decision-making. The overall low numbers on awareness can be a plausible reason behind the very low number of respondents who have ever exercised a data protection right, especially portability.

Consumers expressed concerns about lack of control over their personal data. Most respondents declared to feel comfortable sharing information from their vehicle with different entities but only to the extent that they can choose with whom, and what type of data to share, and stop doing it at any given time.

Legal framework and OEMs conditions might pose disadvantages for innovation by ISPs. Despite being a framework for the protection of the fundamental rights of individuals, the data protection and privacy legal framework also creates limitations constraining the voluntary sharing of data. Further, these limitations might be leveraged to avoid, limit or control the sharing of personal data and foster data concentration, entrenching an advantageous market position for certain player (i.e., OEMs) based on better, even exclusive access to data and the control over the terms and conditions under which data is shared in the market, with adverse effects on ISPs.

Although data portability could have great impact on market and society, the current legal design of the right to data portability under Article 20 GDPR and uncertainties around its application in practice challenge the ability of this tool to serve as a mechanism to put an end to the current situation where OEMs are gatekeepers of the data collected from connected vehicles, hence proving ineffective for serving as a data empowerment or antitrust tool, to the detriment of ISPs.

Regarding contracts and privacy policies, this section studies how there are limitations in practice to the actual control vehicle users have over their personal data processed, and this can discourage seamless access or transmission of data to ISPs, with a negative effect on them.

II. Policy recommendations

The aim of the EU Privacy Regulatory Framework is to protect individuals' rights and freedoms in relation to their privacy and the protection of their personal data. The cornerstone of this

legal framework is to empower users by providing tools that allow them to be in control of their personal data. However, as studied, findings in this Report point at deficiencies impeding consumers from having an actual control over the personal data they share in the context of car connectivity. As explained throughout this Report, this deficiencies are mostly related to (i) shortages in the way that vehicle users receive information about data processing aspects in relation to the processing of vehicle data, and (ii) shortages in relation to the actual control vehicle users have over the personal data shared through their vehicle, as a result of the information shortages, the bypassing of consent for the processing of personal data (e.g. the activation by default of consent for geolocation purposes) and the limitations of the data portability right to serve as an empowerment tool.

A. A comprehensive framework to entrench vehicle users' control over their personal data

At this point it is relevant to refresh the recommendations provided by main European data protection regulators, studied in section II, subsection I.C ("What regulators say?"). When it comes to the processing of personal data in the context of connected vehicles, regulators defend a privacy-by-design approach, i.e., privacy settings that can be easily modified to empower users and give them control over their data. For instance, the EDPB advocates for the implementation of profile management systems within the vehicle allowing each vehicle user to provide individual consents and to save their preferences and ensure that data subjects are well informed and can change the settings associated with their personal data at any time, as well as carrying out the processing of vehicle data locally.

The CNIL proposes that "In-In" data flow scenarios (i.e., the data collected is not transmitted outside the vehicle, remaining under the control of the user) shall be prioritized to the extent possible, to guarantee data privacy at a maximum and keep users in control of their data.[167] User control in this scenario would mean that personal data is not transmitted to the service provider and that the local storage of data relating to geolocation is deactivated by default, except for real-time data-processing. Only those functionalities that are strictly needed for the vehicle to operate would be active by default. In the absence of real-time processing, users would be provided with the option to easily access and delete usage-data (e.g., using a button inside the vehicle or using one's smartphone or using the onboard computer). Finally, it is paramount to inform users about the data that is likely to be stored locally, as well as the data-deletion options.

In "In-Out" data flows scenarios, the CNIL proposes that users are provided with mechanisms to deactivate geolocation at any time, providing that geolocation functionalities are only activated when the user launches a functionality that requires the vehicle's location to be known, and not by default or continuously once the vehicle is started. Where geolocation is active, vehicle users would be informed of this fact, for instance by using icons. Accurate information about the purpose of the processing for each functionality relying on data extracted from the vehicle should be provided.

[167] CNIL, *Compliance package for a responsible use of data in connected cars*, 2017.

The discussion around how data in the connected vehicle can be accessed revolves around three technical models or architectures: (1) Data server platform (including the Extended Vehicle concept); (2) In-vehicle interface (3); and On-Board Application platform.[168]

- **Data server platform**: under this architecture, all data extracted from the vehicle is transferred and stored on a central data server outside of the vehicle. There are three possible implementations of this model: (i) The Extended Vehicle, which is the *status quo* where the data server platform is controlled by the OEM and where ISPs can access the data only through the central data server. An additional derivative of this model is the "neutral server".[169] (ii) The Shared Server, where the central server is operated by a neutral party or a consortium representing both OEMs and ISPs, rather than relying solely on OEMs for the operation of the central server (which technically could work similar to the central server in the extended vehicle concept). (iii) Finally, the B2B Marketplace, which would create a platform between the vehicle and service providers fed by OEMs' back end servers, but maintained by a service provider that would facilitate access by the market.

- **On-board application platform**: "An on-board application platform allows unified deployment of applications on the Human-Machine Interface ("**HMI**") of the vehicle whilst also allowing hosting of applications on the HMI using the vehicle internal resources". [170] In short, the vehicle would function as the platform through which applications and services receive and send data.

  In comparison with the Extended Vehicle solution, this model provides vehicle users with actual control over data. It proposes a scenario in which the vehicle user can decide which apps or which service providers can use the data extracted from the connected vehicle as the data is primarily processed locally at the vehicle. An instance of this type of architecture is the Secure On-Board Telematics Platform ("**S-OTP**").[171]

- **In-vehicle interface**: this model would rely on a physical connector or physical interface to make data available outside the vehicle. An instance of this model already exists in the market: the OBD-II interface, which allows access to standardised datasets such as emissions, fault codes etc.

  Similarly to what happens in the on-board application platform model, under this architecture the data is primarily stored in the vehicle and it is the vehicle user the one controlling the transfer of data to parties outside the vehicle, although the degree of control over the data transferred is lesser than in the on-board application platform model.[172]

From a theoretical standpoint, all the technical solutions for the sharing of data in the context of connected vehicles described hereabove are equally able to comply with data protection and

[168] For a detailed description of each model, as well as the different issues that each of them propose, see C-ITS TRL, *Access to In-Vehicle Data and Resources* – Final Report (2017), pp. 29 -49; Tuvit - M. Bartsch, A. Bobel, Dr. B. Niehöfer, M. Wagner, M. Wahner, *On-Board Telematics Platform Security*, 2020, p. 11-15; FIA Region I and others, *Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach*, 2021.
[169] Tuvit - M. Bartsch, A. Bobel, Dr. B. Niehöfer, M. Wagner, M. Wahner, *On-Board Telematics Platform Security*, 2020, p. 11.
[170] C-ITS TRL, *Access to In-Vehicle Data and Resources* – Final Report (2017), p. 32.
[171] Tuvit - M. Bartsch, A. Bobel, Dr. B. Niehöfer, M. Wagner, M. Wahner, *On-Board Telematics Platform Security*, 2020 and FIA Region I and others, *Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach*, 2021.
[172] C-ITS TRL, *Access to In-Vehicle Data and Resources* – Final Report (2017), p. 42.

privacy regulations.[173] Of course, the compatibility of each technical solution with the legal framework is based on the relevant stakeholders complying with the obligations laid down in the legislation. However, the fact that none of the technical solutions are theoretically incompatible with the legal framework does not mean that some solutions can be more adequate than others to satisfy the legislation's manifested objectives.

Based on the consolidated criteria of the main data protection regulators in the EU, compliance with data protection and privacy regulations requires the provision of tools for the actual control of personal data by vehicle users and a privacy-by-design approach. In this regard, technical solutions which primarily rely on local processing rather than the default transfer of personal data outside the vehicle, on the one hand, and which provide vehicle users with real, effective control over the sharing of personal data with third parties, including with OEMs, on the other, are equally compatible with the EU Privacy Regulatory Framework but significantly better suited to satisfy the legislation's objectives based on the degree of control over personal data that they provide to vehicle users.

For these purposes, both the on-board application platform and the in-vehicle interface models provide the features necessary to ensure vehicle users have control over the data processed by the vehicle, as well as limit potential privacy-related issues by mostly local-based data processing. Based on the degree of control vehicle users can have over their personal data,[174] the on-board application platform seems to be the preferred option, in particular through the instance of a S-OTP.[175]

Recent legislative developments in the EU show that a technical solution such as the S-OTP is in line with the intentions of the EU legislator to create tools to ensure individuals retain full control over their data and allow them to decide who it is shared with, as well as to achieve a competitive data economy. In particular, the Data Governance Act Proposal ("**DGA Proposal**")[176] will promote the availability of data and build a trustworthy environment to facilitate, among other objectives, the creation of innovative new services and products. The DGA Proposal creates a framework to foster a new business model – data intermediation services – that will provide a secure environment in which companies or individuals can share data. For companies, these services can take the form of digital platforms, which will support voluntary data-sharing between companies or facilitate the fulfilment of data-sharing obligations set by law. By using these services, companies will be able to share their data without fear of its being misused or of losing their competitive advantage.

---

[173] *Ibid*., p. 140.

[174] *Ibidem.* Other technical reasons also advocate the on-board application platform over the in-vehicle interface, most notably the lower bandwidth of the latter, see C-ITS TRL, *Access to In-Vehicle Data and Resources* – Final Report (2017), p. 41.

[175] This interpretation is in line with the preferred model for competition purposes. See, for instance, C-ITS TRL, *Access to In-Vehicle Data and Resources* – Final Report (2017), p. 42; and Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017.

[176] Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final. On 30 November 2021, the Council of the European Union and the European Parliament reached a provisional political agreement on the Data Governance Act and, as a result, an updated text was published and submitted to Coreper (Council's Permanent Representatives Committee) for endorsement: Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 14606/21, Interinstitutional File: 2020/0340(COD).

For personal data, such services and their providers will help individuals exercise their rights under the GDPR. This will help data subjects have full control over their data and allow them to share it with a company they trust. This can be done, for example, by means of novel personal information management tools, such as personal data spaces or data wallets, which are apps that share such data with others, based on the data holder's consent.

Policy recommendation: It is advisable to adopt a sector-specific framework defining a technical solution which allows an easy and effective implementation of the principles of the GDPR in the context of the connected vehicle.

From a strict data protection and privacy law perspective, having regard to the GDPR's manifested objectives and the criteria shared by the main EU data protection regulators, technical architectures other than the data server platform (i.e. on-board application platform and in-vehicle interface) are better suited for a proper processing and transfer of personal data in the context of connected vehicles because (i) they increase vehicle users' control over their personal data, and (ii) mitigate possible privacy-related risks by recurring to local processing within the vehicle instead of on external servers.

Accordingly, the sector regulation to be adopted should impose a technical architecture which ensures the foregoing: local data processing and users' actual control over vehicle data.

From a data protection and privacy point of view, the sector regulatory framework should put an emphasis on the compliance obligations, particularly in regard to information and personal data security aspects (basic risk analyses and DPIAs where necessary), that stakeholders involved shall comply with. The standardised procedures that service providers shall pass to be able to access the data held in the vehicle under the S-OTP model provide for an opportunity to develop and allocate these obligations. Firstly, the inherent limitations to provide information through the vehicle's HMI recommend for the provision of specific guidelines on how to provide this information, including through the provision of standardised icons to facilitate user understanding, in line with GDPR's indications. Secondly, the complexities in relation to the selection of appropriate legal basis for the processing of personal data, especially in regard to the interaction between the GDPR and the ePrivacy Directive/ePR Proposal (when adopted), make recommendable to set a common position regarding compatible purposes for which service providers can use personal data obtained via the S-OTP. Finally, the complexity of the processing operations than can derive from this setup call for the development of DPIA templates for the stakeholders involved, ensuring a consistent and coordinated methodology for risk management across the actors with access rights. To ensure the proper allocation of data protection responsibilities from the outset, the role and functions of the automotive gateway administrator[177] shall be determined from the outset and be standard for all service providers with access to the platform. Finally, it would be necessary to define the scope of the data that would be made available through the platform. A broad interpretation of the data that shall be made available is recommended to ensure that vehicle users' control over their data is not inadequately restricted, and also taking into

[177] Gaspare Fiengo; Giulia Lovaste, 2021, *Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform*, Legal Study, 2021, p. 7.

account the legitimate interests of OEMs, particularly regarding the protection of business secrets, as well as the rights of data subjects other than the vehicle user.

These solutions alternative to the data server platform have the virtue of overcoming most of the shortages linked with the legal design and functioning of the data portability right as it would function, in effect, as a data portability mechanism adapted to the particular context of the connected vehicle.

The S-OPT would meet the above-mentioned objectives (effective application of the GDPR principles through local processing and actual users' empowerment) and is considered to be the best suited and most effective architecture for these purposes by ISPs.

Therefore, the adoption of this technical architecture through sector-specific rules would be a valid and appropriate mechanism.

Legislation in this line would need to be reached outside of the EU Privacy Regulatory Framework, for instance through amendments to the Type Approval Regulation or even through the approval of *ad hoc* rules, which shall be accompanied by the amendment to the Type Approval Regulation's data sharing obligations.

B. Partial improvements **to the current framework**

Whether the recommendation provided above might require a process of length, other short to middle-term solutions can be considered to work prior to or in parallel to the effective implementation of a S-OTP model.

Recommendations for enhanced transparency

As studied, there are several points of failure in what refers to transparency in the consumer journey of a person buying a connected vehicle. At point of sale, users are only informed about data processing aspects in case they actively request this information and, if information is provided, it tends to be provided in an incomplete and inaccurate manner. Sales and purchase agreements do not include full information about data processing aspects relating to car connectivity, which users need to find in complex privacy policies, often fragmented across different documents. Some information is not always made available to consumers and in a lot of the cases studied information provided to consumers is incomplete, insufficient and hard to find. The results to the survey points at a general lack of knowledge about data protection rights, especially concerning data portability, as well as a perception shared by most respondents that they have not been provided with adequate information about car connectivity or about their rights in connection therewith.

MS exercises show that official dealers have very different approaches to providing information to consumers. One of the brands (see the study about Brand 4 both in **Appendix III** and **IV** for a combined approach of information practices at its physical and digital point of sales) has specifically tackled information challenges by inserting specific information aids throughout the consumer journey: at the point of sale stage, they inserted a big banner located at the middle of the point of sale, that the sales representative used to provide information on vehicle geolocation functionalities, remote vehicle lock, and monitoring of gas consumption and needed repairs. That same brand shows efforts in their digital channels by making privacy policies regarding the connected vehicle easily accessible in its website and warning consumers wishing

to sell their vehicles to reset all the information saved by the vehicle before selling it. The combination of similar information icons at the physical and digital point of sale indicates that this is a corporate effort of the OEM to enhance information practices across its dealership network, including its web shop. Even in this case, some shortages were found in its information processes to a big extent due to the inherent complexity of the processing of personal data behind connected vehicles. Outside of this particular case, coordinated approaches to the provision of information between the dealer and the OEM were not explicit, having the effect of deteriorating the information and resources available for consumers in regard to the processing of personal data by connected vehicles.

> **Policy recommendation**: a coordinated approach between dealers and OEMs to provide the mandatory information on personal data processing is highly recommended based on the results of the MS exercises. On the other hand, the very different approaches between OEMs to the way information is articulated and the general complexity of the content of the documents studied call for a coordinated action also across OEMs.
>
> An effort for increased harmonisation, availability and understandability of privacy policies and other information touchpoints can be achieved in the form of soft laws or guidelines. A coordinated EU approach would be preferrable given the multijurisdictional nature of data processing in most of the cases, for instance by an update or revisit of the guidelines already provided by pan-EU data protection regulators, such as the EDPB and the EDPS, especially focusing on information shortages and remedies in the context of car connectivity.
>
> Notwithstanding the above, intervention at a legislative level could be recommended for the provision of standardised icons in order to provide mandatory data protection information in an easily visible, intelligible and clearly legible manner, as well as a meaningful overview of the intended processing in the specific context of car connectivity. This can be achieved through delegated acts by the Commission regarding the icons and the procedures for providing such icons. This initiative would incardinate into the wider context of the GDPR transparency frameworks. A cooperative approach between national data protection authorities individually or jointly through the EDPB can be an interim solution while EU-wide icons are developed.[178]

Recommendations for better control through consent and data portability

In the context of car connectivity, GDPR's consent requisites mean that vehicle users shall decide if personal data can be provided and to whom for a specific purpose that was made explicit to the individual before the processing starts. It means that withdrawing consent shall be as easy as it was to give consent. Accordingly, organisations collecting and processing personal data, especially OEMs as gatekeepers of the information extracted from the connected vehicle, shall provide for easily mechanisms for each vehicle users to provide consent and withdrawing it at any given time.

Our Study showed that collection of geolocation data sometimes happens "by-default" prior to having obtained consent from the consumer, i.e., collection happens once the app is running

[178] See, for instance, the Italian data protection authority's proposal for this purpose: https://edpb.europa.eu/news/national-news/2021/easy-privacy-information-icons-yes-you-can-italian-dpa-launches-contest_en.

unless deactivated by the user (see brands 3 and 7 in **Appendix IV** for further reference). This is contrary to GDPR's provisions and entails a processing of data of sensitive nature.

Additionally, the Council version of the eRP Proposal provides for several additional legal basis to process data from the connected vehicle without consent from the vehicle user. Notably, the ability to process data for compatible purposes with those for which the data was collected could foster new practices to bypass consent.

> **Policy recommendation**: clear guidelines regarding the interaction between the ePrivacy Directive and the GDPR, as well as the requirements and aspects to observe when obtaining consent in the context of connected vehicles already exist. The existence of infringements shall be dealt with by national data protection authorities under the competencies laid down by law. The eventual adoption of the ePR Proposal and the likely innovative elements it will bring to the table, combined with the particularities of the connected vehicle ecosystem will call for updated guidelines on consent and even specific guidelines in the context of car connectivity.

As presented in length throughout this Report, the potential benefits of the right to data portability are undermined by the legal design and functioning in practice of this right. A summary of the most prominent include limitations to serve as a tool for the transfer of large quantities of data or for a systematic or recurrent transfer, lack of commonly used formats for the processing of vehicle data and existence of several arguments at OEMs disposal to limit or delay the exercise of this right as derived from its nature as a "one off" mechanism (its recurrent exercise before the same data controller could be challenged on the grounds of it being “excessive” based on its “repetitive character”) and from several uncertainties regarding the scope of the right. It is worth mentioning that the right to data portability in the GDPR did not necessarily have in mind a context such as the one provided by the ecosystem around connected vehicles where a single party has sole access to data collection.

Recent legislative developments in the EU can bring interesting insights to the analysis of data portability as an empowerment and antitrust tool, if appropriately designed. In this regard, the Digital Markets Act Proposal (“**DMA Proposal**”)[179] has sought to alleviate unwanted consequences of the considerable economic power concentrated into large providers of core platform services, which might be designated as “gatekeepers”.

In spite of the differences between OEMs and gatekeepers under the DMA Proposal, their situation is not dissimilar in some respects. For instance, OEMs, like large online platforms, benefits from access to and control of vast amounts of data collected from connected vehicles. Likewise, OEMs become intermediaries between vehicle users and third-parties (ISPs), as it happens with regard to very large online platforms and business users leveraging the platform to connect with end-users. When providing data driven services to vehicle users, ISPs are in the need to access data held by OEMs and as a result, OEMs, similarly to those online platforms, have the ability to connect service providers with many end-users. Under these circumstances, OEMs can leverage their central position and access to data to prioritize the portfolio of their services, either acting as an aftermarket service provider, or through its network of official partners. This creates an integrated ecosystem to which third-party providers of such ancillary

[179] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.12.2020 COM(2020) 842 final 2020/0374 (COD).

services do not have access, at least not under equal conditions, and where OEMs, similar to some providers of core platform services, play a dual role as platform operator and service provider. Therefore, they have the ability to foreclose competition for automotive aftermarkets, to the detriment of consumer choice, innovation and competition.

Precisely one of the unwanted consequences deriving from the concentration of power in gatekeepers is the restriction of users' ability to effectively port their data. As a result, among the measures chosen to mitigate this power concentration, the DMA Proposal calls for effective and immediate access to the data that business and end-users provide or generate in the context of their use of the relevant platform services of the gatekeeper, in a structured, commonly used and machine-readable format.[180]

> **Policy recommendation**: the specialties of the car connectivity ecosystem and potential benefits this right could bring justify the design of a sector-specific regulatory solution to establish an effective right to data portability.
>
> The solution shall establish the main traits of the right, the technical requisites for data and service interoperability, standard solutions for safety and security and standard processes for its practical application. This would imply a regulatory package similar to the one proposed for the DMA Proposal which could be achieved, for instance, through amendments to the Type Approval Regulation or through the approval of *ad hoc* legislation.
>
> In line with the DMA Proposal, vehicle users shall be provided with tools to facilitate their exercise of data portability including by the provision of continuous and real-time access to the data provided or generated in the context of their use of the connected vehicle, in a structured, commonly used and machine-readable format. The scope of the right should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that end-users can port that data in real time effectively, such as for example through high quality application programming interfaces.
>
> In relation the traits and scope of the right, the new design shall provide for a mechanism to ensure the right can affect large datasets and regulate clear conditions for recurrent exercise of the right. A broad definition of the data under scope is recommended to ensure that vehicle users' control over their data is not inadequately restricted, and also taking

[180] In this regard, Article 6(1)(h) establishes that gatekeepers shall "provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access". Recital 54 DMA Proposal adds that gatekeepers shall grant "effective and immediate access to the data they [business users and end-users] provided or generated in the context of their use of the relevant core platform services of the gatekeeper, in a structured, commonly used and machine-readable format. This should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that business users and end users can port that data in real time effectively, such as for example through high quality application programming interfaces. Facilitating switching or multi-homing should lead, in turn, to an increased choice for business users and end users and an incentive for gatekeepers and business users to innovate". It should be noted that this obligation is susceptible to be further specified by the European Commission with the aim to define the form, content and other details of the technical measures that gatekeepers shall implement in order to ensure compliance.

into account the legitimate interests of OEMs, particularly regarding the protection of business secrets, as well as the rights of data subjects other than the vehicle user.

I

Appendix I: Arts. 4 And 8 EPR Proposal comparative table

Article 4a (Article 9 VEC & EP) Consent		
1. The definition of and conditions for consent provided for ***under Articles 4(11) and 7 of*** Regulation (EU) 2016/679/EU shall apply.	1. The definition of and conditions for consent provided for ***in*** Regulation (EU) 2016/679/EU shall apply.	(1) The provisions for consent provided for under Regulation (EU) 2016/679/EU shall apply to natural persons and, mutatis mutandis, to legal persons.
2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using ***the appropriate*** technical ***settings of a*** software ***application enabling access to the internet***.	2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed ***or withdrawn*** by using technical ***specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1. When such technical specifications are used by the user's terminal equipment or the*** software ***running on it, they may signal the user's choice based on previous active selections by him or her***. ***These signals shall be binding on, and enforceable against, any other party.***	(1a) Paragraph 1 is without prejudice to national legislation on determining the persons who are authorised to represent a legal person in any dealings with third parties or in legal proceedings.
3. ***End-users*** who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 ***and be reminded of this possibility at periodic intervals of 6 months,*** as long as the processing continues.	3. ***Users*** who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3)***, point (b) of Article 8(1) and point (aa) of Article 8(2)*** shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 as long as the processing continues.	(2) Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8 (1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.
	3 a. Any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and the protection of personal data.	(2aa) Consent directly expressed by an end-user in accordance with Paragraph (2) shall prevail over software settings. Any consent requested and given by an end-user to a service shall be directly implemented, without any further delay, by the applications of the end user's terminal, including where the storage of information or the access of information already stored in the enduser's terminal equipment is permitted.
		(2a) As far as the provider is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).
		(3) End-users who have consented to the processing of electronic communications data in accordance with this Regulation shall be reminded of the possibility to withdraw their consent at periodic intervals of [no longer than 12 months], as long as the processing

		continues, unless the end-user requests not to receive such reminders..
Article 8 - Protection of end-users' terminal equipment information		
The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the ***end-user*** concerned shall be prohibited, except on the following grounds:	1. The use of processing and storage capabilities of terminal equipment and the collection of information from ***end-users***' terminal equipment, including about its software and hardware, other than by the ***user*** concerned shall be prohibited, except on the following grounds:	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or	(a) it is ***strictly*** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or	(a) it is necessary for the sole purpose of providing an electronic communication service; or
(b) the ***end-user*** has given his or her consent; or	(b) the ***user*** has given his or her ***specific*** consent; or	(b) the end-user has given consent; or
(c) it is necessary for providing an information society service requested by the ***end-user***; or	(c) it is ***strictly technically*** necessary for providing an information society service ***specifically*** requested by the ***user***; or	(c) it is strictly necessary for providing a service specifically requested by the enduser; or
(d) if it is necessary for ***web audience*** measuring, provided that such measurement is carried out by the provider of the ***information society service requested by the end-user.***	(d) if it is ***technically*** necessary for measuring ***the reach of an information society service requested by the user***, provided that such measurement is carried out by the provider***, or on behalf*** of the ***provider, or by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or***	(d) if it is necessary for the sole purpose of audience measuring, provided that such measurement is carried out by the provider of the service requested by the enduser, or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested provided that, where applicable, the conditions laid down in Articles 26 or 28 of Regulation (EU) 2016/679 are met; or
2. The ***collection*** of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:		
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	***(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:***	(da) it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud or prevent or detect technical faults for the duration necessary for that purpose; or
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the	***(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;***	(e) it is necessary for a software update provided that:

end-user of the terminal equipment can take to stop or minimise the collection. ***The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.*** 3. The information to be provided pursuant to ***point (b) of*** paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	***(ii) the user is informed in advance each time an update is being installed; and*** ***(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;*** ***(d b) in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:*** ***(i) the employer provides and/or is the user of the terminal equipment;*** ***(ii) the employee is the user of the terminal equipment; and*** ***(iii) it is not further used for monitoring the employee.*** ***1a. No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of processing or storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.*** 2. The ***processing*** of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the ***sole*** purpose of establishing a connection ***requested by the user***; or	(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user, (ii) the end-user is informed in advance each time an update is being installed, and (iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or (f) 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). (g) where the processing for purpose other than that for which the information has been collected under this paragraph is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia: (i) any link between the purposes for which the processing and storage capabilities have been used or the information have been collected and the purposes of the intended further processing; (ii) the context in which the processing and storage capabilities have been used or the information have been

	(aa) the user has been informed and has given consent; or	collected, in particular regarding the relationship between end-users concerned and the provider;
	(ab) the risks are mitigated.	(iii) the nature the processing and storage capabilities or of the collecting of information as well as the modalities of the intended further processing, in particular where such intended further processing could reveal categories of data, pursuant to Article 9 or 10 of Regulation (EU) 2016/679;
	2a. For the purpose of points (d) of paragraph 1 and (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:	
	(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting; and	(iv) the possible consequences of the intended further processing for endusers;
	(b) the processing shall be limited in time and space to the extent strictly necessary for this purpose; and	(v) the existence of appropriate safeguards, such as encryption and pseudonymisation.
	(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and	(h) Such further processing in accordance with paragraph 1 (g), if considered compatible, may only take place, provided that:
	(d) the users shall be given effective possibilities to object that do not affect the functionality of the terminal equipment.	(i) the information is erased or made anonymous as soon as it is no longer needed to fulfil the purpose,
	2b. The information referred to in points (aa) and (ab) of paragraph 2 shall be conveyed in a clear and prominent notice setting out, at the least, details of how the information will be collected, the purpose of processing, the person responsible for it and other information required under Article 13 of Regulation (EU) 2016/679, where personal data are collected. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679.	(ii) the processing is limited to information that is pseudonymised, and
		(ii) the information is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.
	3. The information to be provided pursuant to paragraph 2***b*** may be provided in combination with standardized icons in order to give a	(i) For the purposes of paragraph 1 (g) and (h), data shall not be shared with any third parties unless the conditions laid down in Article 28 of Regulation (EU) 2016/697 are met, or data is made anonymous.

	meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	2. The collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment shall be prohibited, except on the following grounds: a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing or maintaining a connection; or b) the end-user has given consent; or c) it is necessary for the purpose of statistical purposes that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose, d) it is necessary for providing a service requested by the end-user. 2a. For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice is shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. 2b. For the purpose of paragraph 2 points (b) and (c), the collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied. 3. The information to be provided pursuant to paragraph 2a may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

		4. The Commission shall be empowered to adopt delegated acts in accordance with Article 25 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

II

Appendix II: Survey Fact Sheet

I. Survey objective

As a part of this Study, a survey has been conducted for the purpose of getting an understanding on consumer awareness, sensitivity and attitudes towards data sharing and processing in the context of vehicle connectivity, as well as awareness on data protection and privacy rights in this context.

In particular, the survey aimed at understanding: (i) which challenges consumer face when exercising their rights under the GDPR (e.g., data portability); (ii) what are the consumer sensitivity on sharing vehicle data; and (iii) what is the degree of consumer awareness with regard to vehicle data.

II. Methodology

A. Study design

The survey has been conducted from August to November 2021 across several jurisdictions in 3 European regions, i.e.:

- **Southern region** (with respondents in France, Italy and Spain).
- **Continental region** (with respondents in Belgium, Germany, Netherlands and Switzerland).
- **Northern region** (with respondents Denmark, Norway and UK).

The survey has been conducted in more than one language in certain countries to avoid language restrictions and misinterpretations and to reach as many consumers as possible. In particular, in Belgium, the survey was distributed in two languages, Flemish and French. In Switzerland, the survey was distributed in three languages French, German and Italian.

The survey was designed using Qualtrics application and distributed online through FIA's network of mobility clubs.

The survey was not addressed at a targeted audience. In the light of the objectives expressed above, participation was open to any kind of respondent profile and not only to drivers, on the believe that non-drivers can also provide valuable insights on awareness, sensitivity and attitudes towards data sharing and processing in the context of vehicle connectivity.

The jurisdictions were selected based on the capabilities of FIA's mobility clubs in each region as well as on the interest to include non-EU jurisdictions.

B. Analysis

The survey is structured in two main building blocks: (i) awareness, perceptions and attitudes towards data sharing and connectivity; and (ii) data empowerment. Within these blocks, each survey question is aiming at achieving a specific insight in relation to the objectives expressed above. These insights were defined at the time of designing the survey and have been extracted from the survey's results.

Awareness, perceptions and attitudes towards data sharing and connectivity

Data sharing and connectivity are two essentially related concepts. Questions 1 to 10 aim to understand different aspects connected to awareness, perceptions and attitudes towards data sharing and processing in the context of connected vehicles.

Question 1 assesses the percentage of respondents who own connected vehicles. Question 2 aims at measuring the degree of awareness on vehicle connectivity. Question 3 assesses consumer awareness on data sharing in the context of vehicle connectivity and question 4 analyses consumers' perspective about the nature of the information processed and shared in the context of connected vehicles (whether personal, non-personal or both). Question 5 seeks to understand consumers' perceptions on the agents that may receive the data collected from connected vehicles.

Question 6 contrasts four different attitudes towards data sharing. Question 7 assesses awareness about monetization related to data sharing. Question 8 analyses consumers' attitudes towards sharing in exchange for obtaining services.

Question 9 analyses whether users perceive they have control over data shared by their vehicles. If users perceive not to be in control over this data, question 10 assesses the degree of concern related to this lack of control.

Data empowerment: information, consent and data protection rights

Question 11 and question 12 explore whether users perceive to have given consent and, if so, in what format, to the processing of their personal data in the context of connected vehicles.

Question 13 and 14 assess whether consumers perceive they have been provided with information regarding the processing of data in the context of vehicle connectivity and regarding the ways in which they can control the data collected in this context.

Questions 15 and 16 aim to understand consumers' perceptions on the choices they have to control the data collected in the context of connected vehicles, where these choices coincide with the rights that data protection regulations grant to individuals. Question 17 asks whether consumers have exercised any of the aforementioned rights and, where the answer is positive, question 18 measures which specific request was made in each case. Where answer is negative, question 19 explores the reasons why consumers have not exercised any request.

The survey ends by providing users with the chance to provide comments to the survey.

III. Number of responses

Southern region	721
Continental region	1292
Northern region	2876

IV. Questionnaire

1/21 If you owe or drive a vehicle regularly, do you know in which year it was manufactured?

- Yes (please write year below)
- No
- DK/NA[181]

2/21 Did you know that, for some years now, vehicles are equipped with sensors and connectivity features (including its own SIM card and Internet connection) which allow them to connect with other cars, devices, infrastructure, services, etc.?

- Yes
- No

3/21 Did you know that connected vehicles (vehicles equipped with sensors and connectivity features) can collect information from the vehicle and share this information with different entities?

- Yes
- No

4/21 What type of information do you think is being collected and shared?

- Non-personal
- Personal
- Both
- DK/NO

5/21 Do you think information collected from the connected vehicle is shared with any of these entities? (Please select all that apply)

- Car manufacturers
- Vehicle repair services and maintenance
- Public authorities
- Entertainment services
- Hospitality services (restaurants, hotels, cafés, etc.)
- Gas stations
- Parking providers
- Insurance companies
- Emergency services
- All of the above
- None of the above
- Other (please write below)

6/21 Would you be comfortable sharing information from your vehicle with these entities in exchange of services or functionalities that could benefit your driving experience or safety?

- Always
- Yes, but only if I can choose with whom, and what type of data is being shared, and stop doing it, at any given time
- Yes, as long as no personal information is shared
- Never

7/21 Did you know that car manufacturers make money out of the information collected from vehicles?

- Yes
- No

8/21 Would you be willing to share information collected from your vehicle to receive any of the following services? (Please select all that apply)

- Early detection of necessary maintenance and repairs, with detailed monitoring and recommendations
- Suggestions provided by your vehicle about nearby parking locations, repair and maintenance garage, charging spots or petrol stations
- Alerts provided by your vehicle of dangerous driving conditions ahead

[181] Do not know/do not answer.

- Information provided by your vehicle about the traffic and suggestions about best routes
- Information provided by your vehicle about nearby scenic spots, restaurants, tourist attractions, stores or hospitality services
- Adjustments on insurance rates, based on the driving behaviour showed by your vehicle
- Information about offers, discounts, coupons of commercial establishments based on location, season or other elements
- Fuel consumption monitoring for recommendations and discounts in petrol stations
- On-demand vehicle washing available where your vehicle is parked
- Delivery of fuel to your vehicle
- All of the above
- None of the above
- Other (please write below)

9/21 Do you think drivers have control over the information collected and shared by their vehicles?

- Yes
- No
- DK/NO

10/21 How concerned are you about drivers not having control over the information collected and shared by vehicles?

- Very concerned
- Somewhat concerned
- Not too concerned
- Not concerned at all
- DK/NO

11/21 Do you acknowledge having authorized the use of vehicle data by the vehicle manufacturer and/or other entities?

- Yes
- No
- N/A

12/21 How did you authorize the use of vehicle data by the vehicle manufacturer and/or other entities?

- I gave verbal authorization
- I ticked a check box
- I signed a document
- Other (please write below)

13/21 If you have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer, were you informed about the fact that information would be collected from the vehicle and the purposes for which the information could be used?

- I was duly informed
- I was informed partially or the information was not clear enough to fully understand it
- I was not informed at all
- N/A

14/21 If you have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer, were you informed about how to control the information collected from the vehicle (e.g. how to make a request or complaint, who to contact, etc.)?

- I was duly informed
- I was informed partially or the information was not clear enough to fully understand it
- I was not informed at all
- N/A

15/21 Do you think drivers can request any of the following to the entities receiving information collected from the vehicle? (Please select all that apply)

- To let the driver access or provide the driver with a copy of the information
- To update the information when inaccurate
- To erase the information when no longer necessary
- Not to use or to stop using the information in certain circumstances (e.g. for marketing communications)
- All of the above
- None of the above
- DK/NO

16/21 Do you think drivers can do any of the following? (Please select all that apply)

- To request to be informed about who will use the information and how it will be used
- To request to have the information sent to other organizations at their request
- To request that an employee review a decision made by an automated system without any human intervention
- To submit a complaint to a public authority if there is something wrong with the way the information is used or shared
- All of the above
- None of the above
- DK/NO

17/21 Have you ever made any of the requests listed in questions 15 and 16 (e.g. request access to the information collected from the car, its update or erasure, the transfer of this information to other organization, etc.)?

- Yes
- No

18/21 Which request did you make?

- To access to the information collected from the vehicle and/or a copy of it
- To update the information collected from the vehicle
- To erase the information collected from the vehicle
- Not to use or to stop using the information collected from the vehicle in certain circumstances (e.g. for marketing communications)
- To have the information collected from the vehicle sent to other organization
- That a human reviewed a decision made solely by an automated system
- Submitted a complaint before a public authority
- Other (please write below)
- All of the above

19/21 Did you achieve the result you were looking for?

- Yes, completely
- Yes, but only partially
- No, I did not receive an answer
- No, the answer came too late
- No, the process was too complicated
- Not at all

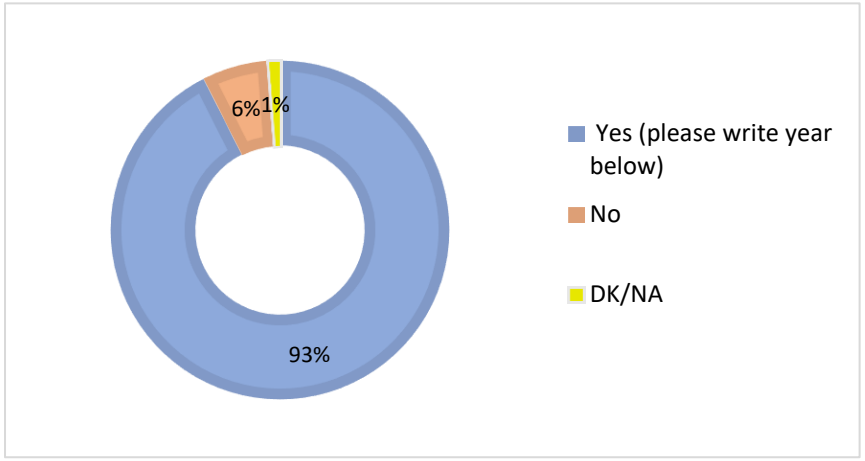
20/21 Why have you never requested any of the above?

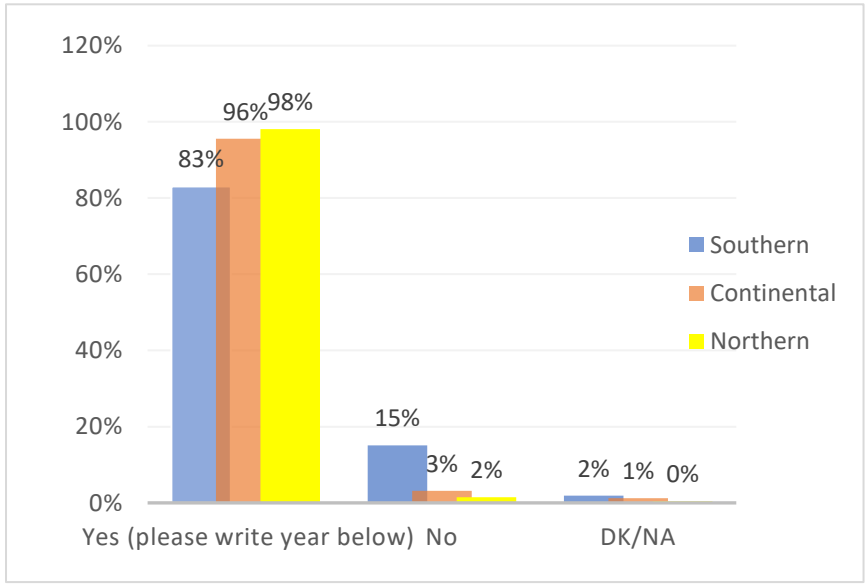
- I did not want or did not have the need to make any of those requests
- I would have liked to but I did not know that I could make any of those requests
- I would have liked to but I did not know how to make it or who to contact
- Other (Please write below)

21/21 Do you have any comments?

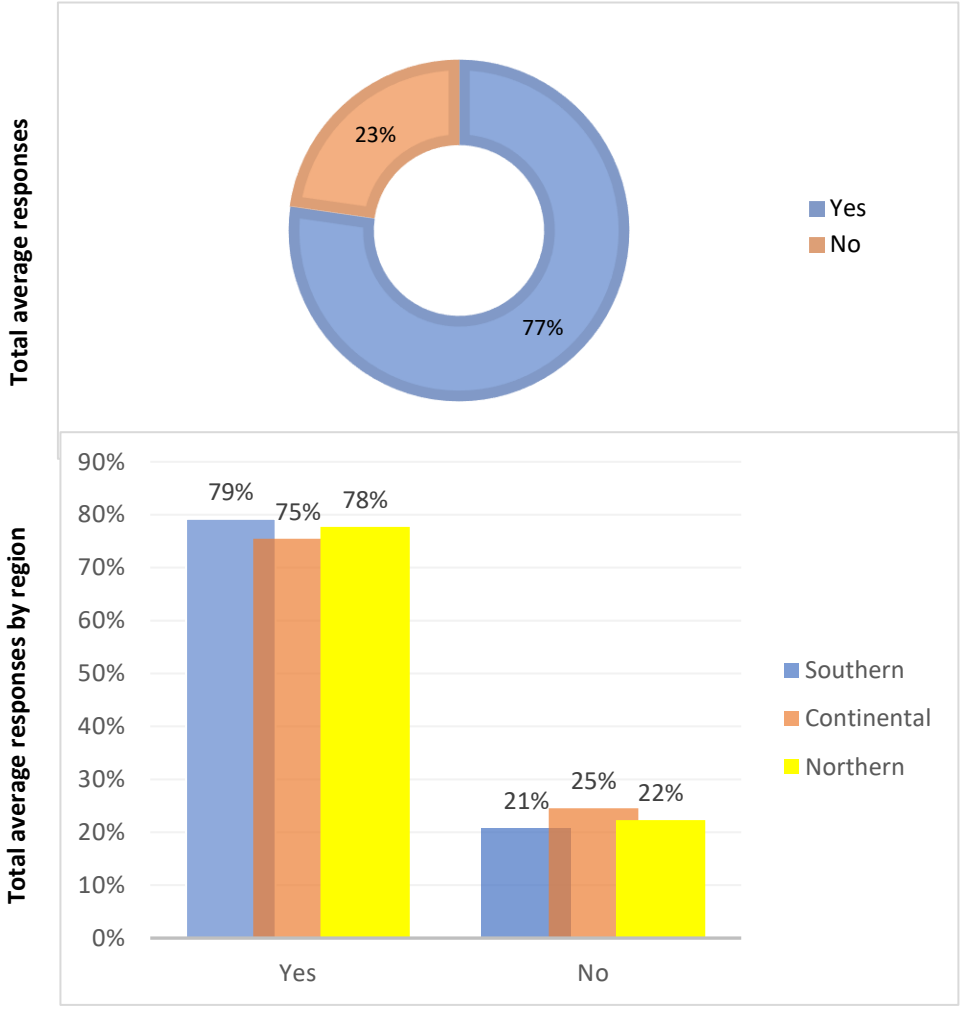
IV. Survey results

1/21 If you owe or drive a vehicle regularly, do you know in which year it was manufactured?

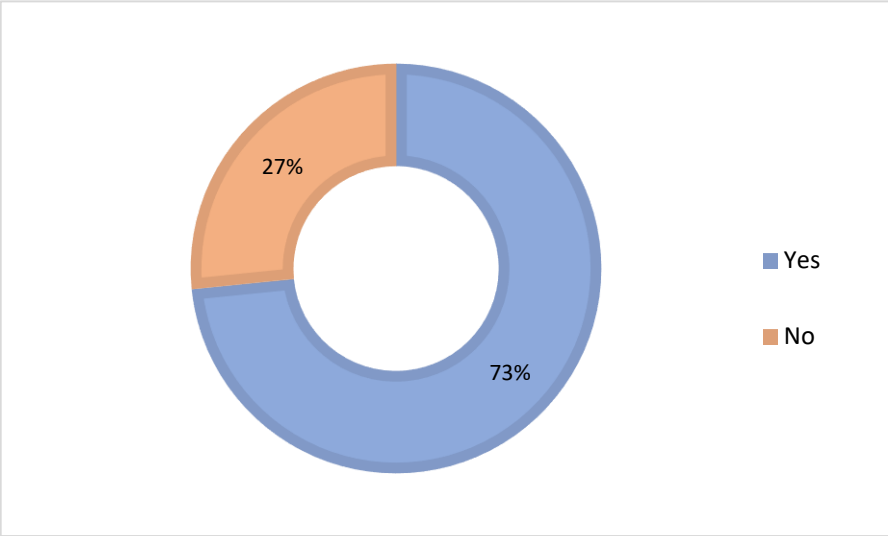


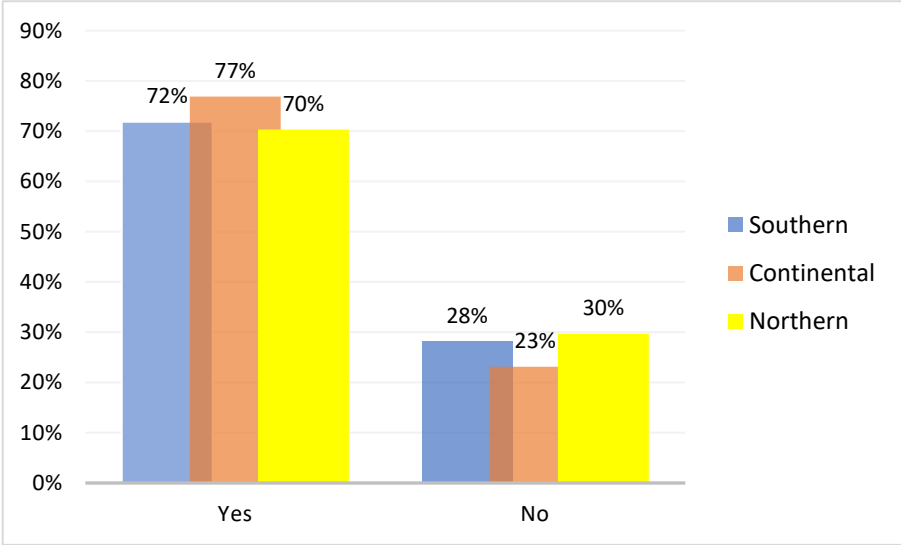


2/21 Did you know that, for some years now, vehicles are equipped with sensors and connectivity features (including its own SIM card and Internet connection) which allow them to connect with other cars, devices, infrastructure, services, etc.?

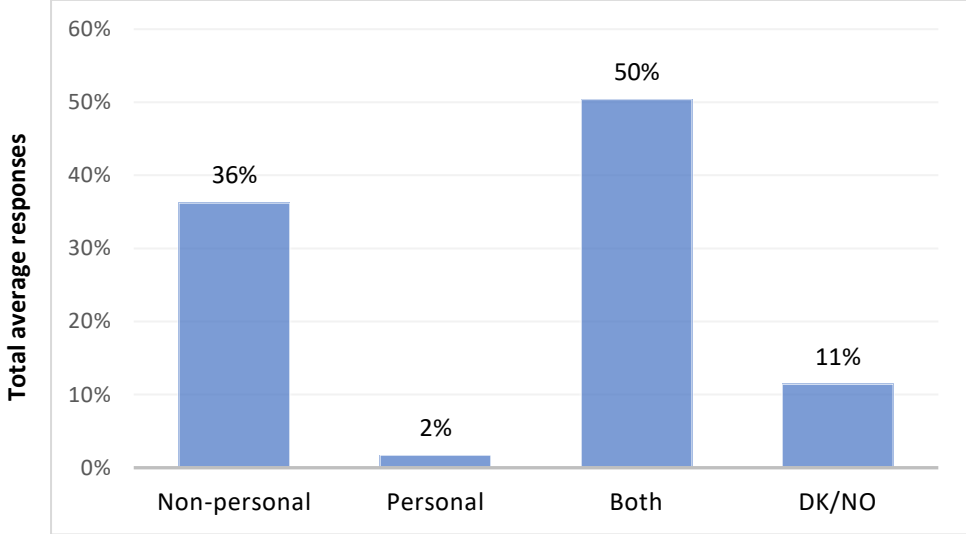


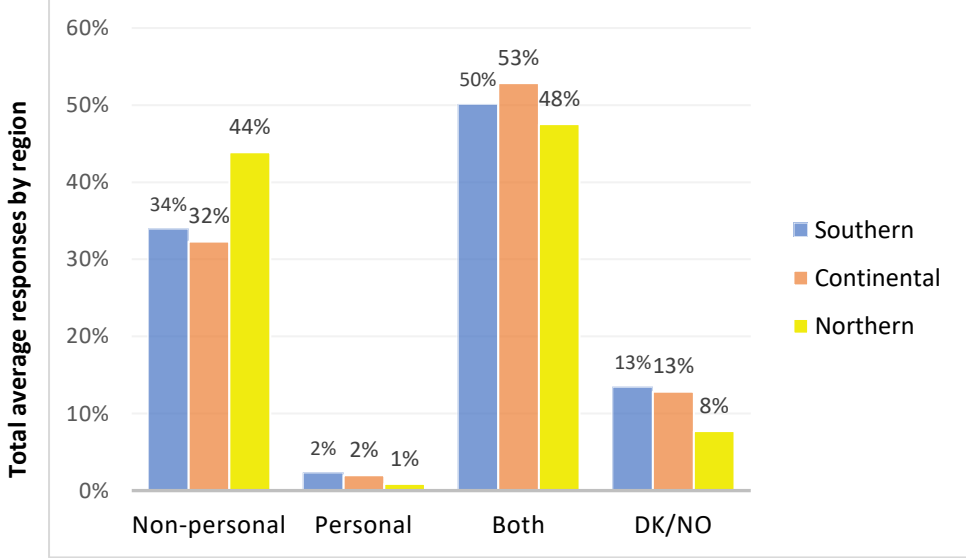
3/21 Did you know that connected vehicles (vehicles equipped with sensors and connectivity features) can collect information from the vehicle and share this information with different entities?



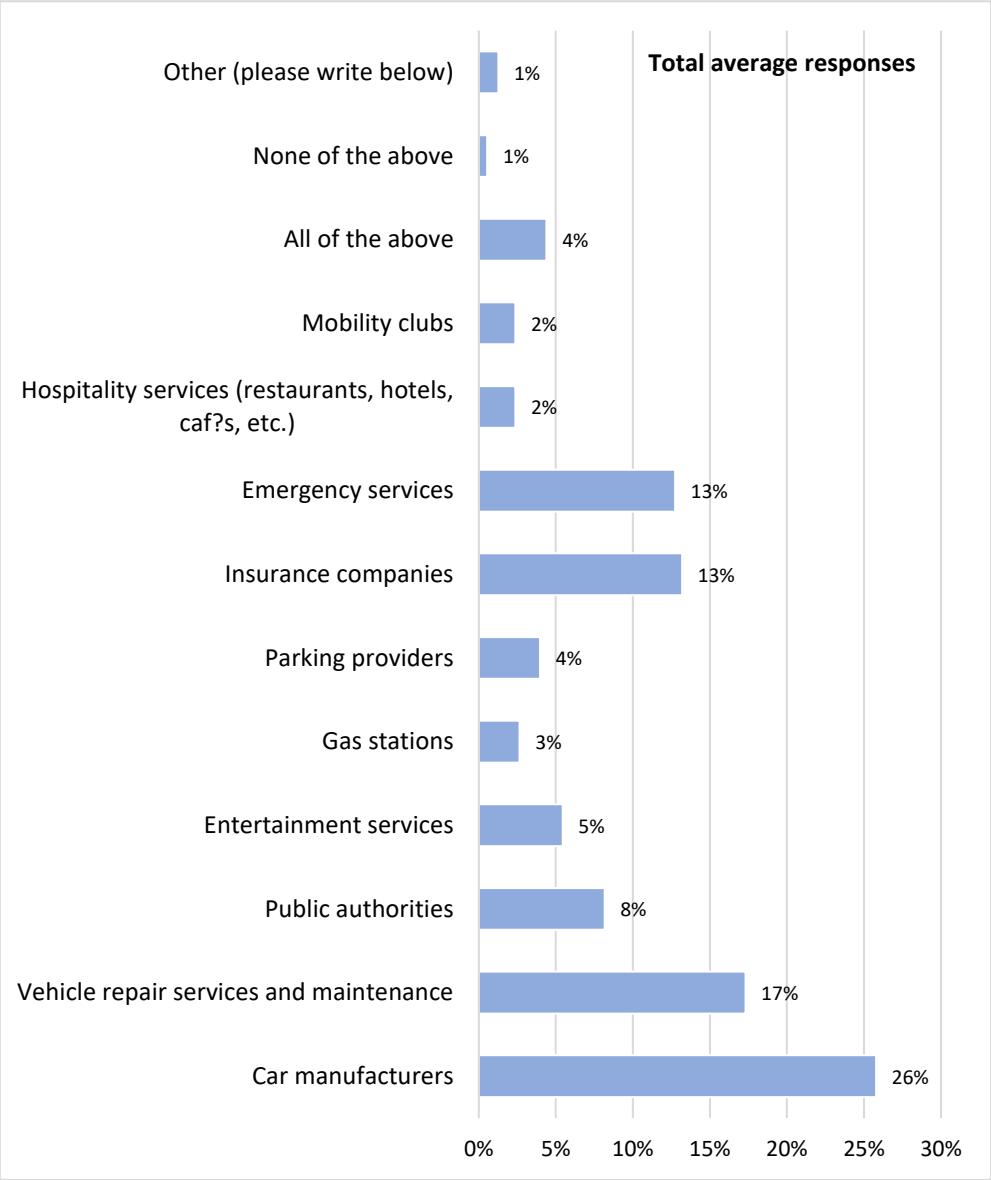


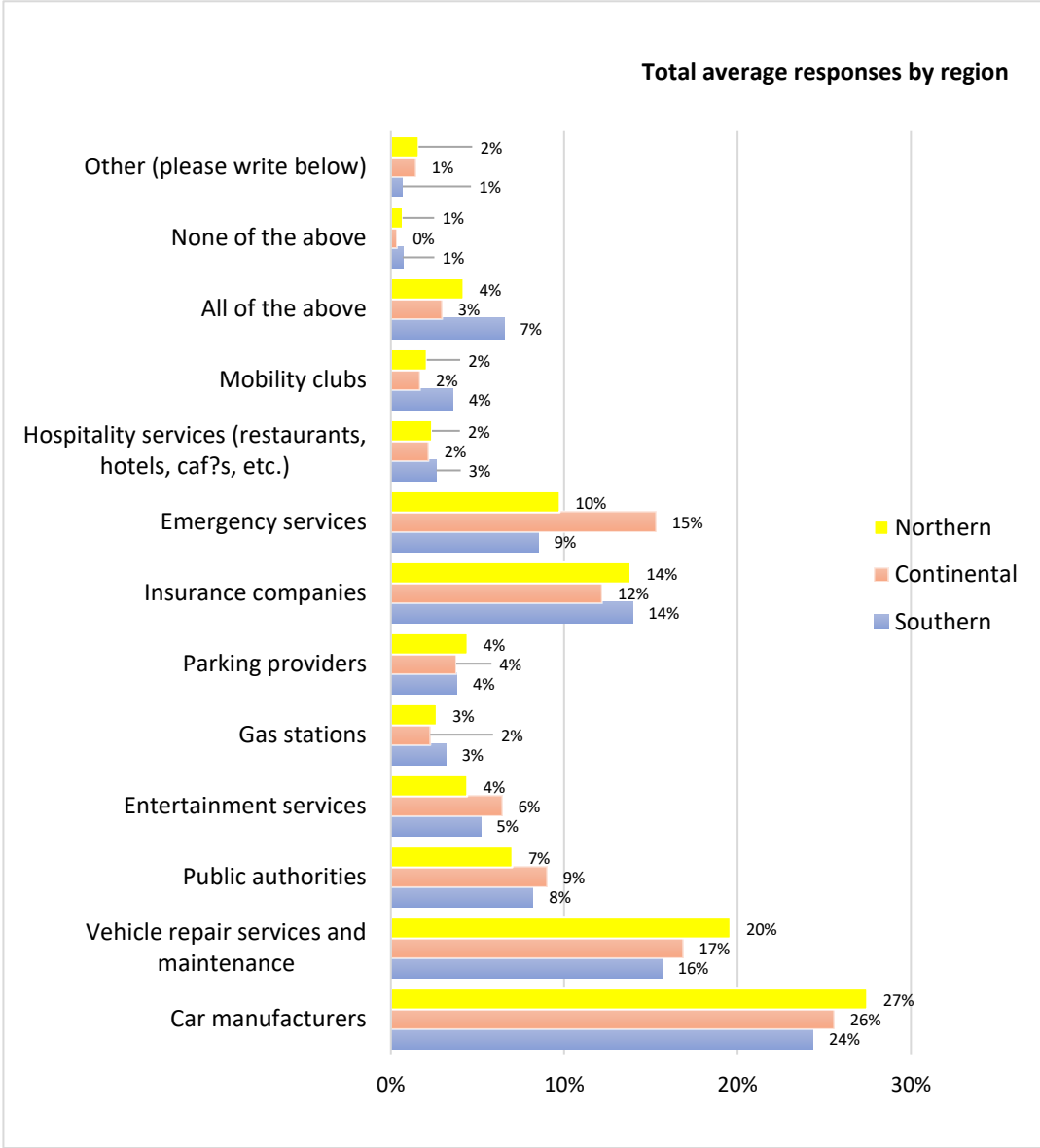
4/21 What type of information do you think is being collected and shared?



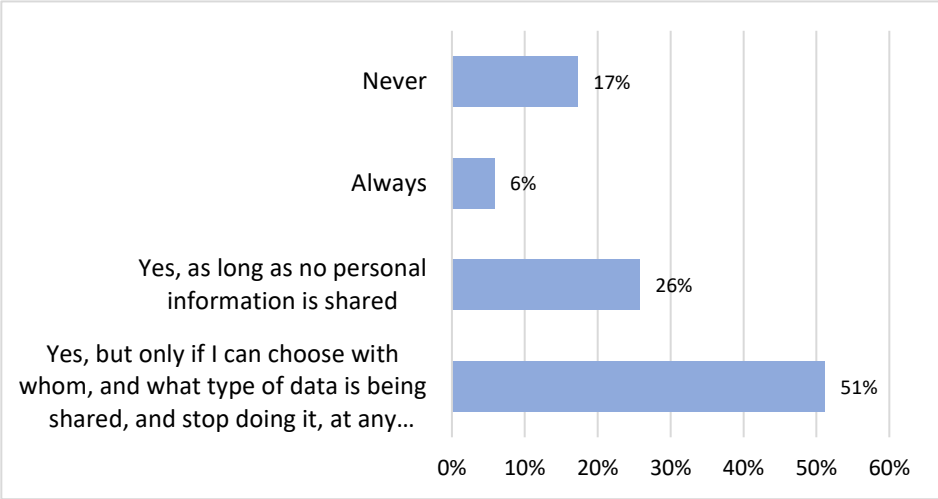


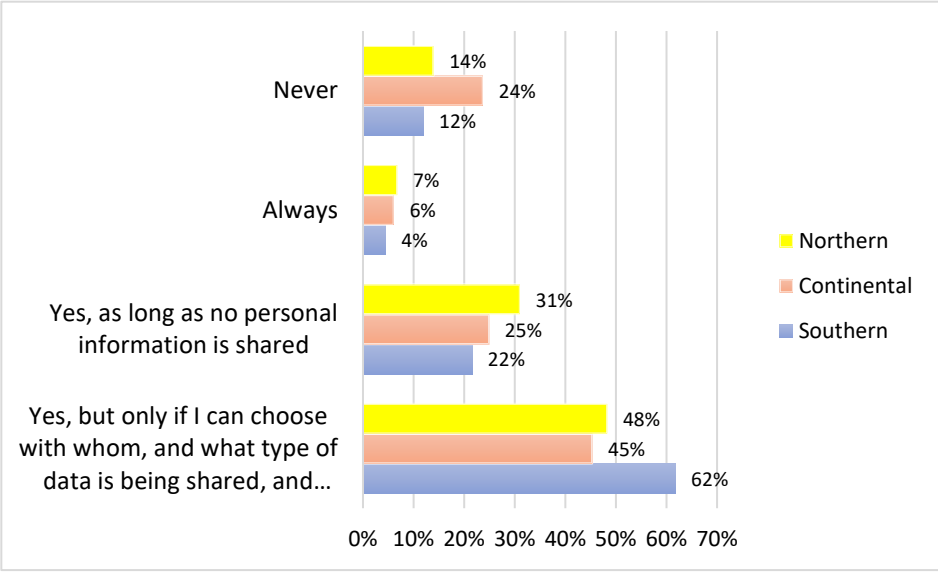
5/21 Do you think information collected from the connected vehicle is shared with any of these entities? (Please select all that apply)



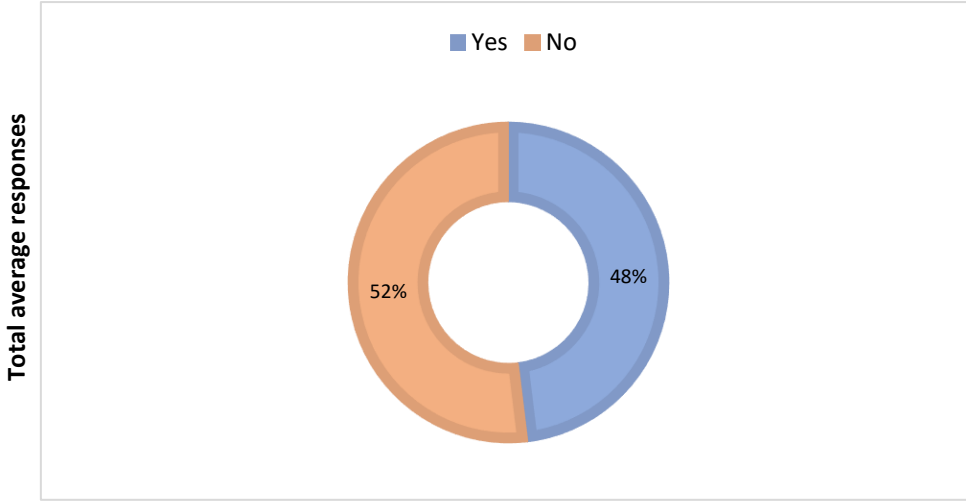


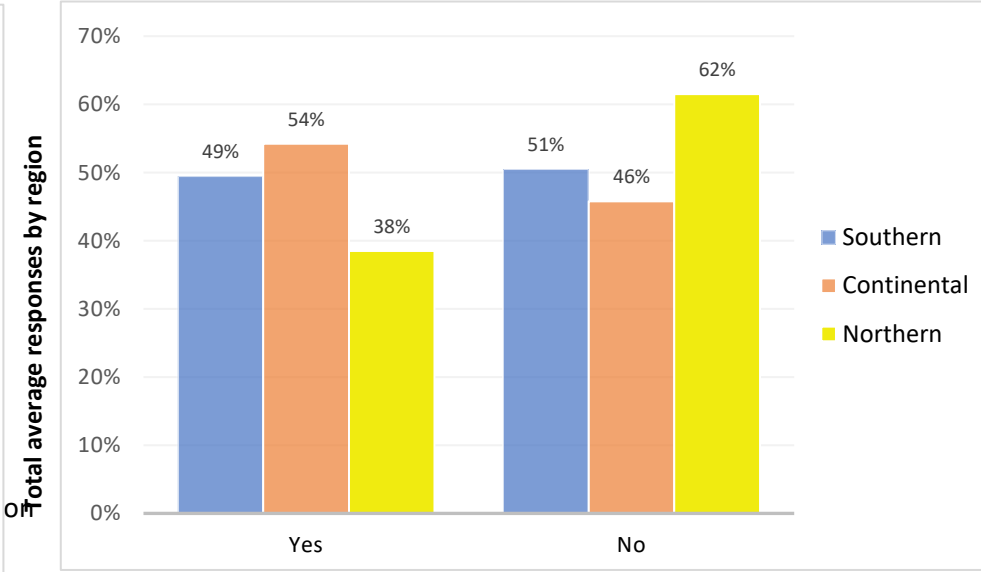
6/21 Would you be comfortable sharing information from your vehicle with these entities in exchange of services or functionalities that could benefit your driving experience or safety?



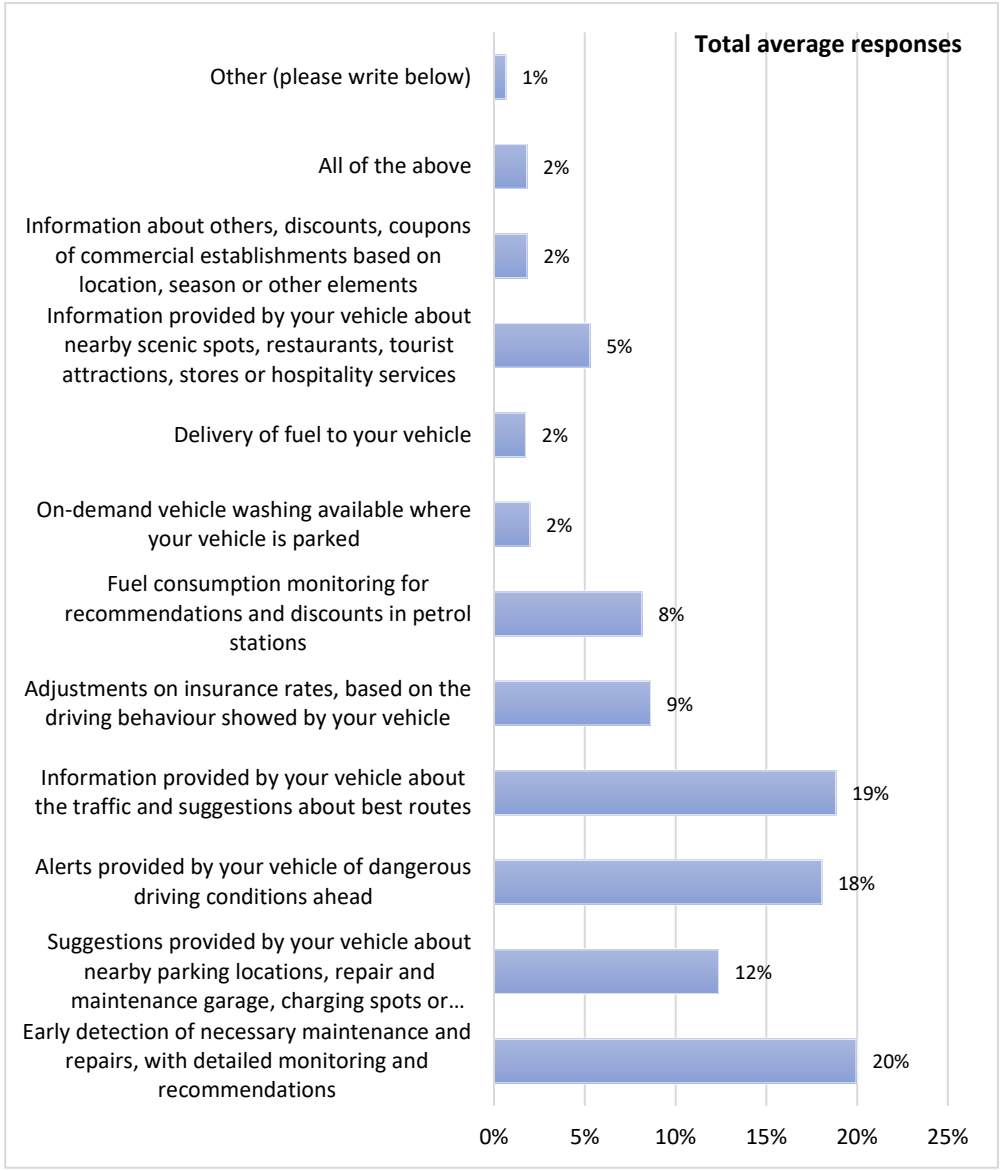


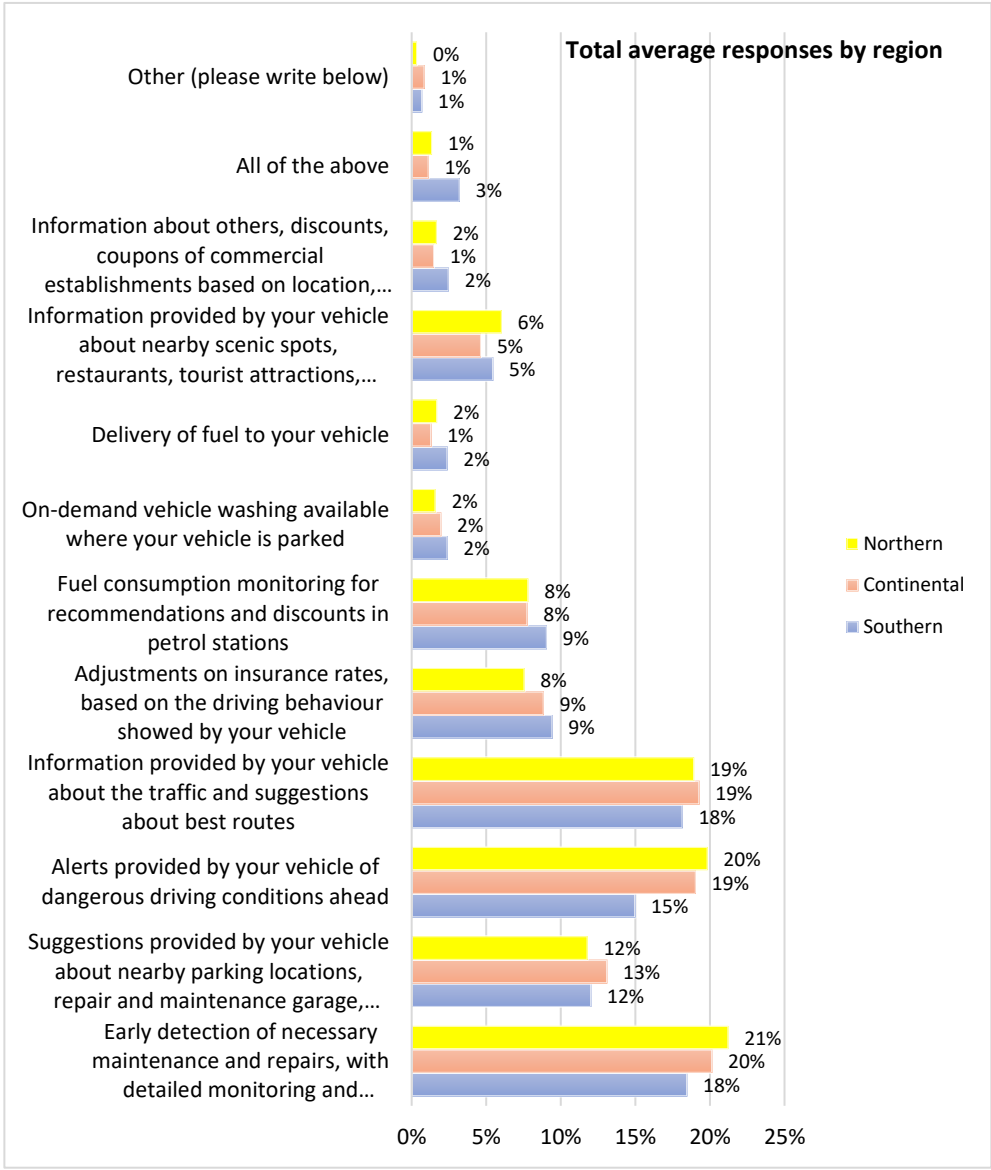
7/21 Did you know that car manufacturers make money out of the information collected from vehicles?



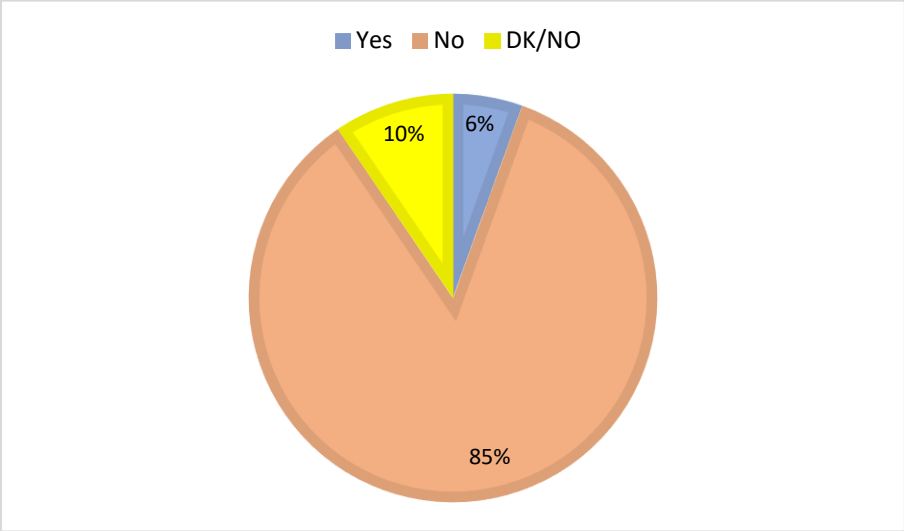


8/21 Would you be willing to share information collected from your vehicle to receive any of the following services? (Please select all that apply)

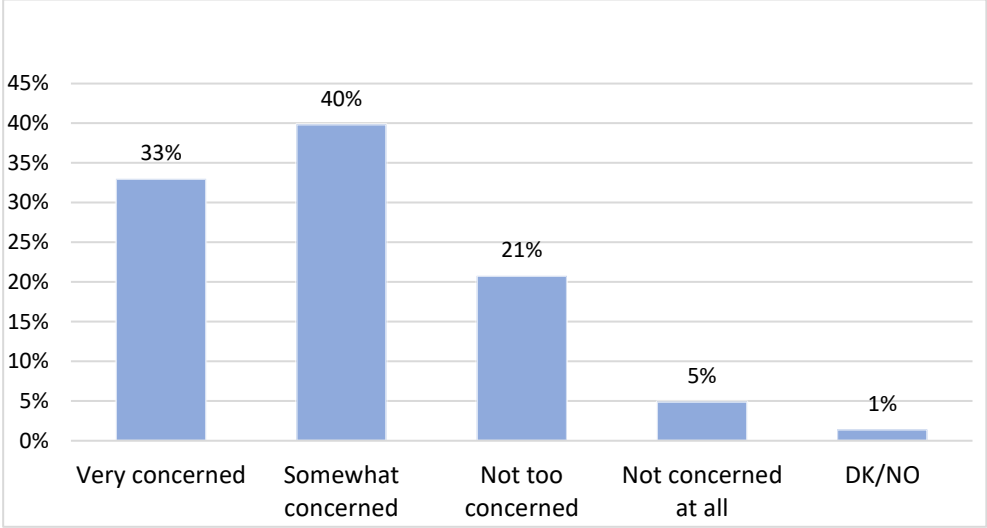


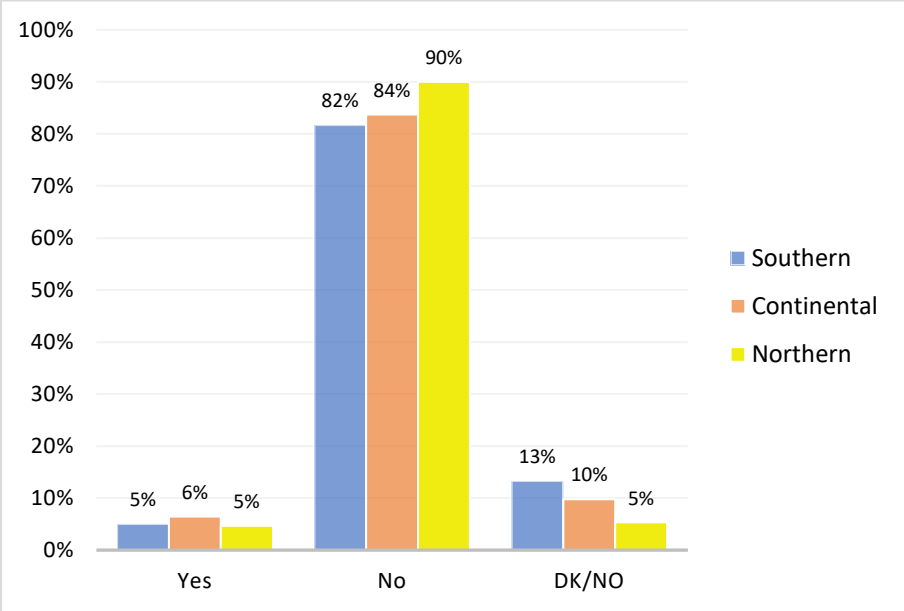


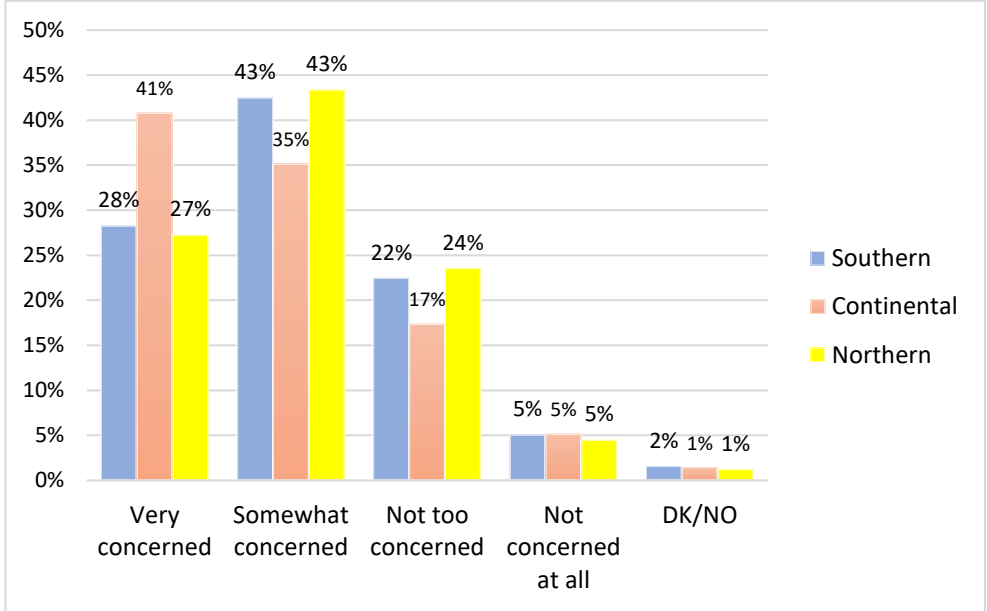
9/21 Do you think drivers have control over the information collected and shared by their vehicles?



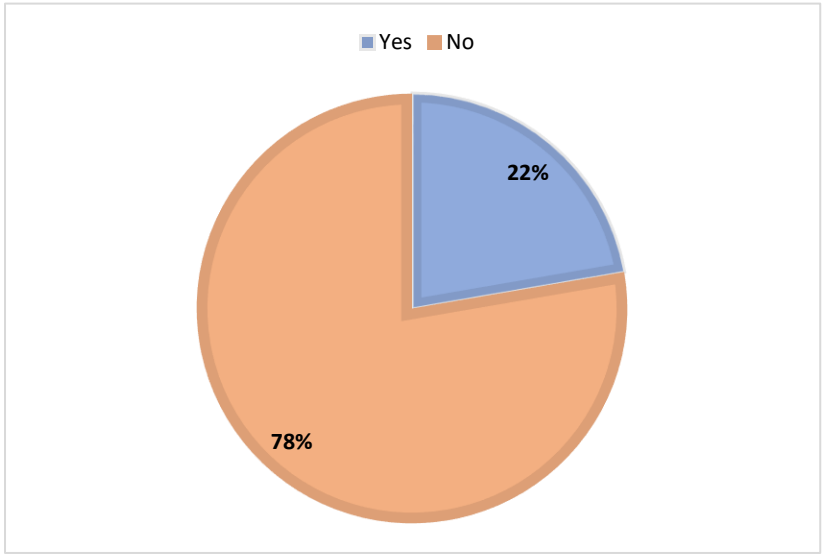
10/21 How concerned are you about drivers not having control over the information collected and shared by vehicles?

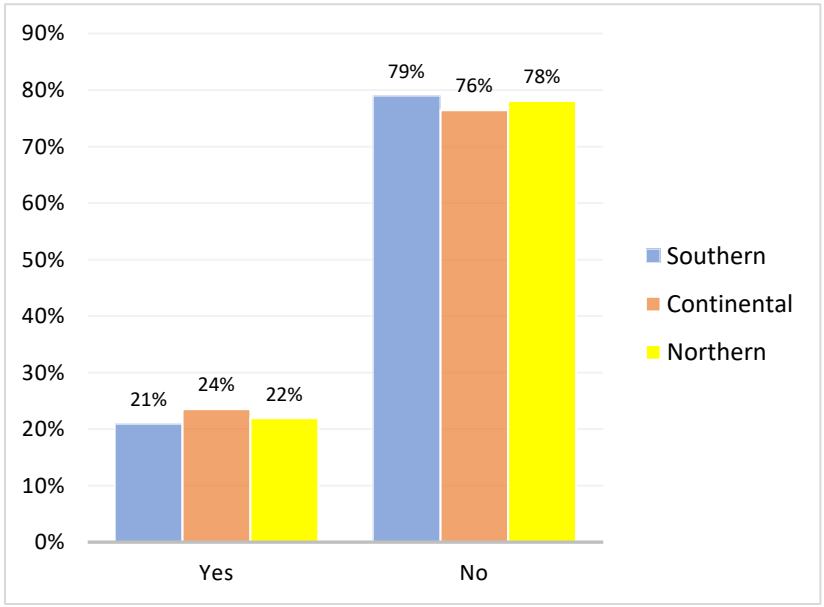




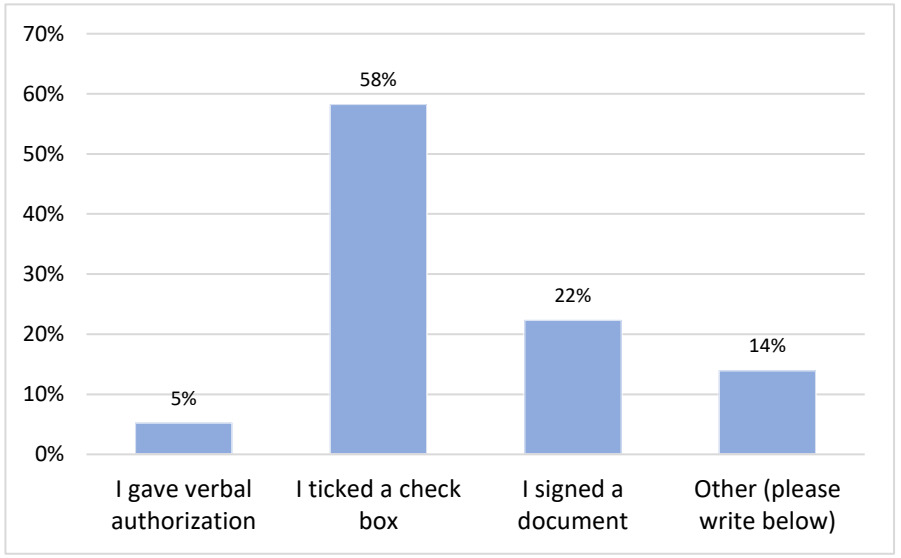


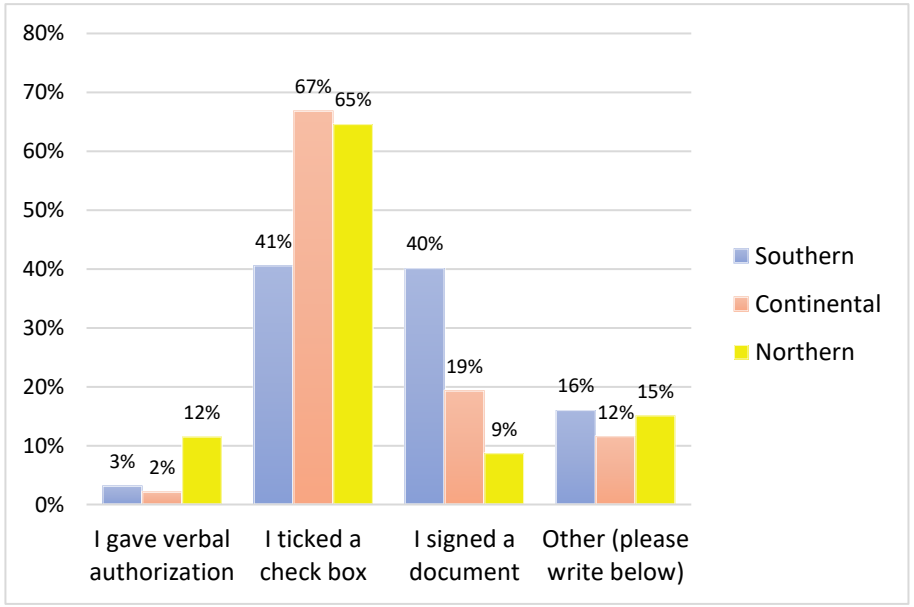
11/21 Do you acknowledge having authorized the use of vehicle data by the vehicle manufacturer and/or other entities?



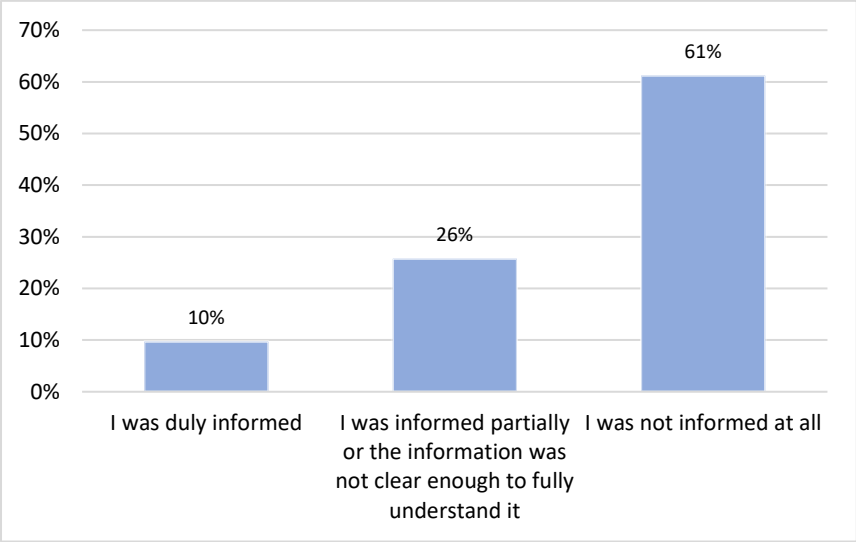


12/21 How did you authorize the use of vehicle data by the vehicle manufacturer and/or other entities?

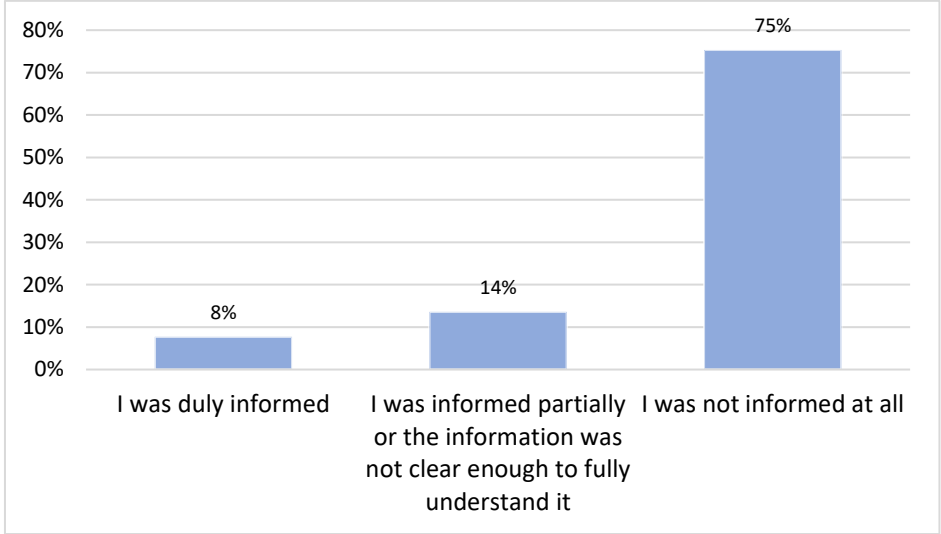


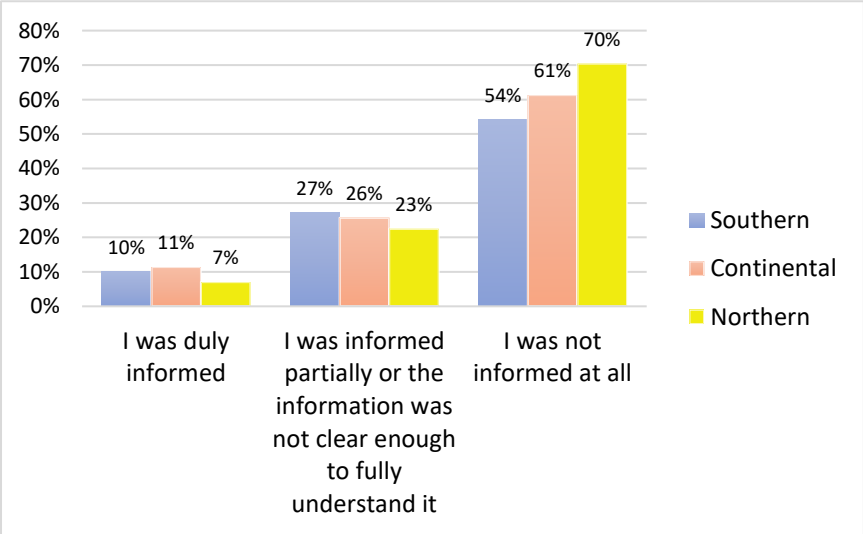


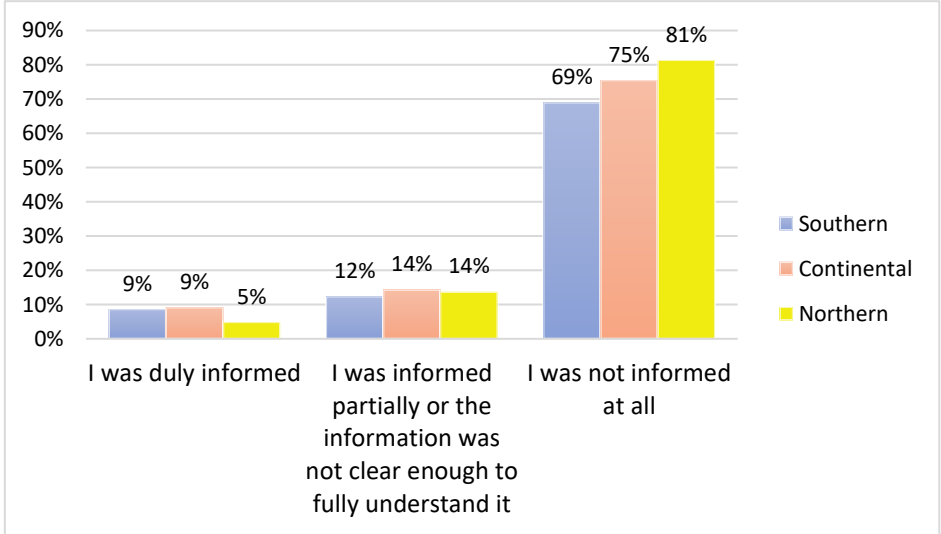
13/21 If you have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer, were you informed about the fact that information would be collected from the vehicle and the purposes for which the information could be used?



14/21 If you have purchased a vehicle with connectivity features from a vehicle dealer or manufacturer, were you informed about how to control the information collected from the vehicle (e.g. how to make a request or complaint, who to contact, etc.)?

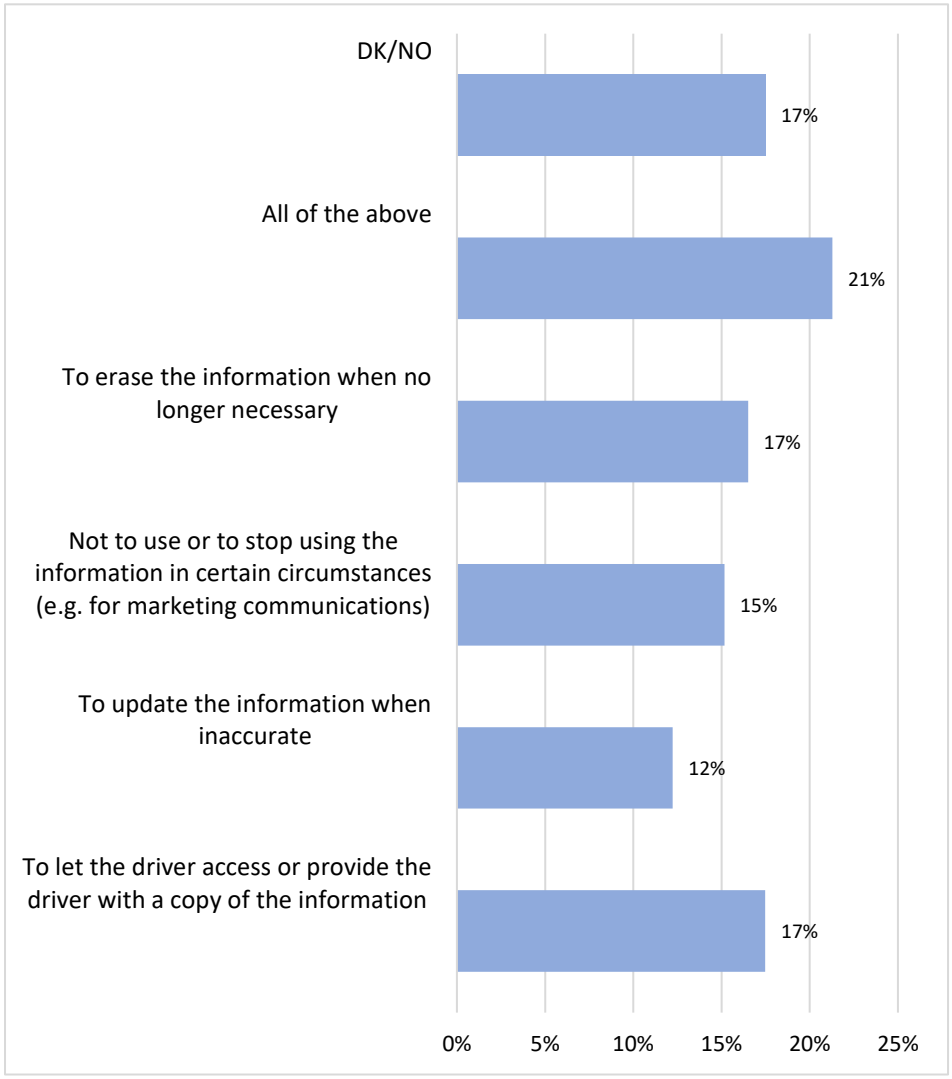




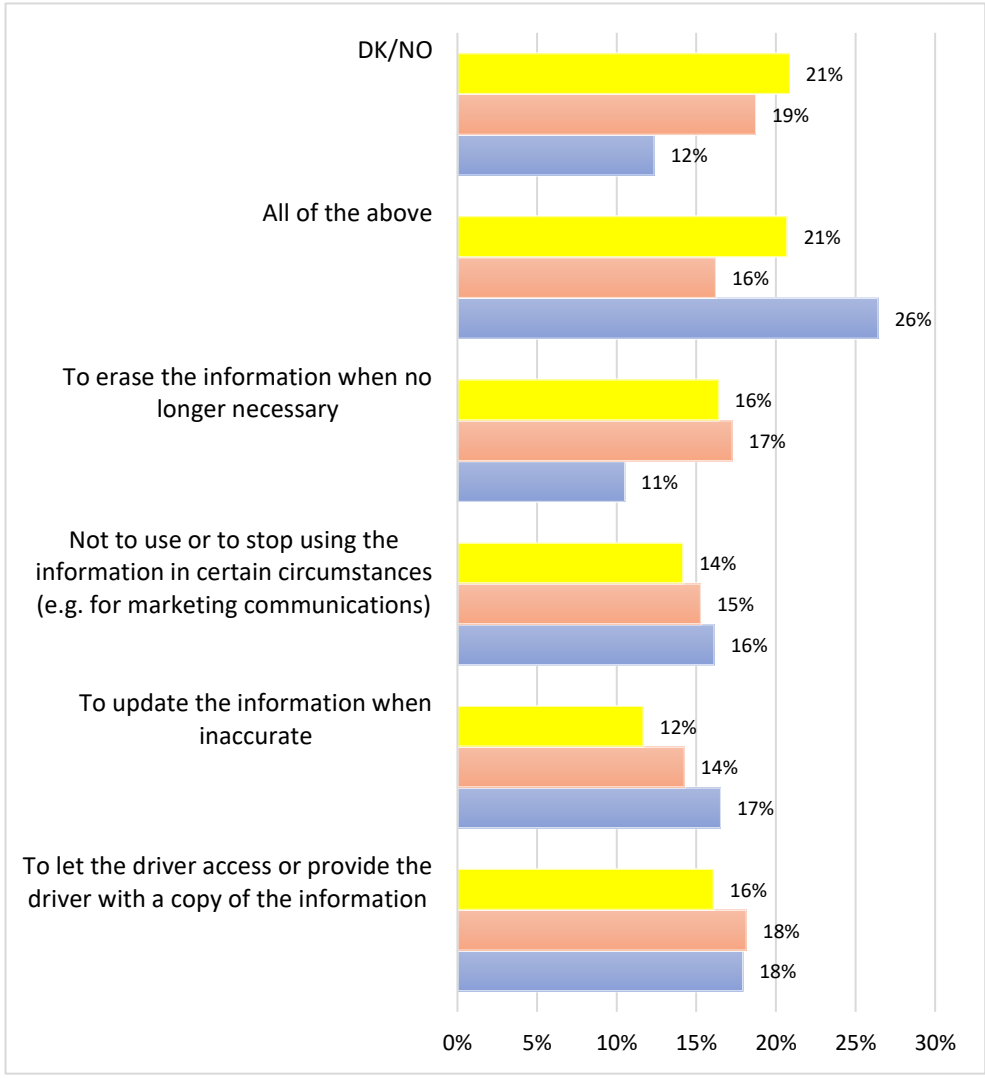


15/21 Do you think drivers can request any of the following to the entities receiving information collected from the vehicle? (Please select all that apply)

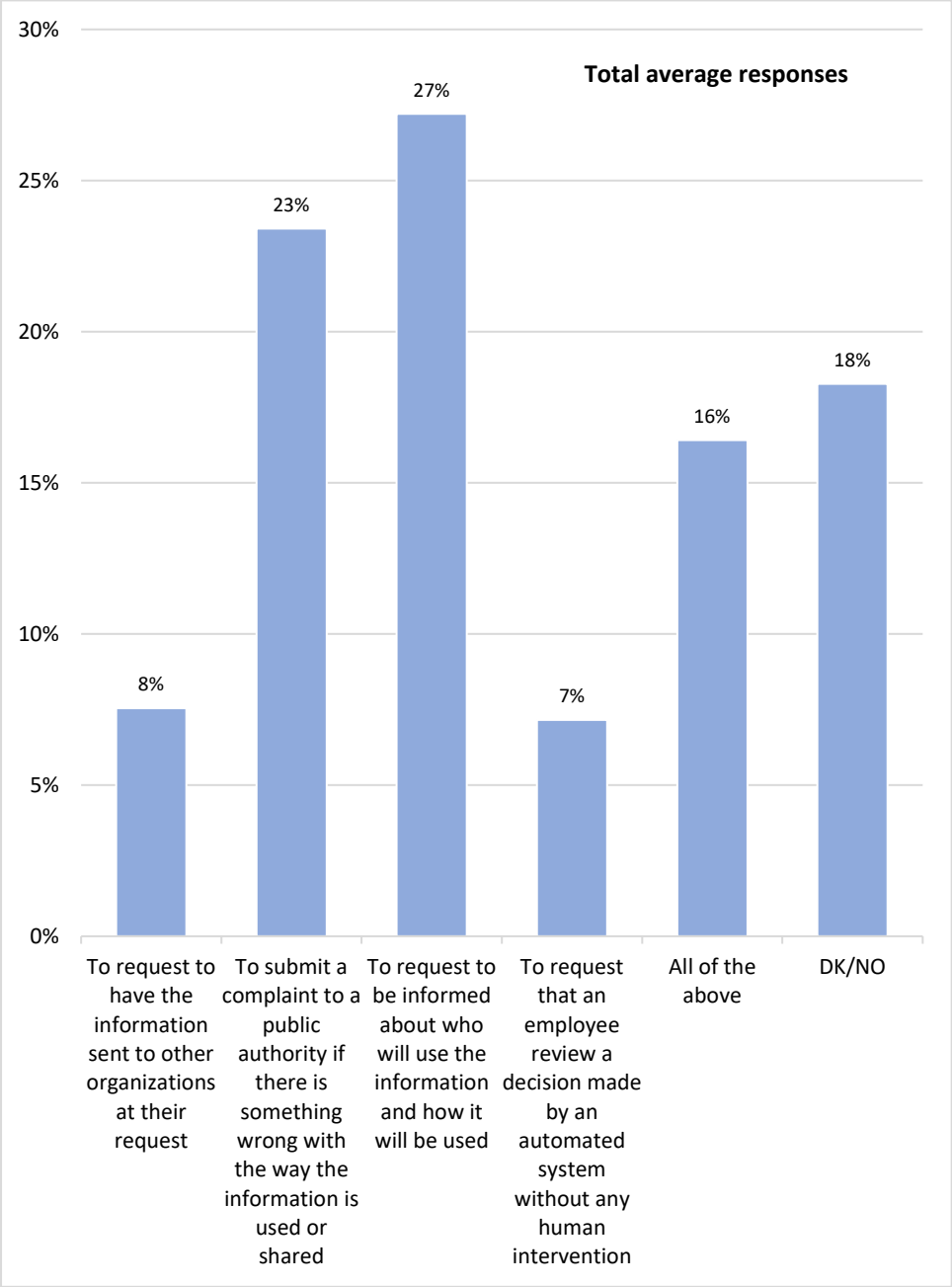
Total average responses

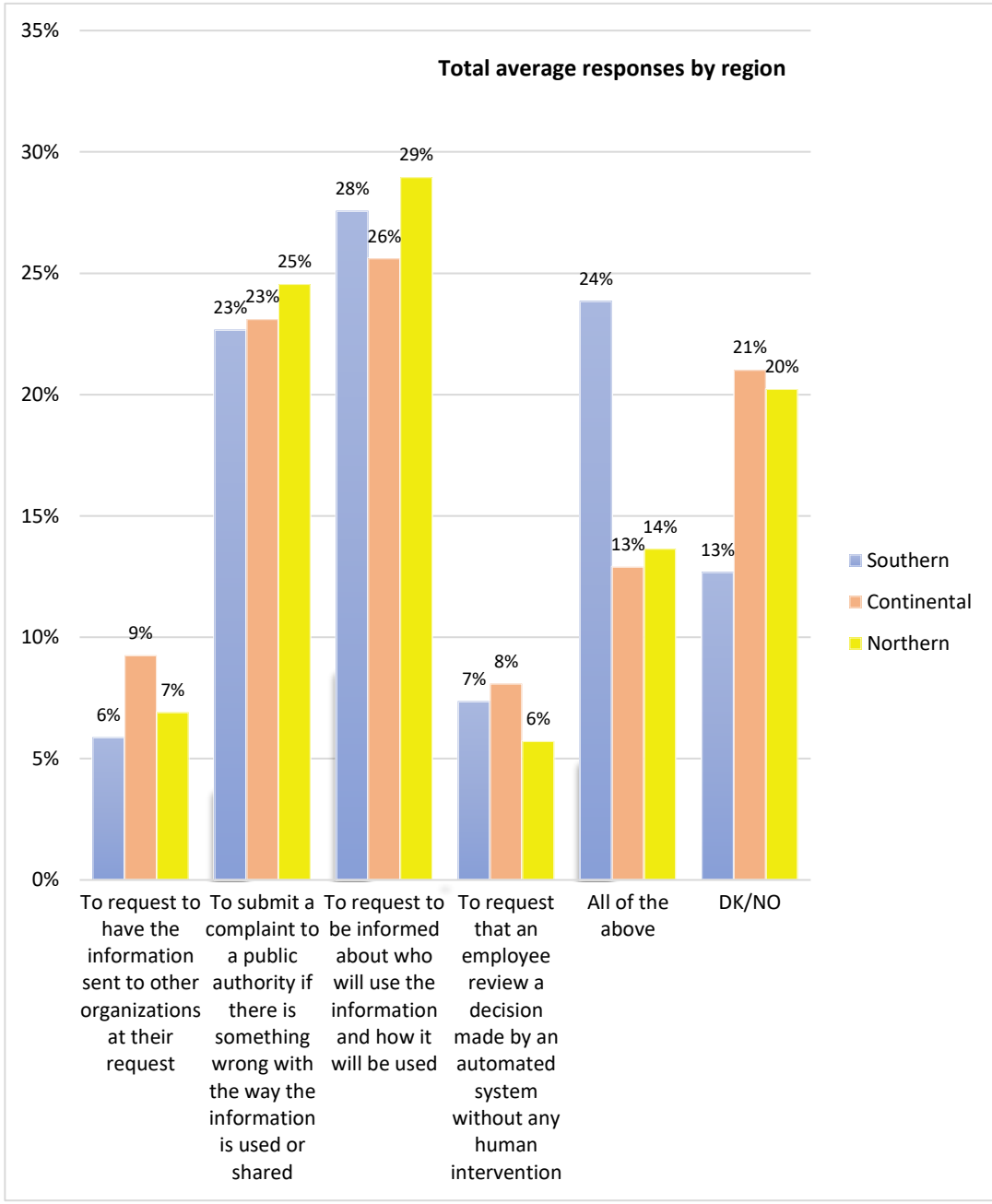


Total average responses by region



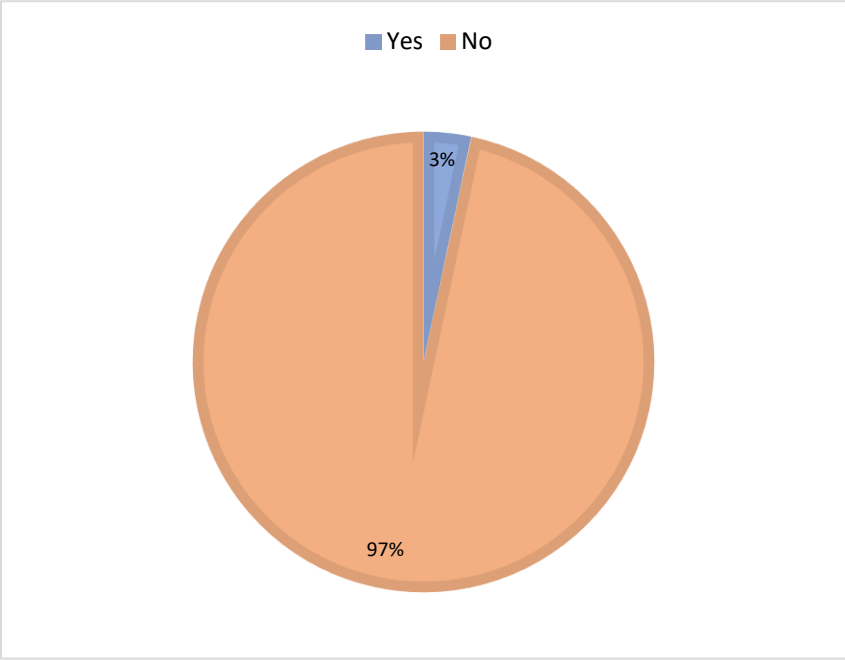
16/21 Do you think drivers can do any of the following? (Please select all that apply)



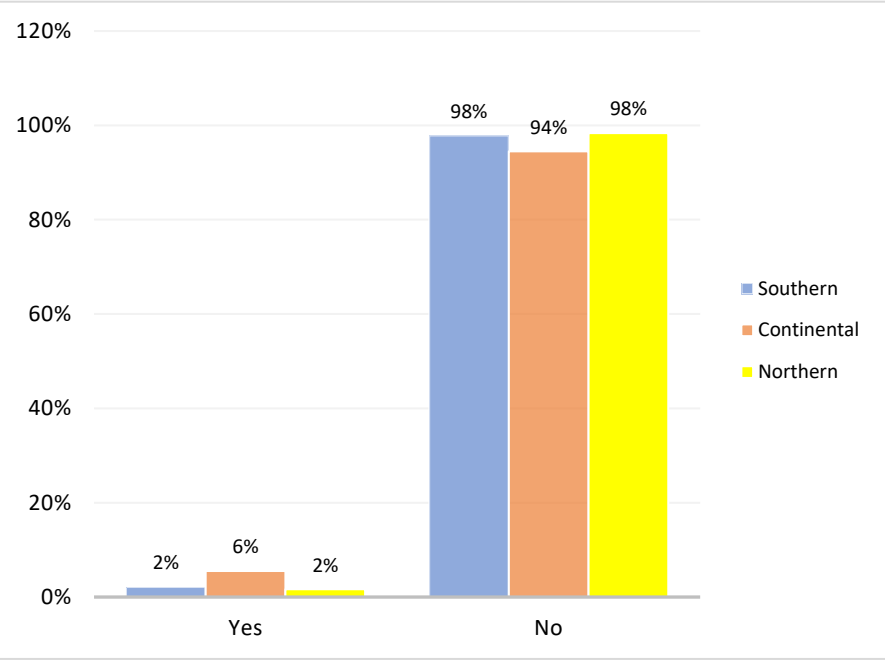


17/21 Have you ever made any of the requests listed in questions 15 and 16 (e.g. request access to the information collected from the car, its update or erasure, the transfer of this information to other organization, etc.)?

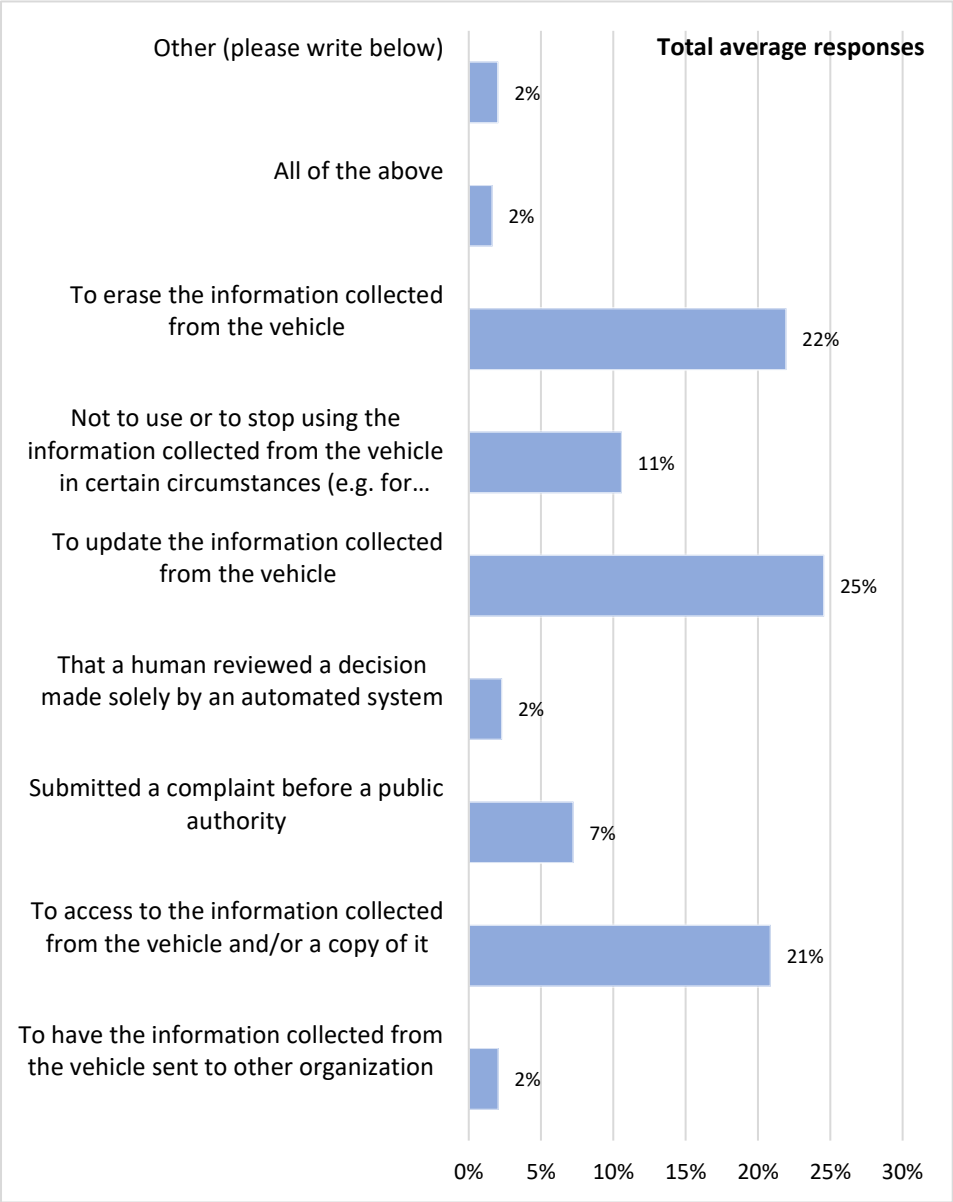
Total average responses

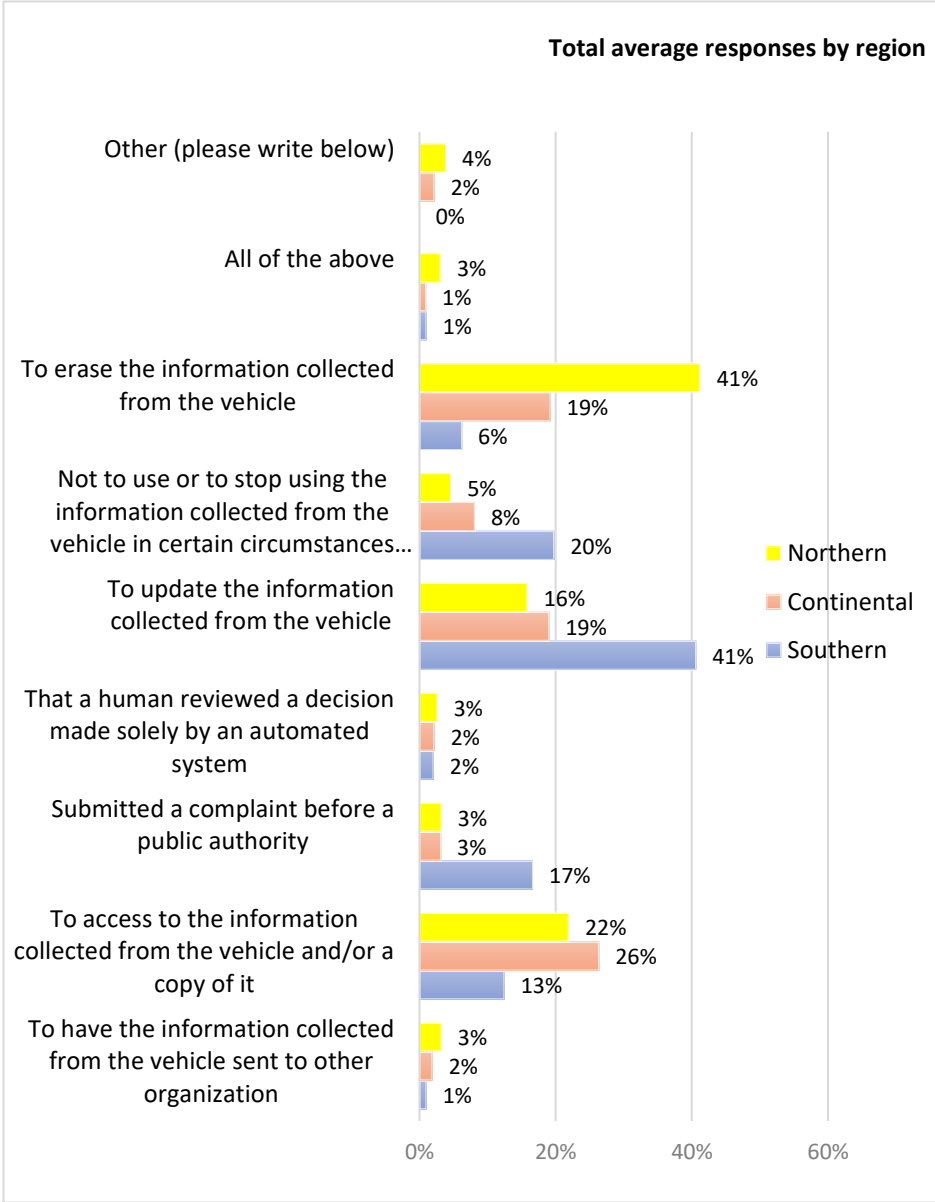


Total average responses by region

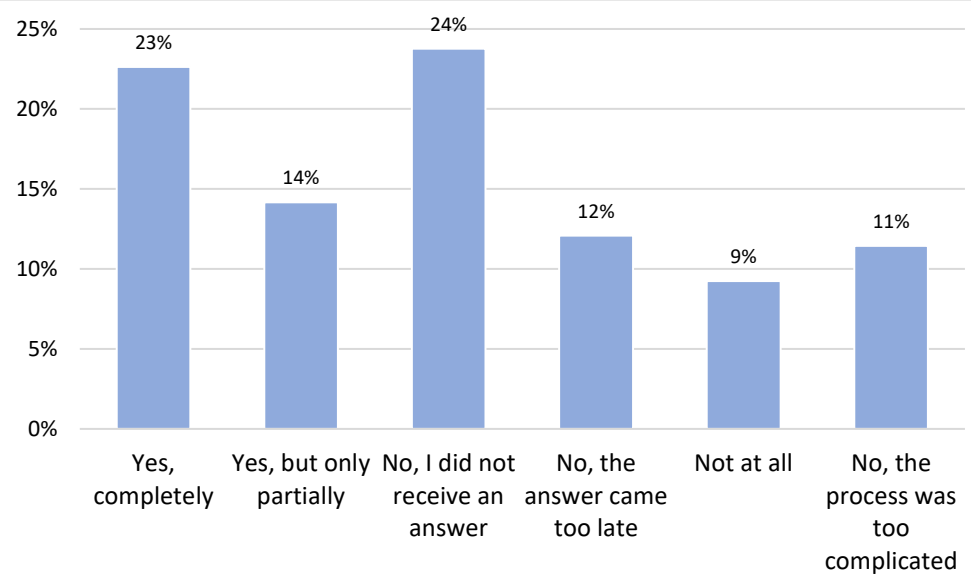


18/21 Which request did you make?

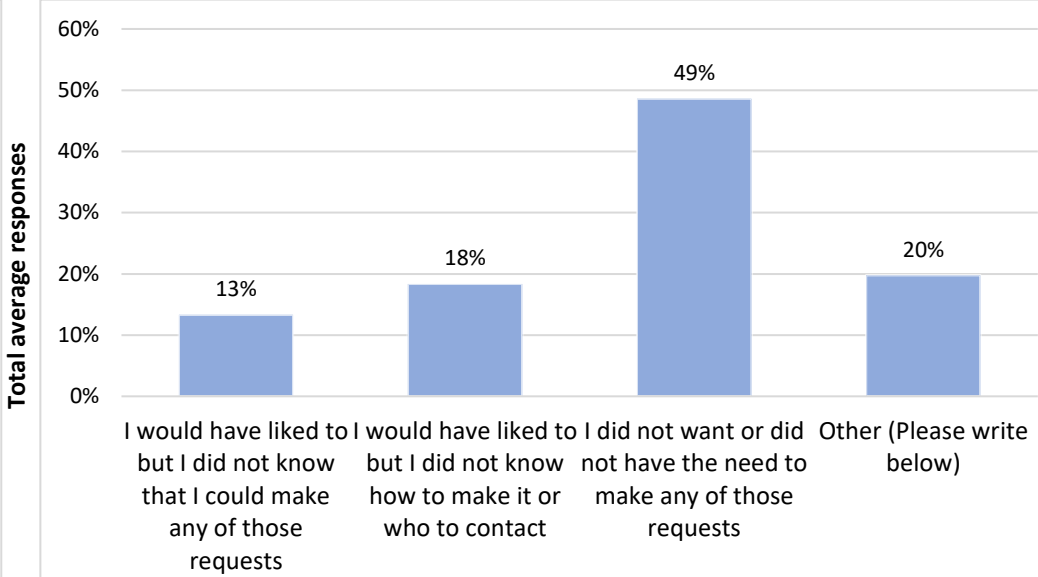


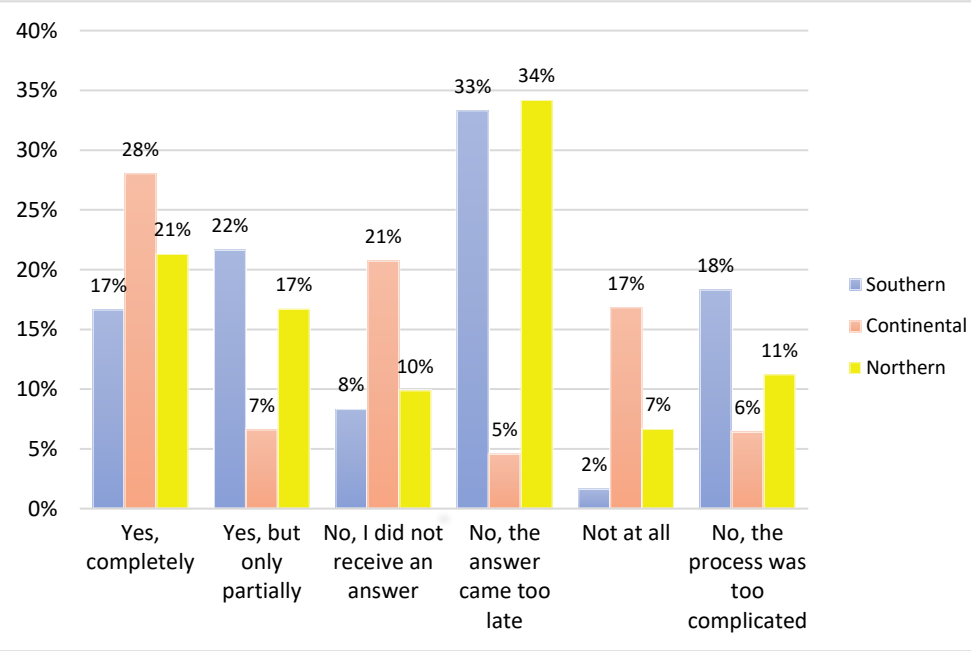


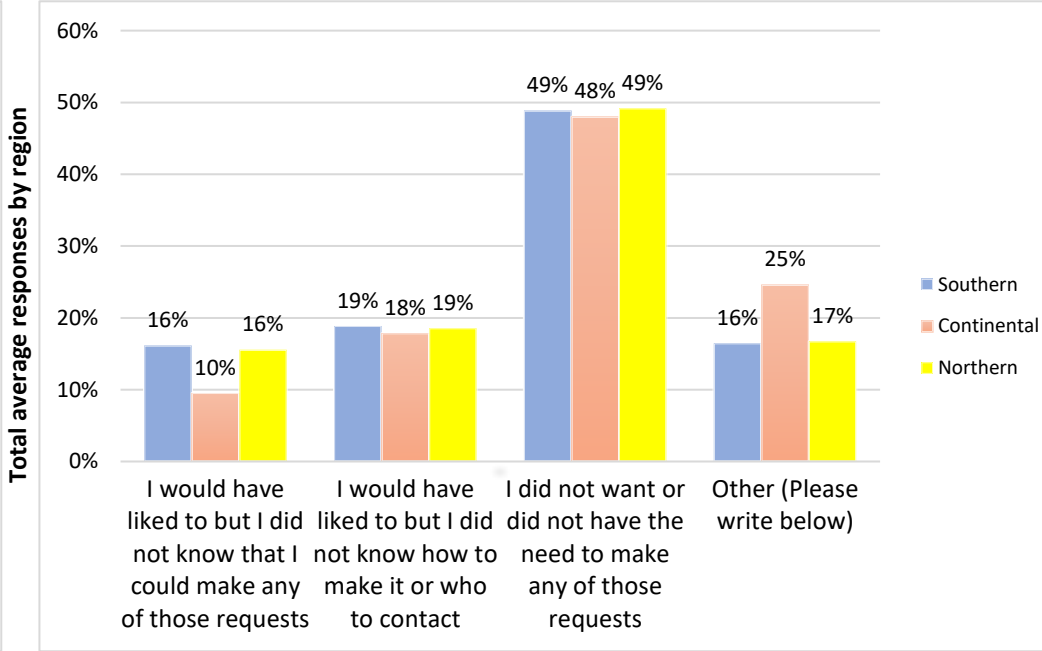
19/21 Did you achieve the result you were looking for?



20/21 Why have you never requested any of the above?







III

Appendix III: Mystery Shopping Fact Sheet

For the purpose of complementing the research on the degree of consumer awareness with regard to vehicle data, during the month of August 2021 four *'Mystery shopping'* ("**MS**") exercises were conducted at different vehicles' point of sales.

Mystery shopping is a technique where, typically, an undercover researcher visits a particular establishment assuming the role of a normal consumer to test and measure the quality of service and customer experience. In the context of the Study, the MS exercises specifically aimed at assessing the extent and clarity to which consumers are informed about the vehicle data collection, use, ownership, and consent. This Appendix describes in detail the methodology followed to conduct the four MS exercises as well as each of the visits and exercises performed in the relevant points of sale.

I. Methodology

A. Selection criteria

The specific point of sales visited in the MS exercises were selected because they sell vehicles of a brand pertaining to one the four automobile groups with the highest annual turnover globally in the year 2020.[182]

B. General approach

As indicated above, the ultimate goal of the MS exercises was to evaluate the level and transparency of information provided to consumers at the vehicle points of sales.

In the interest of the process' success, during the visits the questions about the collection and processing of vehicle data were incorporated in a "standard" exchange of information which would normally take place before purchasing a vehicle. Accordingly, the person conducting the exercise ("**Mystery Shopper**") tried to mimic a normal customer behaviour which would be considered as common and natural in the market concerned, through the type of questions that would be expected from an average potential buyer with a "reasonable interest" in connected vehicle functionalities.

In this context, an average potential buyer having a "reasonable interest" in connected vehicle functionalities means a consumer interested in purchasing a vehicle with connectivity functionalities and therefore trying to get a general understanding of the operation and implications of these functionalities. In order to ensure that all relevant aspects were covered, some lines of inquiry showed some concern regarding the protection of the Mystery Shopper's personal data.

The Mystery Shopper avoided overly sophisticated or excessive inquiring; on the one hand, in order not to raise sales representatives' suspiciousness and risk the success of the process; and, on the other hand, because the main objective of the MS exercises was to assess the information than an average non-specialist consumer would obtain under normal circumstances. For the same reasons, the Mystery Shopper avoided insisting in those aspects where the sales representatives provided incomplete or imprecise responses or directly avoided answering. During the MS exercises, especial attention was paid to sales representatives':

[182] Based on https://www.statista.com/statistics/232958/revenue-of-the-leading-vehicle-manufacturers-worldwide/.

- Predisposition to talk about data processing aspects in the context of vehicle connectivity without being asked by the Mystery Shopper.
- Manifested knowledge regarding the main aspects relating to the processing of vehicle data and ability to explain these aspects to an average consumer.

C. In-shop approach and collection of information by the Mystery Shopper

In each of the on-site visits made to the points of sale, the Mystery Shopper directly approached or, alternatively, was approached by a sales representative to inquire about the type of vehicle of interest.

Attention was paid only to vehicles with connectivity functionalities, as determined by:

i. the possibility to connect the mobile phone to the vehicle (Bluetooth, wire or other) for basic interaction with the vehicle's operating system; and

ii. the existence and ability to use the vehicle manufacturer's app.

In each MS exercise, the Mystery Shopper made sure to go through the following aspects during the conversations with the sales representatives (hereinafter referred to as the "**Minimum Issues**"):

i. **Data nature**: What kind of data does the vehicle collect and process?

   a. Special attention was paid to the collection and processing of data that could be sensitive (e.g. driver's behaviour, location).

   b. In addition, special attention was paid to the distinction between data processed in relation to the vehicle manufacturer's app and data processed by the vehicle regardless of downloading /using the app.

ii. **Data sharing**: Who does the vehicle send data to?

   a. Special attention was paid to whether the data is shared with entities other than the vehicle manufacturer.

iii. **Data subjects' rights**: What rights do vehicle owners/users have and how can they exercise them?

   a. Special attention was paid to access and portability rights.

iv. **Consent**: Is data processing consented? How?

Where any of these Minimum Issues above were not mentioned by the sales representative *motu proprio,* the Mystery Shopper inquired about them in a natural manner, using the following pre-defined lines of inquiry:

- Regarding **data nature**:
  - In order to understand the nature of the data collected and processed,
    - where the sales representative mentioned functionalities or services that could require data about the driver or vehicle usage, the Mystery Shopper inquired about whether location data or driver's behaviour data was needed; or

        - the Mystery Shopper directly inquired about the nature of the data collected and processed.
    - In order to understand the distinction between data that was processed in relation to the vehicle manufacturer's app and data processed by the vehicle regardless of downloading/using the app, the Mystery Shopper inquired about what would happen if the app was not downloaded/used, whether downloading/used the app was obligatory and whether any data would be collected and processed if the app was not downloaded/used.

- Regarding **data sharing**, in order to understand whether any data is shared with third parties:
    - the Mystery Shopper directly inquired about whether any data was shared with third parties, specifically mentioning repair/maintenance services; and/or
    - the Mystery Shopper mentioned the possibility that the data could be shared with insurance companies thus potentially raising the insurance premiums.
- Regarding data subjects' rights, in order to understand which rights vehicle drivers have:
    - the Mystery Shopper showed some discomfort/insecurity about data practices and inquired whether there was any chance to see, modify or erase data at the driver's request; and
    - with regard to portability, the Mystery Shopper inquired whether it would be possible to send data to third parties at the driver's request; for instance, from official repair services to other alternative repair services.
- Regarding **consent**, the Mystery Shopper directly inquired whether data processing would be consented and how it would be provided.

To the extent possible, the Mystery Shopper sought simplicity and brevity to ensure that the exercises were correctly reported in writing once out of the point of sale.

Throughout the conversations and interaction with the sales representatives, the Mystery Shopper retained mental evidence of the information provided by the latter, distinguishing between:

a) Information provided *motu proprio* by the sales representative (**I1**).

b) Information provided only after the Mystery Shopper´s inquiry (**I2**).

c) Information not provided, even after inquiring (**I3**).

Each MS exercise was considered completed when: (i) all Minimum Issues had been gone through or inquired about; and (ii) a vehicle purchase offer was provided to the Mystery Shopper.

D. Analysis approach

As commented, the MS exercises performed for the Study aimed at evaluating the extent and clarity to which consumers are informed about the vehicle data collection, use, ownership, and consent at the point of sales.

Assessment of the extent to which consumers are informed was performed by (i) evaluating whether the Minimum Issues had been mentioned by the sales representatives; and (ii) categorizing the information provided by the sales representatives into the three categories mentioned above: I1, I2 and I3.

Evaluating the clarity of the information provided by the sales representative involved a two-step process: in a first stage, the Mystery Shopper transcribed the different exercises, emphasizing those points in the conversation where connectivity and data processing aspects were mentioned. This information was analysed, in a second stage, by privacy and data protection experts to derive conclusions.

E. Quality control

- The MS exercise methodology has been coordinated and reviewed by the leadership of the expert Study to ensure the right definition of the MS exercise approach, flow, team designation and resource allocation.
- The Mystery Shopper was a data protection and privacy expert with over 5-year professional exercise to ensure proper understanding of raw data in its legal context.
- The team conducting the analysis was composed by data protection and privacy experts with solid knowledge and well-known reputation in the market.
- Any possible personal data that might have been collected throughout the MS exercises was immediately anonymised.

II. MS experiences in detail

A. Point of sale 1 – Brand 1

A. Detail of the experience

The Mystery Shopper directly approached the sales representative to start the process. Attention was set at a couple of models with connected capabilities. Given the delay in semiconductor manufacturing, the available stock was limited, shifting the conversation to one specific model.

The sales representative showed the vehicle and explained its different features and functionalities. The sales representative did not mention functionalities related to vehicle connectivity.

The Mystery Shopper inquired whether it was possible to connect the phone and whether there was an app. The sales representative confirmed that the vehicle was equipped with Android Auto and Apple's CarPlay and that there was an app available for users that allow them a number of functionalities such as locating the vehicle, locking it remotely, monitoring the state of the vehicle or starting the engine remotely. The sales representative did not follow-on these topics and only continued the conversation upon further questioning by the Mystery Shopper.

The Mystery Shopper asked whether Android Auto and Apple's CarPlay are simply an extension of the mobile phone's screen or whether any data is collected by the vehicle manufacturer. The sales representative answered that it is only an extension of the mobile phone´s screen.

The Mystery Shopper asked about data collection by the vehicle manufacturer through the app and the sales representative explained that any data collection is limited to that necessary to provide the app functionalities. When inquired about the nature of the data collected, the sales representative drew a parallelism with the mobile phone and explained that any kind of data could be collected to the extent that it is related to vehicle usage.

The Mystery Shopper showed worry about the collection of data and possible sharing with third parties and the sales representative said that the use of this data would only take place in the vehicle manufacturer's environment and only to the extent necessary to provide app functionalities, the eCall functionality, road assistance or costumer support. The Mystery Shopper inquired about the eCall functionality and road assistance and the sales representative explained these are mandatory features that any new vehicle must include and that all new vehicles have an e-SIM for remote communication purposes in cases of emergency, breakdown or costumer support. The Mystery Shopper asked whether these features would collect data even without having downloaded the app and the sales representative explained that it is mandatory to download the app in order to activate the e-SIM but that it can be erased at a later stage if worried about data usage by the vehicle manufacturer. The Mystery Shopper asked whether the processing of data for eCall and road assistance would happen even after the app was erased and the sales representative responded that data processing might not take place, but that these functionalities might stop working. The sales representative added that, if requested by the Mystery Shopper, it could be possible to try to speak to the vehicle manufacturer to avoid the need to download the app and activate the eCall and road assistance functionalities without the app, as they are compulsory.

The Mystery Shopper inquired whether it could be possible to consent to data usage and the sales representative explained that all data processing would be consented through the app and that probably the app would request one consent to several different data processing purposes. The Mystery Shopper asked whether it would be possible to know which information the vehicle manufacturer would collect from the vehicle and the sales representative answered affirmatively. The Mystery Shopper showed curiosity about the possibility to request the sending of the data to a different third party in case the Mystery Shopper would decide to change the vehicle eventually, to which the sales representative answered that probably that would be possible.

Once the Mystery Shopper said that there were no additional questions, they checked the model's availability and discussed the financials. The sales representative formalized the offer to the Mystery Shopper and sent an email with the details, after which the exercise concluded.

B. Main results:

- **None of the Minimum Issues would have been mentioned or discussed if not inquired** by the Mystery Shopper.
- Once asked about vehicle connectivity aspects, the sales representative was open to talk about them although, once inquired to deepen into data processing aspects, the sales representative did not offer clear answers to the extent that:
    - The explanation about whether data would be collected regardless of the use of the app was confusing and not conclusive. The sales representative explained that downloading the app was necessary to activate the e-SIM and therefore activating the eCall, road assistance and customer support functions, which are compulsory. Nevertheless, the sales representative suggested the Mystery Shopper to erase the app right after downloading it to avoid data usage by the vehicle manufacturer. The sales representative could not explain whether erasing the app would also stop processing of data in relation to the eCall and bCall[183] functions.
    - The explanation about how the user could consent to processing of vehicle data was unclear. The sales representative noted that consent might be somehow bundled in the app for all the possible services available.
    - The sales representative clearly stated that data did not leave the vehicle manufacturer's environment.
    - The sales representative explained that Apple's CarPlay/Android Auto functions are merely an extension of the mobile phone, thus not providing vehicle information to Apple/Google nor phone information to the vehicle manufacturer.

[183] The bCall functionality refers to a service which allows car users to call local road assistance in case of a breakdown.

B. Point of sale 2 - Brand 2

A. Detailed description of the exercise:

The sales representative approached the Mystery Shopper while the latter examined a vehicle in the exhibition. They talked about models the Mystery Shopper could be interested on. Based on the Mystery Shopper's manifested preferences, the attention was set at one specific model.

The sales representative showed the vehicle and explained its different features and functionalities. The sales representative did not mention functionalities related to vehicle connectivity. Then the Mystery Shopper inquired whether it was possible to connect the mobile phone and whether there was an app. The sales representative confirmed the vehicle is prepared to interact with Android Auto and Apple's CarPlay and that there is an app available for users that allows them a number of functionalities, such as locating the vehicle and advising of needed maintenance. The sales representative did not continue talking about these topics, only resuming the conversation on connectivity functionalities and data processing upon further questioning by the Mystery Shopper.

The Mystery Shopper asked about data collection by the vehicle manufacturer, for instance through Android Auto or through the app. The sales representative replied that maybe location data is collected, but only to the extent necessary to allow app functionalities. The sales representative explained that no other data is collected and that, in any case, all data collection would always be consented and that the vehicle manufacturer complies with all relevant regulations.

The Mystery Shopper inquired about possible data collection in relation with the eCall functionality and the sales representative explained this was mandatory and that every new vehicle has this feature.

When asked about the possibility to know which data would be collected by the vehicle manufacturer the sales representative manifested not to be in a position to answer that question and assured that any data processing by the vehicle manufacturer would be always compliant with regulations.

When inquired whether it would be possible to erase the data, for instance by erasing the app or before selling the vehicle to a third party, the sales representative explained that it is not necessary to download the app in the first place.

The Mystery Shopper also inquired whether it would be possible to request the data to be sent to an independent repair service provider for a cheaper service and the sales representative indicated that he did not know and focused on the economic aspects of recurring to an independent repair service provider.

The sales representative provided the model's availability and explained the financial aspects of the potential purchase. The sales representative formalized the offer to the Mystery Shopper and gave it in hard copy to the latter, after which the exercise concluded.

A. Main results:

- The sales representative showed **little predisposition to talk about vehicle connectivity aspects and the implications thereof**.

- **None of the Minimum Issues would have been mentioned or discussed if not inquired by the Mystery Shopper**.
- The sales representative showed **unprepared to explain the implications of the use of vehicle connectivity aspects**, to the extent that he admitted not to be in a position to answer questions related to data processing.
- The **sales representative deliberately avoided privacy matters**, persistently focusing on the fact that privacy is preserved by the vehicle manufacturer, that data does not leave the vehicle manufacturer's environment and that the vehicle manufacturer only uses the data for app services, but without answering or going into detail on any of the specific matters raised by the Mystery Shopper.
- The **explanation about data collection and processing was very unclear**, leaving uncertainty around what type of data is collected and whether it is collected in relation to the app or regardless of it.

C. Point of sale 3 – Brand 3

A. Detailed description of the exercise:

The sales representative approached the Mystery Shopper while the latter examined a vehicle in the exhibition. The Mystery Shopper pointed at a model of interest.

The sales representative showed the vehicle and described its different features and functionalities, including that the vehicle is prepared to interact with Android Auto and Apple's CarPlay.

The Mystery Shopper inquired whether there was an app made available by the manufacturer. The sales representative confirmed the vehicle manufacturer has an app available for users with different functionalities, emphasizing on the possibility to remotely lock the vehicle. The sales representative did not explain possible personal data processing aspects.

The Mystery Shopper asked about data collection by the vehicle manufacturer, to which the sales representative replied that location data was collected for the operation of the eCall functionality and to provide services related with the app, if downloaded. After being asked, the sales representative pointed out that downloading the app was not mandatory. The Mystery Shopper asked whether data would be collected even without having downloaded the app and the sales representative pointed out that at least location data could be processed. Furthermore, the sales representative explained that vehicles are growingly like mobile phones and can collect data about vehicle usage and send it to the vehicle manufacturer. The Mystery Shopper manifested at this point its uneasiness about obscure data processing and the sales representative stated that no data would leave the vehicle manufacturer's environment and, therefore, it would not be shared with third parties, as this would be illegal.

When asked about the possibility to know which data would be collected by the vehicle manufacturer, ways of deleting this data (e.g. if the vehicle was later sold to a third party) or the chance to request the vehicle manufacturer to send the vehicle data to a third party, the sales representative shifted the conversation to the technical characteristics of the vehicle, explaining that data processing aspects are secondary and app-related, which is not compulsory to download in any case.

When asked whether users were given the chance to consent to data processing in case the app was downloaded, the sales representative answered affirmatively and explained that all consents were managed through the app.

Once no further questions remained on the Mystery Shopper's side, the sales representative searched for the model's availability and provided information about the financial aspects of the potential purchase. The sales representative formalized the offer to the Mystery Shopper and sent an email to the Mystery Shopper, after which the exercise concluded.

B. Main results:

- **None of the Minimum Issues would have been mentioned or discussed if not inquired** by the Mystery Shopper.
- The sales representative showed predisposition to talk about vehicle connectivity at the beginning of the process, although this attitude shifted towards a more cautious

position once the Mystery Shopper showed uneasiness about obscure data processing activities.

- The sales representative showed **unprepared or unwilling to explain vehicle connectivity aspects** to the extent that:
    - The sales representative provided an unclear explanation of the type of data that was collected by the vehicle, with only focus on geolocation.
    - The explanation about data collection through the app was equivocal and misguiding as it focused on geolocation data in the beginning and, when confronted with the fact that vehicle usage data such as gas consumption or speed monitoring was also data revealing the driver's habits, the sales representative simply indicated that vehicles are increasingly similar to mobile phones.
    - When asked about rights linked to the processing of personal data, such as access, erasure or portability, the sales representative avoided these topics and the response was restricted to stating that privacy is preserved and vehicle manufacturers only use the data for app-related services.

D. Point of sale 4 – Brand 4

A. Detailed description of the exercise:

The Mystery Shopper approached the sales representative at the point of sale after arranging a visit. After discussing the Mystery Shopper's preferences, given that the available stock was limited because of the delay on semiconductors manufacturing, the attention was set on one specific model.

The sales representative showed the vehicle and described its different features and functionalities, including that the vehicle was equipped with Android Auto and Apple's CarPlay and that the vehicle manufacturer has an app available. In order to explain the app's functionalities, the sales representative used a big banner located at the middle of the point of sale, focusing primarily on vehicle location, remote vehicle lock, and monitoring of gas consumption and needed repairs.

Despite mentioning the existence of vehicle connectivity functionalities, the sales representative did not refer to personal data processing aspects. The Mystery Shopper asked about data collection by the vehicle manufacturer in relation with the abovementioned functionalities, to which the sales representative answered that no data was collected from the driver. The Mystery Shopper insisted and inquired whether no data from the driver is collected and the sales representative replied that only geolocation data is collected and that, unlike mobile phones, vehicles did not process data from their users.

The Mystery Shopper asked whether it is mandatory to download the app and the sales representative indicated that it is not necessary.

In view that the sales representative insisted that no data processing takes place, the Mystery Shopper and the sales representative searched the model's availability and discussed the financial aspects of the potential purchase. The sales representative formalized the offer to the Mystery Shopper and gave it in hard copy to the Mystery Shopper, after which the exercise concluded.

B. Main results:

- **None of the Minimum Issues would have been mentioned or discussed if not inquired** by Mystery Shopper.
- **There was some predisposition to talk about vehicle connectivity functionalities** to the extent that the point of sale had a big banner explaining app-related features. Nevertheless, the **explanation focused exclusively on practical information on functionalities for users and not on personal data processing underneath**.
- The sales representative showed **significantly unprepared or deliberately unwilling to explain personal data processing aspects related to vehicle connectivity to the Mystery Shopper,** as he specifically rejected that the vehicle used data about the vehicle driver. Only upon insistence by the Mystery Shopper about possible data collection, the sales representative admitted that geolocation data might be involved, but insisted on the fact that any sharing would be illegal.

The sales representative deliberately avoided discussing data processing aspects and deviated attention from these points when asked.

IV

Appendix IV: Assessment of consumer vehicle purchase contracts and privacy policies

I. Methodology

The assessment of consumer vehicle purchase contracts and privacy policies is the research line aiming at getting an understanding on:

(i) the clarity of the information/conditions and implications on the sharing and processing of vehicle data; and
(ii) whether consumer consent is requested in connection to the use of their (personal) data, including third-party use.

This process consisted on the review and analysis of different types of OEMs' contractual/informative documents relevant to the processing of personal data in the context of the connected vehicles. In particular, we have reviewed (i) purchase and sale agreements from dealers in Spain; (ii) general website privacy policies of different vehicle brands applicable in certain EU/UK jurisdictions; and (iii) privacy policies in relation to data processing for the connected vehicle for different brands applicable in certain EU/UK jurisdictions; (iv) app privacy policies for vehicle connectivity services and (v) any other documentation which could be useful to understand the data processing in the context of connected vehicles (e.g. installation orders for vehicle connectivity, privacy policies of related automotive services).

The reason behind analysing, not only sale and purchase agreements, but also additional documentation strives on achieving the most complete picture about the information provided by OEMs regarding the processing of personal data. While sales and purchase agreements have a data protection section or annex, this does not cover connectivity functionalities but instead refers to the fulfilment of the purchase order, marketing activities, etc. We reviewed website privacy policies to confirm that no information about data processing in the context of connectivity functionalities is provided therein. We verified this is the case as website privacy policies generally deal with the processing of data in the context of each particular websites (e.g., registration, cookies, newsletter). Where available, we have located and reviewed privacy policies in OEMs websites dealing specifically with data processing aspects in the context of connected vehicles. Where we could not find these privacy policies in the OEMs websites, we downloaded the apps for the provision of connectivity services and analysed the app privacy policies available therein. We have also verified whether other documentation includes information relevant for the purposes of the Study, which is the case, for instance, of an installation order to set up connectivity functionalities in a vehicle. This section of the Report describes the individual results of each reviewing, sorted by brand.

The documentation has been obtained through publicly available sources, where available, or, in the case of the purchase agreements, these are documents that have been voluntarily shared with EY and for which there was not a confidentiality agreement in place.

The documentation analysed pertains to one brand belonging to each of the automobile groups studied during the MS experiences and other brands for which a sale and purchase agreements had been gathered.

The review was carried out during August and September 2021 and revisited before publication of the Report. Documents were last accessed on 30/11/2021.

The identity of the brands involved in the review has been deidentified to avoid brand and/or reputational issues.

II. Analysis by brand

A. Brand 1

The following documents were reviewed:

1. Sale and purchase agreement (Spain).
2. Documentation related to the installation of connectivity capabilities in a vehicle.
3. Web privacy policy.
4. Single sign-on privacy policy.
5. App privacy policy.

After reviewing the abovementioned documentation for the purpose of assessing the clarity of the information and implications on the sharing of vehicle data and whether consumer consent is requested in connection to the use of personal data, including third-party use, we have arrived at the following conclusions:

Information is not always available

No information regarding personal data processing relating to vehicle connectivity is provided in the sales and purchase agreement or at the general website privacy policy. The information is neither provided or made available in the websites dedicated to present the vehicles and connectivity functionalities.

This information would therefore be provided or made available to users only and to the extent that they download the app in connection to enjoying Brand 1 connectivity services. Therefore, this suggests that consumers do not get information about the implications of data processing in the context of connected vehicles unless they download the app, and never before.

We have verified that the data processing relating to the eCall functionality is not mentioned in app privacy policies (except in some cases where emergency value-added services are offered) that have been reviewed. Accordingly, this suggests that information in this regard should be provided either in the sales and purchase agreement, or in the vehicle owner's manual. Taking into account that the reviewed sales and purchase agreements do not include any information on this functionality, it seems that the information about this processing is not being made available to consumers, at least, before purchasing the vehicle.

Likewise, whether other connectivity functionalities involving data processing were available and activated without the need to download the app, the information about these processing would not be available for users, at least, before the purchase of the vehicle.

In addition, the information related to the processing of personal data in the context of connected vehicles is not provided to the consumer in the moments where this information might be of relevance to them, i.e., during the consideration stage in the purchase process.

Unclear and incomplete information about data sharing

The information provided in the app privacy policy regarding data sharing with third parties is complex and unclear at points.

According to this information data is shared with Brand 1 "Importer" for personalized marketing purposes based on the consumer's prior consent. It is not clear who the Importer is and the type of processing activities for which the transfer will take place.

In addition, the privacy policy does not say to what third parties Brand 1 will share data for the fulfilment of legal obligations. This is contrary to the criteria set by the Article 29 Working Party (which is currently the EDPB) in its guidelines on transparency, which state that "[t]he actual (named) recipients of the personal data, or the categories of recipients, must be provided" or the categories of recipients.[184]

[184] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP260 rev.01, 2018, p. 37.

B. Brand 2

The following documents were reviewed:

1. Sale and purchase agreement (Spain).
2. Web privacy policy web.
3. App privacy policy.

After reviewing the abovementioned documentation for the purpose of assessing the clarity of the information and implications on the sharing of vehicle data and whether consumer consent is requested in connection to the use of personal data, including third-party use, we have arrived at the following conclusions:

Information is not always available

The analysis of this section is similar to the analysis regarding Brand 1. In this regard, information on these aspects is only provided in relation to the Brand 2 app at the moment of downloading. We refer to Brand 1 analysis for further reference.

Insufficient information for consumers to understand the implications of the processing of data in the context connected vehicles

The information regarding personal data processing in relation to connectivity functionalities is provided in the app privacy policy.

This information is limited to describing the minimum legal aspects required by Article 13 GDPR, without taking into consideration whether the information provided is sufficient for an average consumer to understand the scope and consequences that the processing entails. From our perspective, the information provided does not allow consumers to get a notion that their vehicle will be processing a variety of data, of very diverse nature and sources, including information, such as geolocation, that might be of special sensitivity, and combining this information to provide the different services under the Brand 2 app umbrella. In particular, the information provided is insufficient to understand the possible risks and implications linked to the purchase of a connected vehicle or the enjoying of the services mentioned.

For instance, there is not information about the service providers with which data can be shared in case the different services are used, the purposes of the sharing or the practical implications of the sharing, for instance, the scope of the information which will be shared. Another example is the limited information about periods for which the data will be stored.

Recital 39 GDPR states that “natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data...”. The Data Protection Working Party 29 recalls in its guidelines on transparency that the principle of transparency is directly linked to the principle of fairness in the sense that a fair processing entails that data subjects must be able, with the information provided, to understand the processing, its scope, consequences and potential risks, in order to achieve the level of protection that the GDPR grants for users. This is especially predicable in relation to processing activities that are complex in nature or were unexpected data processing could take place. Precisely in these situations, the Data Protection Working Party 29 position is that data controllers should not limit themselves to providing the information prescribed under Articles 13 and 14 GDPR but “should also separately spell out in

unambiguous language what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data."[185]

Incomplete information about the exercise of data protection rights

The information in the app privacy policy regarding data subjects' personal data protection rights provides a brief explanation of the rights available to them but does not mention how data subjects shall exercise them. As the Article 29 Working Party recall in their guidelines on transparency, "GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to meaningfully position data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal data".[186]

Without any information regarding how to exercise these rights, including the modalities available to facilitate these rights, the average consumer will likely be a position of inability to exercise these rights.

Lack of control

A combined analysis of the previous considerations calls into question whether the current informative framework is achieving one of the GDPR's flagships, which is that natural persons should "have control of their own personal data", as stated in Recital 7.

In a situation where consumers are

i. not provided with information to allow them to be able to understand the implications of the processing, barely even to get a notion through that information about the fact that their connected vehicle will be collecting, processing and sharing a variety of data of different nature; and

ii. not provided with information or means about the modalities at disposal of data subjects to exercise the rights granted by law,

it is reasonable to challenge whether consumers have actual control over their personal information or whether there is simply a factual illusion of control, but no real means to exercise it.

[185] *Ibid*., p. 7.
[186] *Ibid.,* p. 26.

C. Brand 3

The following documents were reviewed:

1. Web privacy policy.
2. App privacy policy.[187]
3. Connected car privacy policy 1.
4. Connected car privacy policy 2.

After reviewing the abovementioned documentation for the purpose of assessing the clarity of the information and implications on the sharing of vehicle data and whether consumer consent is requested in connection to the use of personal data, including third-party use, we have arrived at the following conclusions:

Fragmentation of the information's location, lack of understanding of applicable framework for the processing

The information on data processing in the context of connected vehicles is fragmented across different documents. The information regulating the processing of personal data in the context of connected vehicles can be found in the following locations: the connected car privacy policy 1 and the connected car privacy policy 2. Surprisingly, the app privacy policy does not include information on data processing in this context.

As a result of this fragmentation, it is not clear which is the framework applicable to the processing of personal data in the context of connected vehicle.

Difficult access to the relevant information

The web privacy policy does not include information about the processing of personal data in relation to connectivity functionalities.

Information which is available on the web regarding data processing in this context can be found in the connected car privacy policy 1 and the connected car privacy policy 2. These two documents, nevertheless, are not found in the websites of Brand 3 which present the vehicles and their connectivity functionalities, but it is part of a different web environment addressed at the presentation of Brand 3 app, which is the entity offering connectivity services for Brand 3. This entails that consumers do not have the information available when they are at the consideration stage of the purchase process, thus not being able to fully understand the implications of their potential purchase. Furthermore, the document connected car privacy policy 2, which is the one which best describes the processing in the context of connected vehicles, is not easily available in the Brand 3 websites but require extensive browsing in order to be able to find it.

Article 12 GDPR explains that information must be immediately apparent to data subjects and the Data Protection Working Party 29, in its guidelines on transparency, clarified that this requisite means that "it should be immediately apparent to them [data subjects] where and how this information [referring to information relating to data processing aspects] can be

[187] At the date of publication of this Report, the app privacy is the same as the web privacy policy, as the app links to the web. Therefore, the app does not include information about the processing of personal data by the connected vehicle, despite being an app to control the Brand's connected services.

accessed".[188] This is not the current situation; on the contrary, consumers would need to make a significant time investment just to be able to find the information which is applicable to the processing.

Difficult to find information and inadequate timing

As previously explained, the information related to the processing of personal data in the context of connected vehicles is not provided to the consumer in the moments where this information should be made available to them, i.e., during the consideration stage in the purchase process or before the data is collected and processed. Neither the websites dedicated to presenting the vehicles and their features nor the app privacy policy provide access to this information.

As a consequence, the information is not provided in a timely manner i.e., prior to the processing starts. The Data Protection Working Party 29 explained that providing information on personal data processing "in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 [GDPR] applies, under Article 13.1 the information must be provided 'at the time when personal data are obtained'.[189]

Consent by default regarding geolocation

The document connected car privacy policy 2 states that the consumer must activate the privacy mode if they do not want the vehicle's geolocation data to be used.

Accordingly, consumers have to activate the privacy mode to avoid the processing of their geolocation which seems to be active by default. It remains unclear whether geolocation data is processed in the cases where the app is not downloaded.

Undermining of consumer's control over data through inadequate use of legitimate interest

In the document connected car privacy policy 2 there are several occasions on which legitimate interest is used as the basis for processing. Consent is used only in a few cases.

Legitimate interest is a legal basis to process personal data which can be used by data controllers to the extent that the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".[190] In order to use this legal basis, data controllers need to put in place sufficient safeguards to ensure that data subjects' privacy is preserved and their rights do not prevail over data controller's legitimate interest. Typically, these safeguards include reinforcing transparency and providing an easily accessible opt-out mechanism for users.

The use of legitimate interest in the cases showed in the document does not provide for any of these safeguards: on the one hand, transparency has not been reinforced but, on the contrary, despite the complexity of the information provided to consumers, information is not provided in a timely manner and is not easily accessible. Regarding the opt-out mechanism, the document

[188] *Ibid.,* p. 8.
[189] *Ibid.,* p. 15.
[190] Article 6(1)(f) GDPR.

explains that it is possible to object to processing for legitimate interest through the Brand 3 app. Nevertheless, the opt-out mechanism explained does not exist in the app.

As a result, the use of legitimate interest in this case serves as a way to bypass consent and provide a false illusion of control to the user.

Invalid transfer or outdated information on data transfers outside the EU

In the document connected car privacy policy 2 the information regarding transfers of data outside the EU states that the EU-US Privacy Shield is relied upon to cover the transfer. Nevertheless, this instrument was invalidated by the European Court of Justice and is no longer valid.[191]

[191] Judgment of the Court (Grand Chamber) of 16 July 2020, C-311/18 - Facebook Ireland and Schrems.

D. Brand 4

The following documents were reviewed:

1. Sale and purchase agreement (Spain).
2. Web privacy policy.
3. Privacy policy connected vehicle 1.
4. Privacy policy connected vehicle 2.

After reviewing the abovementioned documentation for the purpose of assessing the clarity of the information and implications on the sharing of vehicle data and whether consumer consent is requested in connection to the use of personal data, including third-party use, we have arrived at the following conclusions:

Generally speaking, Brand 4 offers complete, clear, intelligible and easily accessible information regarding the processing of data in the context of connected vehicles.

During this Study, through the MS exercises, it was possible to verify that Brand 4 makes efforts to comply with privacy and data protection regulations, because the official point of sale visited by the Mystery Shopper had a big banner, located in a visible location in the point of sale where the potential buyer was taken for further understanding of connected capabilities. Another example of these efforts is the fact that Brand 4's privacy policies about the connected vehicle are easily accessible in its website and that, for instance, the privacy policies warn consumers selling their vehicles to reset all the information saved by the vehicle before selling it.

In saying that, there are some aspects that it is worth analysing for the purposes of this Study:

Fragmentation of the applicable framework for the processing

Information regarding data processing in the context of connected vehicles is to be found in two different documents: the privacy policy connected vehicle 1 and the privacy policy connected vehicle 2.

The reason for this separation is not apparent and will likely lead to consumer confusion and information fatigue.

Unclear information regarding an aspect of data sharing

In the two documents that provide information about data processing aspects in relation to connected vehicles, it is mentioned that data from the connected vehicle can be shared with "professional consultants", without further explanation about who this refer to, the reasons for the transfer and the legal basis on which this is covered.

E. Brand 5

The following documents were reviewed:

1. Sale and purchase agreement (Spain).
2. Web privacy policy.
3. App privacy policy.

After reviewing the abovementioned documentation for the purpose of assessing the clarity of the information and implications on the sharing of vehicle data and whether consumer consent is requested in connection to the use of personal data, including third-party use, we have arrived at the following conclusions:

Information is not always available

No information regarding personal data processing relating to vehicle connectivity is provided in the sales and purchase agreement or at the general website privacy policy. The information is neither provided or made available in the websites dedicated to present the vehicles and connectivity functionalities.

This information would therefore be provided or made available to users only and to the extent that they download the app in connection to enjoying Brand 5 connectivity services. Therefore, this suggests that consumers do not get information about the implications of data processing in the context of connected vehicles unless they download the app, and never before.

We have verified that the data processing relating to the eCall functionality is not mentioned in app privacy policies (except in some cases where emergency value-added services are offered) that have been reviewed. Accordingly, this suggests that information in this regard should be provided either in the sales and purchase agreement, or in the vehicle owner's manual. Taking into account that the reviewed sales and purchase agreements do not include any information on this functionality, it seems that the information about this processing is not being made available to consumers, at least, before purchasing the vehicle.

Likewise, whether other connectivity functionalities involving data processing were available and activated without the need to download the app, the information about these processing would not be available for users, at least, before the purchase of the vehicle.

In addition, the information related to the processing of personal data in the context of connected vehicles is not provided to the consumer in the moments where this information might be of relevance to them, i.e., during the consideration stage in the purchase process.

Lack of clarity about data sharing

The document explaining information regarding data processing in the context of connected vehicles is the app privacy policy.

In the section of the document explaining which entities might receive data, Brand 5 explains that data *might* be shared with its partners with the aim of enhancing the services. In relation to this statement, there are several aspects to analyse:

- The use of the verb *might*, makes it unclear whether the transfer will take place or the criteria that can motivate this kind of transfers, for the consumer to understand when they could happen.[192]
- It is not clear which partners it could be referring to and no information is provided for the average consumer to be able to determine, at least, the nature of the partners it could be referring to. This is contrary to the criteria set by the Data Protection Working Party 29 in its guidelines on transparency, which states that "[t]he actual (named) recipients of the personal data, or the categories of recipients, must be provided" or the categories of recipients.
- The legal basis allowing the data sharing between these entities is unclear. If the legal basis was consent or legitimate interest, there is not sufficient information to provide the consumer with actual means of control, i.e., the information about withdrawing consent or opting-out.

[192] The Data Protection WP29 has clarified, in its guidelines on transparency, p. 9, that language qualifiers such as "'may', 'might', 'some', 'often' and 'possible' should also be avoided for transparency purposes. Whether indefinite language ought to be used, it should be justified.

F. Brand 6

The following documents were reviewed:

1. Sale and purchase agreement (Spain).
2. Web privacy policy.
3. App privacy policy.

After reviewing the abovementioned documentation for the purpose of assessing the clarity of the information and implications on the sharing of vehicle data and whether consumer consent is requested in connection to the use of personal data, including third-party use, we have arrived at the following conclusions:

Information is not always available

The analysis of this section is similar to the analysis regarding the Brand 5 app. In this regard, information on these aspects is only provided in relation to the Brand 6 app. We refer to Brand 5 analysis for further reference.

Insufficient information for consumers to understand the implications of the processing of data in the context connected vehicles

The information regarding personal data processing in relation to connectivity functionalities is provided in the app privacy policy.

This information is limited to describing the minimum legal aspects required by Article 13 GDPR, without taking into consideration whether the information provided is sufficient for an average consumer to understand the scope and consequences that the processing entails. From our perspective, the information provided does not allow consumers to get a notion that their vehicle will be processing a variety of data, of very diverse nature and sources, including information, such as geolocation, that might be of special sensitivity, and combining this information to provide the different services under the Brand 6 app umbrella. In particular, the information provided is insufficient to understand the possible risks and implications linked to the purchase of a connected vehicle or the enjoying of the services mentioned.

For instance, there is not information about the service providers with which data can be shared in case the different services are used, the purposes of the sharing or the practical implications of the sharing, for instance, the scope of the information which will be shared. Another example is the limited information about periods for which the data will be stored.

Recital 39 GDPR states that “natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data...”. The Data Protection Working Party 29 recalls in its guidelines on transparency that the principle of transparency is directly linked to the principle of fairness in the sense that a fair processing entails that data subjects must be able, with the information provided, to understand the processing, its scope, consequences and potential risks, in order to achieve the level of protection that the GDPR grants for users. This is especially predicable in relation to processing activities that are complex in nature or were unexpected data processing could take place. Precisely in these situations, the Data Protection Working Party 29 position is that data controllers should not limit themselves to providing the information prescribed under Articles 13 and 14 GDPR but “should also separately spell out in

unambiguous language what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data."[193]

Storage limitation concerns

All information about data processing in the context of connected vehicles is included in the app privacy policy. This document declares that "all data will be stored while account is active and kept for 10 years after inactivity".

In this regard, applying the same criteria to data of very different nature can result in excessive processing, lack of control by the consumers and lengthening of risks. For instance, data that has been obtained through consent, like that related to contact preferences, seems better suited for shorter retention periods once consent has been withdrawn.

Lack of clarity about data sharing

Despite the extensive information regarding the recipients of data shared by the data controller, in all the reviewed documents it is very difficult to understand on what grounds personal data is shared with third parties and whether it can be justified by law.

It seems that data sharing to third entities is never based on consent, no matter the purpose for which the data is shared.

[193] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP260 rev.01, 2018, p. 7.

G. Brand 7

The following documents were reviewed:

1. Web privacy policy UK.
2. Connected vehicle privacy policy UK.
3. Web privacy policy ES.
4. Connected vehicle privacy policy ES.
5. App privacy policy ES.

Inconsistency and fragmentation

Information regarding data processing in the context of vehicle connectivity is fragmented in two ways:

In the first place, there is not uniform information across European jurisdictions, but each jurisdiction has their own documentation, with different content. It seems that each jurisdiction performs different processing activities with the data processed in the context of connected vehicles. This is eye-catching as the Brand 7 OEM is always the data controller, jointly with a local brand.

In the second place, information regarding data processing in the context of vehicle connectivity is scattered across different documents and privacy policies, including the connected vehicle privacy policy available at the website, and the app privacy policy, available after downloading the app.

Incomplete information

The information about vehicle connectivity aspects for Spain is very limited, especially about the type of data collected from the vehicle in the context of connected services. For instance, there is no information about whether data is collected through sensors in the vehicle.

In all reviewed privacy policies, there is very limited information about the rights consumers have in relation to the processing of their personal data. Specifically, in the connected vehicle privacy policy and the app privacy policy, there is not an explanation on what each right mean so consumers can understand what they can do in relation to their data.

Lack of clarity

It is not clear what categories of data are being processed in the context of connected vehicles. For instance, from app, it seems that data collected does not include sensor activity.

There is not clear information about the legal basis used to process personal data. This means that it is not clear when it is necessary to provide consent or whether the processing is necessary for a legal obligation, the provision of a service or whether there is a legitimate interest.

Information about the rights available for consumers and how to exercise them is very limited. In all cases, there is not an explanation of what each right entail neither the way to exercise them. It is therefore not possible for users to know to what they can withdraw consent or object to processing.

As a result, it is not clear for an average user to understand the implications of the complex processing involved in vehicle connectivity contexts, nor information to understand their rights and how to exercise them.

Storage limitation concerns

The analysis at this point is similar to that explained in the Brand 6 section for Brand 6 app. We refer to that section for further reference.

Lack of clarity about data sharing

The analysis at this point is similar to that explained in the Brand 6 section for Brand 6 app. We refer to that section for further reference.

V

Appendix V: Bibliography

Articles (authors in alphabetical order)

Centre on Regulation in Europe ("cerre"), *Making data Portability More Effective for The Digital Economy*, 2020. Available at: https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf. Last accessed: 30/11/2021.

EDPS, Preliminary Opinion of the European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, 2014. Available at: https://edps.europa.eu/sites/default/files/publication/14-03-26_competitition_law_big_data_en.pdf. Last accessed: 30/11/2021.

Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P. Markatos, *User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users, In Proceedings of the Web Conference*, 2021. Available at: https://arxiv.org/pdf/2102.08779.pdf. Last accessed: 30/11/2021.

Engers, Tom & de Vries, Dennis, *Jusletter-IT privacy-on-wheels*, 2019, p. 4. Available at: https://www.researchgate.net/publication/332029756_Jusletter-IT_privacy-on-wheels_c73e8c1672_de. Last accessed: 30/11/2021.

European Commission, *Competition policy for the digital era*, 2019. Available at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. Last accessed: 30/11/2021.

European Commission, *Digital Transformation Monitor – The race for automotive data, 2017*. Available at: https://ati.ec.europa.eu/sites/default/files/2020-05/The%20race%20for%20automotive%20data%20%28v1%29.pdf. Last accessed: 30/11/2021.

Félicien Vallet, *The GDPR and Its Application in Connected Vehicles—Compliance and Good Practices*, 2019. Available at: https://www.researchgate.net/publication/333374054_The_GDPR_and_Its_Application_in_Connected_Vehicles-Compliance_and_Good_Practices. Last accessed: 30/11/2021.

FIA Region I and others, *Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach*, 2021. Available at: https://www.fiaregion1.com/wp-content/uploads/2021/03/2021-02-S-OTP-Paper-vFin.pdf. Last accessed on 30/11/2021.

Gaspare Fiengo, Giulia Lovaste, 2021, *Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform*, Legal Study, 2021. Available at: https://www.fiaregion1.com/wp-content/uploads/2021/06/FIA-Final-Report-ISPs-Liabilities-20210531.pdf. Last accessed: 30/11/2021.

Graef, Inge and Husovec, Martin and van den Boom, Jasper, Spill-Overs in Data Governance: *The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, 2019, TILEC Discussion Paper No. DP 2019-005. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3369509 or http://dx.doi.org/10.2139/ssrn.3369509. Last accessed: 30/11/2021.

Gill, Daniel and Kerber, Wolfgang, *Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data,* 2020. Available at SSRN: https://ssrn.com/abstract=3715357 or http://dx.doi.org/10.2139/ssrn.3715357. Last accessed on 30/11/2021.

Kerber, Wolfgang and Frank, Jonas, *Data Governance Regimes in the Digital Economy: The Example of Connected Cars*, 2017. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064794 or http://dx.doi.org/10.2139/ssrn.3064794. Last accessed: 30/11/2021.

Kerber, Wolfgang, *Data-Sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars*, 2019. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3445422 or http://dx.doi.org/10.2139/ssrn.3445422. Last accessed: 30/11/2021.

Kerber Wolfgang, *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 2019, JIPITEC 310. Available at: https://www.jipitec.eu/issues/jipitec-9-3-2018/4807. Last accessed: 30/11/2021.

Kerber, Wolfgang and Zolna, Karsten K., *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, 2020. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3719098 or http://dx.doi.org/10.2139/ssrn.3719098. Last accessed: 30/11/2021.

Matte, Célestin & Santos, Cristiana & Bielova, Nataliia, *Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?*, 2020. Available at: https://hal.inria.fr/hal-02566891/document. Last accessed: 30/11/2021.

McMurren, Juliet and Verhulst, Stefaan G., Data to Go: The Value of Data Portability as a Means to Data Liquidity, Juliet McMurren and Stefaan G. Verhulst, 26/10/2021. See: https://medium.com/data-stewards-network/data-to-go-the-value-of-data-portability-as-a-means-to-data-liquidity-682bb39368e0. Last accessed: 30/11/2021.

Michal S Gal, Oshrit Aviv, *The Competitive Effects of the GDPR, Journal of Competition Law & Economics*, Volume 16, Issue 3, 2020. Available at: https://academic.oup.com/jcle/article/16/3/349/5837809?login=true. Last accessed: 30/11/2021.

Nadezhda Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology*, 2018, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176. Available at: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176. Last accessed: 30/11/2021.

OECD, *Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies*, 2019. Available for payment at: Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies | OECD iLibrary (oecd-ilibrary.org).

Osborne Clark, *What EU Legislation says about car data - Legal Memorandum on Connected Vehicles and Data, Legal Study Commissioned by FIA Region I in the context of the My Car My*

Data Campaign, 2017. Available at: https://www.fiaregion1.com/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf. Last accessed: 30/11/2021.

Statista Digital Market Outlook – Market Report, Connected Car Report 2019, 2018. Available for payment at: https://www.statista.com/study/43034/connected-car-report/.

Tuvit - M. Bartsch, A. Bobel, Dr. B. Niehöfer, M. Wagner, M. Wahner, *On-Board Telematics Platform Security*, 2020. Available at: https://www.fiaregion1.com/wp-content/uploads/2020/06/20200615_FIA_vehicle_security_report.pdf. Last accessed on 30/11/2021.

Political initiatives (in chronological order)

EU Commission, A Digital Single Market Strategy for Europe, 6.5.2015, COM(2015) 192 fin. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN. Last accessed: 30/11/2021.

EU Commission, A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, 30.11.2016, COM(2016) 766 fin. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766. Last accessed: 30/11/2021.

EU Commission, C-ITS Platform – Final Report, 2016. Available at: https://transport.ec.europa.eu/system/files/2016-09/c-its-platform-final-report-january-2016.pdf. Last accessed: 30/11/2021.

EU Commission, Building a European data economy, 10.1.2017, COM(2017) 9 fin. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN. Last accessed: 30/11/2021.

EU Commission, Towards a common European data space, 25.4.2018, COM(2018) 232 fin. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0232:FIN. Last accessed: 30/11/2021.

C-ITS TRL, Access to In-Vehicle Data and Resources – Final Report (2017). Available at: https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf. Last accessed on: 30/11/2021.

EU Commission, On the road to automated mobility: An EU strategy for mobility of the future, 17.5.2018, COM(2018) 283 fin. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0283:FIN:EN:PDF. Last accessed: 30/11/2021.

European Commission Staff Working Document, Guidance on sharing private sector data in the European data economy, Accompanying the document, "Towards a common European data space", 25.4.2018, SWD(2018) 125 fin. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:125:FIN. Last accessed: 30/11/2021.

EU Commission, A European strategy for data, 19.2.2020, COM(2020) 66 fin. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066. Last accessed: 30/11/2021.

Legislation in force – directives (in chronological order)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as revised by directive 2009/136/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058. Last accessed: 30/11/2021.

Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance), OJ L 162, 21.6.2008, p. 20–26. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0063. Last accessed: 30/11/2021.

Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040. Last accessed: 30/11/2021.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024. Last accessed: 30/11/2021.

Legislation in force – regulations (in chronological order)

Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (Text with EEA relevance), OJ L 171, 29.6.2007, p. 1–16, as amended by subsequent regulations and as developed by delegated acts. Available at: EUR-Lex - 32007R0715 - EN - EUR-Lex (europa.eu). Last accessed: 30/11/2021.

Regulation (EU) 2015/758 of the European Parliament and of the Council 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, OJ L 123, 19.5.2015, p. 77–89. Available at: EUR-Lex - 32015R0758 - EN - EUR-Lex (europa.eu). Last accessed: 30/11/2021.

Regulation (EU) 2016/679 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 (General Data Protection Regulation). Available at: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu). Last accessed: 30/11/2021.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the EU (Text with EEA relevance.),

PE/53/2018/REV/1, OJ L 303, 28.11.2018, p. 59–68. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807. Last accessed: 30/11/2021.

Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users. Available at: https://eur-lex.europa.eu/eli/reg/2019/2144/oj. Last accessed: 30/11/2021.

Proposed legislation

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications):

- European Commission version. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52017PC0010. Last accessed: 30/11/2021.
- European Parliament version. Available at: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html?redirect. Last accessed: 30/11/2021.
- Council of the EU version. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=ENn. Last accessed: 30/11/2021.

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final. Available at: EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu). Last accessed: 31/11/2021.

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.12.2020 COM(2020) 842 final 2020/0374 (COD). Available at: https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf. Last accessed: 30/11/2021.

Proposal for a Regulation on Type approval of motor vehicles regarding access to in-vehicle generated data. Available at: In-vehicle generated data – EU rules for services based on access to car data (europa.eu). Last accessed: 30/11/2021.

Guidelines from supervisory authorities (in chronological order)

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20.6.2007. Available at: 12251/03/EN (europa.eu). Last accessed: 30/11/2021.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2.4.2013. Available at: Draft outline for WP29 opinion on "purpose limitation" (europa.eu). Last accessed: 30/11/2021.

Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9.4.2014. Available at: Legitimate interest opinion (europa.eu). Last accessed: 30/11/2021.

Article 29 Data Protection Working Party, Guidelines on the right to "data portability", 5.4.2017, WP 242 rev.01. Guidelines endorsed by the EDPB. Available at: wp242_rev_01_en_D8A6FCF6-9039-846A-0C8040819826D818_44099.pdf. Last accessed: 30/11/2021.

CNIL, Compliance package for a responsible use of data in connected cars, 2017. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf. Last accessed: 30/11/2021.

International Working Group on Data Protection in Telecommunications, Report on connected vehicles, 9-10.4.2018. Available at: 2018-IWGDPT-Working_Paper_Connected_Vehicles.pdf (datenschutz-berlin.de). Last accessed: 30/11/2021.

European Data Protection Supervisor, TechDispatch on Connected Cars, Issue 3, 20.12.2019. Available at: TechDispatch #3: Connected Cars | European Data Protection Supervisor (europa.eu). Last accessed: 30/11/2021.

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, 12.3.2019, p.14. Available at: TechDispatch #3: Connected Cars | European Data Protection Supervisor (europa.eu). Last accessed: 30/11/2021.

European Data Protection Board, Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications European Data Protection Board, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, version 2.0, 9.3.2021. Available at: edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf (europa.eu). Last accessed: 30/11/2021.

Article 29 Data Protection Working Party, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 4.5.2021. Available at: edpb_guidelines_202005_consent_en.pdf (europa.eu). Last accessed: 30/11/2021.

European Data Protection Board, statement 03/2021 on the ePrivacy Regulation, 9.3.2021. Available at: EDPB (europa.eu). Last accessed: 30/11/2021.

CASE LAW

Court of Justice of the European Union, Judgment of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland – C-582/14. Available at: https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN. Last accessed: 30/11/2021.

Court of Justice of the European Union, Judgment of 16 July 2020, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems – C-311/18. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3569845. Last accessed: 30/11/2021.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over
150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

ey.com/es_es

FIA

The Fédération Internationale de l'Automobile (FIA) Region I, based in Brussels, is a consumer body comprising 103 Mobility Clubs that represent over 36 million members from across Europe, the Middle East and Africa. The FIA Region I represents the interests of our members as motorists, riders, pedestrians and passengers. We work to ensure safe, affordable, clean and efficient mobility for all.

Learn more at www.fiaregion1.com

Performed by:

Building a better working world

Commissioned by: