Study on the provision of information to consumers about the processing of vehicle-generated data

Final report

Written by: *Ipsos and Time.lex*

January - 2023

EUROPEAN INNOVATION COUNCIL AND SMES EXECUTIVE AGENCY

EUROPEAN COMMISSION

Directorate-General for Justice and Consumers

Contact (DG JUST): Clemens SCHUBERT

E-mail: just-e3@ec.europa.eu

European Commission
B-1049 Brussels

Implemented under the Contract n° 2020 85 07 under the Framework Contract n° CHAFEA/2018/CP/03 with Consumers, Health, Agriculture and Food Executive Agency (CHAFEA) acting as Contracting Authority, replaced by European Innovation Council and SMEs Executive Agency (EISMEA) as of 1 April 2021 (Commission Implementing Decision (EU) 2021/173 of 12 February 2021)

LEGAL NOTICE

DS-05-23-007-EN-N
ISBN 978-92-76-99073-4
doi: 10.2838/745640

Luxembourg: Publications Office of the European Union, 2023

Study on the provision of information to consumers about the processing of vehicle-generated data

Final report

Contents

1. INTRODUCTION 6
2. BACKGROUND AND RESEARCH OBJECTIVES 7
3. STUDY OVERVIEW AND METHODOLOGY 10
   - 3.1. Overview of the conducted work 10
   - 3.2. Scope of the study 11
   - 3.3. Detailed methodology for each task 16
4. STUDY RESULTS 23
   - 4.1. Notes on the interpretation of the results 23
   - 4.2. Mapping of the relevant regulatory framework 26
   - 4.3. Consumers' expectations 53
   - 4.4. Assessment framework 69
   - 4.5. Traders' practices 78
   - 4.6. Recommendations 85
5. ANNEX 1 – FEEDBACK ON EACH MANUFACTURER 88
   - 5.1. BMW 88
   - 5.2. Hyundai 97
   - 5.3. Peugeot 101
   - 5.4. Renault 106
   - 5.5. Tesla 112
   - 5.6. Toyota 119
   - 5.7. Volkswagen 123
6. ANNEX 2 – ASSESSMENT SCOPE FOR EACH MANUFACTURER 129

1. Introduction

This report presents the final findings of a study on the provision of information to consumers about the processing of vehicle-generated data. The central goal of this study was to gain insight into the legal requirements (from an EU consumer law perspective) and consumer expectations when it comes to the provision of information about data processing that occurs as part of the internet-connected services of cars, and to compare these requirements and expectations against actual practices among large car manufacturers in a selection of European markets that sell connected cars. This comparison formed the basis for an analysis of these manufacturers, in order to identify best practices and areas where improvement is needed. This, in turn, formed the basis for the formulation of concrete recommendations about actions that manufacturers could take in this regard.

The report provides an overview of the background of the study and the research objectives (Chapter 2), describes the methodology used for the study (Chapter 3), and gives a detailed overview of the study results and the conclusions and recommendations drawn from these results (Chapter 4). The findings in this report are also supported by a detailed examination of individual manufacturers by the study team, presented in Annex 1.

2. Background and research objectives

Connected cars and vehicles process data on the surrounding area, the car and the driver ([1]). These data are not only stored in the car; they can also be shared with manufacturers or other service providers, other cars, devices and road infrastructure, enabling the car to digitally connect and interact with its surroundings ([2]). Some connectivity technologies have already been implemented in the vast majority of today's cars, such as event data recorders, which collect operational data related to crashes or on-board diagnostic information to measure emissions and identify performance issues. Other technologies are increasingly provided in new cars. These include location information and user recognition, among others ([3]). Data are used and shared in different ways: for instance, aggregate data can be used for traffic flow optimisation, road hazard identification or congestion management; and individual car data are shared to facilitate the provision of roadside assistance, electric vehicle charging or parking payments ([4]).

The global connected car market size is expected to more than triple between 2020 and 2027 ([5]), with a compound annual growth rate of 26 % ([6]). This predicted growth suggests that in the very near future connected cars will no longer be luxury models, limited to premium brands, but will be sold as midmarket models. Senior executives from the world's leading automotive companies predict that connectivity and digitalisation will remain the most important trends until 2025, only ranking behind battery electric vehicles ([7]).

This growth is also reflected in consumers' attitudes towards connected cars: interest in connected cars is high in European countries, and many consumers envisage that their next car will have features that allow it to communicate with its surroundings ([8]), implying that it will share data with other vehicles, devices or road infrastructure ([9]).

With this growing connected car market, there is also a steady increase in the exchange and use (i.e. processing) of consumers' personal data generated by connected cars. These data are not only used within cars; they are also increasingly becoming a valuable source of information for car manufacturers and third-party companies engaged in related businesses, such as insurance companies. Therefore, connected cars are turning into massive (personal) data hubs. Until now, regulatory guidelines and recommendations have focused on the proper treatment of personal data from a data

---

([1]) Marktwächter Digitale Welt, 2017. *Connected Car nimmt Fahrt auf – wohin steuert das Auto der Zukunft?* Verbraucherzentrale NRW, Düsseldorf.

([2]) PwC, 2015. *Internet of Things – Connected cars*.

([3]) National Automobile Dealers Association and Future of Privacy Forum, 2017. *Personal Data in Your Car.*

([4]) Otonomo, 2019. *A Privacy Playbook for Connected Car Data.*

([5]) It needs to be kept in mind that in response to the COVID-19 outbreak various automobile companies in Europe have temporarily shut down or reduced or suspended production, which has led to a strong fall in global trade and slowed down connected car market growth (Fortune Business Insights, 2020. *Market Research Report* (https://www.fortunebusinessinsights.com/industry-reports/connected-car-market-101606, last accessed: 20 December 2022)).

([6]) Fortune Business Insights, 2020. *Market Research Report* (https://www.fortunebusinessinsights.com/industry-reports/connected-car-market-101606, last accessed: 20 December 2022).

([7]) KPMG, 2017. *Global Automotive Executive Survey 2017*.

([8]) Federation Internationale de l'Automobile (FIA) Region I, 2016. *What Europeans Think about Connected Cars*, FIA Region I, Brussels.

([9]) Otonomo and SBD Automotive, 2020. *What European consumers think about connected car data and privacy.*

protection point of view ([10]). At the same time, they also have a strong consumer protection and consumer rights angle, which has received much less attention. Indeed, consumers are known to share concerns about the use and sharing of their personal data beyond data protection concerns. Their main concerns relate to the disclosure of information, the commercial use of personal data and vehicle hacking. While a majority of consumers seem to feel comfortable transmitting vehicle breakdown diagnostic data and other vehicle data, they do not feel comfortable sharing the identity of the driver or the emails they have sent or the telephone numbers they have called ([11]). Certainty that personal data are not disclosed to another party would increase their trust in connectivity features in their vehicle ([12]).

In this regard, it is crucial that the perspective of consumers is taken into account when developing guidelines and policies regarding the treatment of personal data in connected cars. Indeed, there is growing demand to consider consumer expectations, to increase their confidence and trust in connectivity features. This includes the need to obtain valid consent from the consumer for every transaction that may include the processing of personal data, providing them with different options for types of (car) data that they can share and using plain language to ensure that they understand what data they are agreeing to share. Recent research has also clearly shown that consumers expect to be in full control of any data collected related to the vehicle they own or drive and of the transmission/sharing of these data. Most notably, they would like to have the option to deactivate connectivity features and decide when and for how long data are shared ([13]).

With the above context in mind, the main goal of this study was to assess **how car manufacturers and (licensed) car dealers** ([14]) **comply with their obligations under the relevant EU consumer law**, with regard to the **provision of the clear and transparent information on the processing of vehicle-generated data** that consumers need in order to make a **fully informed purchasing decision**.

More specifically, the research objectives of the project were as follows:

- to better understand **what information consumers consider most important** when it comes to the processing of vehicle-generated data in connected cars, and the level of compliance of car manufacturers and licensed car dealers with their obligations under EU consumer law with regard to the provision of such information during the marketing and pre-contractual phases of commercial communication;

- on the basis of this understanding, provide a set of preliminary recommendations to car manufacturers and licensed car dealers on how to improve the provision of information to consumers during the marketing and pre-contractual phases of

([10]) European Data Protection Board (EDPB), 2020. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed: 20 December 2022).
([11]) FIA Region I , 2016. *What Europeans Think about Connected Cars*, FIA Region I, Brussels.
([12]) Deloitte, 2017. *Automotive Data Treasure – Vehicle digitalisation and the question of data treasures*.
([13]) FIA Region I, 2016. *What Europeans Think about Connected Cars*, FIA Region I, Brussels; Deloitte, 2017. *Automotive Data Treasure – Vehicle digitalisation and the question of data treasures*.
([14]) That is, car dealers that operate under a franchise of or by certification from a specific car manufacturer.

commercial communication on the processing of vehicle-generated data by connected cars.

3. Study overview and methodology

3.1. Overview of the conducted work

Figure 3.1 below provides a schematic overview of the objectives of the study, the different tasks conducted as part of the study and how these tasks helped in reaching the objectives. These tasks were as follows.

- **Task 1. The team mapped the relevant EU consumer law provisions** regarding informing consumers of the processing of vehicle-generated data that apply during the marketing and pre-contractual phases of commercial communication and, where relevant, their interface with relevant provisions from other areas of EU law ([15]). This task served to identify the legal requirements that traders have to abide by in providing information about vehicle-generated data. The study focused on consumer law and not on the legal domain of personal data protection. To avoid any possible misunderstandings, the study did not assess consumers' concerns through the application of data protection laws, nor through any test based on these laws.

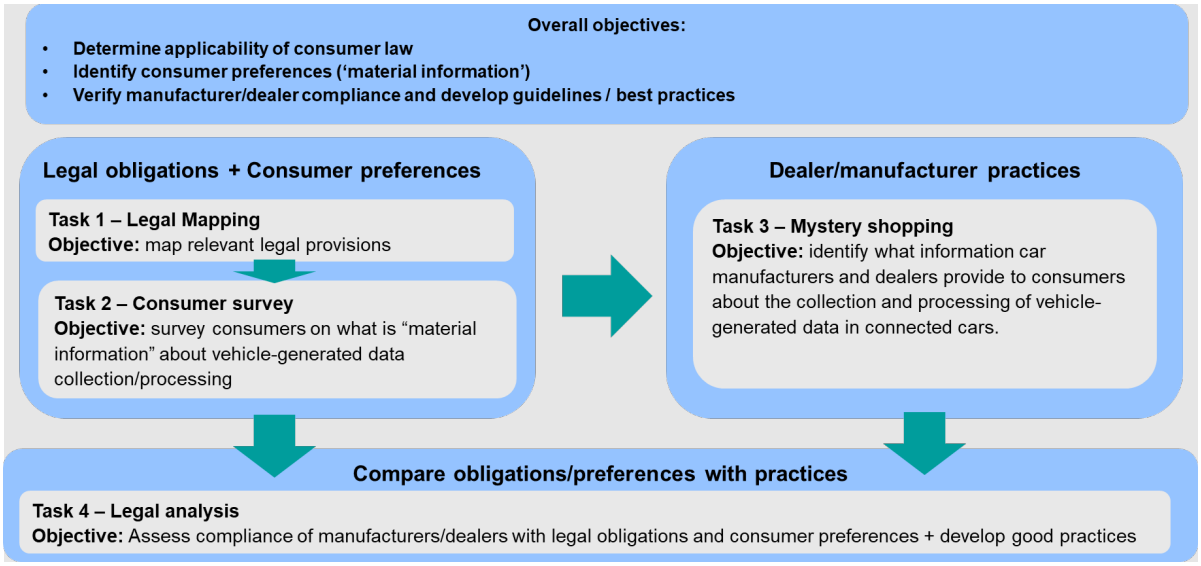
- **Task 2. A consumer survey assessed consumers' expectations** of receiving material information about the processing of vehicle-generated data in connected cars.

- **Task 3. A mystery shopping exercise** investigated whether and how car dealers and manufacturers in seven EU Member States provide information on the processing of vehicle-generated data. This task consisted of physical dealership visits as well as the analysis of printed and online documents.

- **Task 4.** In the last task, **a legal analysis** was conducted by the study team on the results of the mystery shopping exercise, comparing them with the regulatory requirements of consumer law and consumer expectations, in order to examine manufacturers' practices.

([15]) It should be noted that EU directives need to be transposed into the national legal orders of the Member States. In order to facilitate this exercise, the study focused only on the text of the directives as far as EU directives are concerned and not on the national implementing laws.

Figure 3.1. Schematic overview of the study



3.2. Scope of the study

The work for this study was conducted based on explicitly defined concepts and within boundaries in terms of:

- the legal framework that was considered relevant;
- the definition of what constitutes 'material information' for consumers and how the requirements manufacturers/dealers have to abide by are established;
- which manufacturers were studied;
- the geographical area within which data were collected.

3.2.1. Legal scope

The study focused on the provision of clear and transparent information on the processing of vehicle-generated data that consumers need in order to make fully informed purchasing decisions (i.e. material information, as referred to in Articles 6 and 7 of the Unfair Commercial Practices Directive (UCPD) ([16]) and the pre-contractual information required by Article 5 of the Consumer Rights Directive (CRD)) ([17]). It

([16]) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, OJ L 149, 11.6.2005, pp. 22–39.

([17]) Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament

considered that car manufacturers and other actors may use vehicle-generated data for commercial purposes or other purposes that may directly or indirectly affect the interests of the consumer, who is not always sufficiently aware of the collection, processing, transmission or use of the data, or of the true impact thereof. Such data can, in most cases, be considered **personal data**, as defined in the General Data Protection Regulation (GDPR) ([18]), as these data constitute information about a natural person who is identifiable ([19]). The data may reveal information about the consumer's location and other locations visited, driving behaviour, etc. Consumers' (personal) data can be used to target them with marketing information, or can be shared (for a fee) with insurance companies in order to calculate their insurance premiums or to modify or exclude insurance obligations. The data can also be used by car manufacturers to follow up on the conditions of the guarantee or for maintenance, etc. These were the concerns that were considered.

Thus, the focus was on **transparency and information obligations** (set out mainly in the UCPD and the CRD), specifically in relation to information that may have an impact on the consumers, with or without their awareness (an impact that may occur in different stages of the ongoing consumer relationship). Furthermore, the documents, formal or informal, that bind the consumer or are used as evidence of their explicit or implicit consent to information sharing in line with certain contractually binding provisions (even contractual provisions of third parties) were considered important (referring mainly to the Unfair Contract Terms Directive (UCTD)) ([20]). The control that consumers may exercise over their rights was also considered important (for example, to prevent the trader unilaterally modifying terms and conditions or modifying the services).

The usability and requirements of the connected system (e.g. the compatibility of certain products ([21]), such as smartphones, and the issue of consumers being locked in to the system ([22])), which can be linked to the CRD and the Sales of Goods Directive, were considered less important given the amount of information that had already been collected through the research, but are still included in the research.

The study also examined whether certain provisions of the annexes to the directives could apply. In this respect, we found that point 22 of Annex I to the UCPD, concerning

---

and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, pp. 64–88.

([18]) 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, OJ L 119, 4.5.2016, pp. 1–88. 'Personal data' is defined in Article 4(1).

([19]) For a detailed overview of which data may be considered personal in this context, see, for example, EDPB, 2020. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed: 20 December 2022), in particular Nos 1 and following and Nos 59 and following.

([20]) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, pp. 29–34.

([21]) This may have an impact on data portability.

([22]) When consumers cannot migrate their data to different systems and/or different cars and are de facto forced to continue to allow data processing in order to be able to drive their cars or to drive them safely, they are locked in to their current system without a reasonable possibility of switching to alternative products. This evidently limits the scope of consumers' choice.

the hiding of the commercial intent of the trader, was applicable, as well as point 1(i) of the annex to the UCTD (stating that consumers must have had the opportunity to become acquainted with the contractual terms), point 1(j) (providing that traders must not alter the terms of the contract unilaterally, or at least respect certain conditions) and point 1(k) (stating that traders must not alter unilaterally without a valid reason any characteristic of the product or service).

Having regard to the volume of our overall findings and the theoretical issues that needed to be analysed in our report, it was considered that the forbidden practice 'including in marketing material an invoice or similar document seeking payment which gives the consumer the impression that he has already ordered the marketed product when he has not' (Annex I to the UCPD, point 21) was not directly relevant in the context of data capturing.

The general description of the relevant consumer rights and the corresponding obligations of traders concerning information was complicated given the overlap between various consumer law provisions. The relevant provisions of Articles 6 and 7 UCPD, Article 5 CRD, and Articles 3 and 5 UCTD relate to overlapping situations and have common purposes, while at the same time there are relevant differences between them. Furthermore, these rules apply to different stages of the marketing and pre-contractual phases of commercial communication. The study determined that these differences and the conditions for the application of the rules needed a description that was sufficiently detailed. This resulted in the inclusion in the study of an extensive theoretical output.

We emphasise that, while this study concerns the provision of information on the processing of vehicle-generated data, it only focuses on the requirements in this respect under EU consumer law, and not under EU data protection law (i.e. mainly the GDPR and the e-Privacy Directive ([23])). In this study, the study team solely examined the provision of information, lack of transparency thereof or its omission through the application of compliance tests that exist under EU consumer law. It does not examine these through the application of compliance tests that exist under EU data protection law. As examined further in Section 4.2, the framework of EU consumer law and the framework of EU data protection law are considered separate legal frameworks that can both be applied independently, and that are regarded not as exclusive but as complementary. Both have their own objectives, scopes and requirements, and they call for different compliance tests. Therefore, the assessments, results and conclusions of the study cannot be regarded as assessments, results or conclusions in relation to EU data protection law.

Moreover, although the study team examines the practices of car manufacturers and dealers in detail, the study does not intend to make legal judgements about these practices. The factual findings and conclusions of the study do not state or imply that a certain observed practice constitutes an infringement of any existing legal provision. The identification, assessment and enforcement of measures to combat infringing practices remain the exclusive responsibility of the authorities competent to decide on these aspects under the respective legal frameworks. Such decisions will depend on a

([23]) 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 (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47.

case-by-case assessment of the relevant practices, considering all the relevant circumstances of each case.

3.2.2. Definition of 'material information'

A central concept in this study is that of material information. In particular, the study investigates whether manufacturers and car dealers adequately provide such material information about data processing in connected cars to consumers. Material information, under the UCPD guidelines, is defined as information that the average consumer needs to make a fully informed purchasing decision ([24]). More specifically, it is information that is likely to influence a transactional decision, either by its presence or by its absence. Put concretely, if such material information is withheld from the consumer, they might decide to purchase the good or subscribe to the service, whereas they might not have done so if the information had been given. This creates a risk of detriment due to the consumer purchasing or subscribing to an unwanted good or service, incorrectly using the product, or being subjected to service provisions and/or contract obligations they were not aware of.

In the context of this study, the primary source used to establish what information a consumer needs to receive must always be the information that traders are explicitly required to provide under the applicable law, as introduced in Section 3.2.1 above and as discussed extensively in Section 4.2 (especially Sections 4.2.1.4 and 4.2.1.5). It is, however, possible that what consumers find it most important to receive information about when they are considering purchasing a connected vehicle goes beyond those legal requirements; that is, while the applicable legislation requires traders to provide consumers with certain information that is generally considered to be important, consumers may immediately also be interested in other aspects and are likely to ask traders spontaneously about information that is not explicitly required by the applicable law. Therefore, this subjective consumer perspective was very useful in setting priorities for the assessment performed in this study and ultimately for competent authorities, who are, in line with the applicable legislation, responsible for assessing what information an average consumer would consider so important (i.e. material) that it could affect their decision to purchase or not to purchase a connected car. Specifically, the topics that were found to be most important relative to other topics received higher scrutiny in our evaluation of the information provided by traders, although without losing sight of those topics that consumers were seemingly relatively less interested in but are nonetheless crucial from a purely legal perspective.

3.2.3. Geographical scope

Data collection for the study took place in seven EU Member States: **Germany**, **Ireland**, **Spain**, **France**, **Italy**, **Poland** and **Sweden**. These Member States were selected so

([24]) As described in European Commission, 2021. Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, OJ C 526, 29.12.2021 (UCPD guidance), pp. 1–129, Section 2.9.1.

that there would be an appropriate mix of Member States in terms of geography, country size and sales volume of connected cars. While this allows for some validity of the study results for the wider EU / European Economic Area (EEA), we emphasise that the findings of the report presented here only pertain to the Member States for which data were collected, and that we draw no conclusions about the situation in other EU/EEA countries.

This scope is specifically relevant to the following tasks.

- Task 2: the online consumer survey to identify consumer preferences and expectations with regard to providing information about processing of vehicle-generated data by connected cars. This survey was conducted in the seven Member States mentioned above.

- Task 3: the mystery shopping exercise that took place in these seven Member States. This applies to both the physical dealership visits and the assessment of printed and digital information, which was restricted to what was available in these Member States (e.g. the national manufacturers' websites).

The geographical scope was also relevant to the determination of the manufacturer scope (see the next section): the study covered the connected car models most sold in these seven Member States, in order to avoid investigating models with low sales volumes in these specific Member States (with the exception of Tesla, the inclusion of which was not based on sales data; see the next section).

3.2.4. Manufacturer scope

Data collection for this study focused mostly on the most sold car models with connected services (standard or optional), with only one model per manufacturer considered, and at least two non-European manufacturers/models included. Based on these provisions and on car sales data within the seven EU Member States in the scope of the study, the six largest manufacturers were identified: Volkswagen, Renault, Peugeot, Toyota, BMW and Hyundai. In addition to these six manufacturers, Tesla was also included in the study. Tesla was selected not because of its sales figures but because of its large market share in the electric vehicle segment and its overall focus (also in the perception of consumers) on software and the 'smart' use of data as part of its branding, making it a relevant manufacturer to include in the study.

For each of these models, the most sold model (and trims within this model) that offered (by default or optionally) connected services were identified. These are presented in Table 3.1.

Table 3.1. Models and trims included in the study

Manufacturer	Model	Trim ([a])
Volkswagen	Golf	All trims
Renault	Clio	All trims
Peugeot	5008	Roadtrip, GT and GT Pack trims

Toyota	Corolla	All trims
BMW	3 Series	All trims
Hyundai	Kona	Prime trim and higher
Tesla	Model 3	All trims

([a]) Trim names were adapted where necessary depending on the name used in each Member State.

3.2.5. Mystery shopping scope

The mystery shopping exercise covered **the process of purchasing a connected car before the actual purchase (i.e. agreement to pay) of the car**. While it was common that the full purchasing process could not be completed in one visit to the dealer, including two visits per mystery shopping exercise would have caused the timing of the mystery shopping exercise to become highly unpredictable: the time between the first and second visits can be very long, depending on the availability of the car and the **order book of the dealer**. Multiple shopping visits per manufacturer were conducted to compensate for this.

Some services from manufacturers or third-party service providers in the area of 'connectedness' could also be offered or made available **after** the purchase of the car. This did not mean that the information the consumer received about these services and the data processing involved before the purchase could not be checked; indeed, that was the purpose of the visits. However, any information and materials that would only be made accessible after the purchase of the car were not evaluated in this study. This could happen, for instance, because separate registration procedures, the purchase of a separate service, proof of car ownership, the downloading of a smartphone app, etc. could be required to access this information.

This did not hinder the fulfilment of the study's research objectives. Indeed, the main objective was to evaluate whether information given to the consumer is compliant with the legal framework for information provision and in line with what the consumer finds important in order to make an informed decision on purchasing a car. By definition, the consumer can only do this based on the information that is provided prior to the purchase of the car.

3.3. Detailed methodology for each task

This section provides more detailed information about the design and implementation of each of the different tasks, and how they feed into each other as well as into this final report.

3.3.1. Task 1 – Legal mapping

3.3.1.1. Design

The purpose of Task 1 was to provide an overview of how EU consumer law and, possibly, other relevant EU legislation apply during the marketing and pre-contractual phases of commercial communication as regards the processing of vehicle-generated data by connected cars. The focus of the research was on the EU consumer protection legislation and its interface with other relevant areas of EU law, for example data protection legislation. The purpose was not to analyse the data protection legislation as such ([25]); however, the data protection legislation and the literature in this field provided the practical context for describing the interface (i.e. that there exists a point of intersection) with consumer law.

The legal mapping consisted of the following steps.

1. Identification of the relevant regulatory framework

First, an inventory was made of the obligations stated primarily under the UCPD, the UCTD and the CRD, and they were linked to the purchase of a connected car.

We also studied whether other legal instruments could come into play (such as the Consumer Sales Directive, e-Call and the Cybersecurity Regulation (Regulation (EU) 2019/881)). These instruments were considered irrelevant to consumer protection issues in the context of the study. Furthermore, we excluded specific issues related to distance sales, as the study covered not online purchases but purchases by consumers who completed face-to-face transactions with traders, where the consumers interacted with the traders, received some information and contractual or 'informative' documents during the interaction, and were normally able to try out the cars and their data connection systems.

2. Analysis of the relevant legislation

The analysis aimed to clarify the obligations of the traders, considering the time when obligations must be fulfilled and the criteria and conditions that are required for the application of certain obligations. It related the obligations to the impacts that they have on the transactional decision of the average consumer, in a certain time frame or certain circumstances, etc. Certain concepts, such as the ideas of an invitation to purchase and material information, were analysed and applied to the cases that were relevant, that is, those involving the purchase of a connected car, which may involve certain risks in relation to the use of the data collected.

([25]) See, for an analysis of the data protection legislation in relation to connected vehicles, EDPB, 2020. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed: 20 December 2022).

Obligations set forth in different instruments were grouped into workable themes. The trader's duty to provide correct and sufficient information was by far the most important obligation, which already required a deep analysis in itself. This duty spanned a large part of the three directives that were studied. We studied the clarity of information and the clarity of terms and conditions (in privacy policies as well as the directives) as separate topics. We presented the issues regarding the unilateral modification of contractual terms and the characteristics of goods and services as a separate theme under the sources of legislation. As we had presumed, aggressive practices were deemed less obvious than misleading practices, although the rule concerning aggressive practices was applied in our context. We referred to that, but not as a separate theme. The 'catch-all' general prohibition of acting against professional diligence (Article 5 UCPD) was applied in our context and was listed as a separate theme.

The relevant legal sources were identified through desk research. Desk research focused on international legal handbooks, articles in legal magazines and on websites, the Commission guidelines/notices on the relevant directives, case-law, and enforcement actions and policies of surveillance authorities where available. Printed materials and online materials were consulted and reviewed in different languages. Case-law and enforcement actions were mainly found in Germany and the Scandinavian countries (particularly Norway). We used examples in the field of connected products (wristbands and toys) and social media.

3.3.1.2. Output and use

A full description of the results of the legal mapping can be found in Section 4.2.

The legal mapping identified the legal requirements that car manufacturers and dealers need to abide by when it comes to the provision of information to consumers on the processing of vehicle-generated data by connected cars. These requirements informed the scope and priorities of the mystery shopping exercise (i.e. what needed to be checked in that exercise), as well as the final legal analysis in which the findings from the mystery shopping exercise were compared again with the identified legal obligations.

3.3.2. Task 2 – Survey on consumer expectations

3.3.2.1. Design

The main objective of Task 2 was to carry out a consumer survey to identify what information about the processing of vehicle-generated data consumers consider most important when purchasing a connected car, from their perspective (see Section 3.2 above for a discussion on the definition of 'material information' and the relevance of consumer preferences/expectations in this regard).

To establish what information consumers feel they need about the processing of vehicle-generated data in order to make a fully informed decision when purchasing a connected car, an online survey was carried out among a representative sample (at country level) of 1 438 consumers across seven EU Member States (Germany, Ireland, Spain, France, Italy, Poland and Sweden). In each of these Member States, at least 200 consumers

were surveyed. The survey targeted frequent drivers (defined as driving a car at least once per month) and those who indicated that they were likely to become frequent drivers in the 12 months following the survey. The resulting sample is representative of the population in terms of age, gender, education and household financial situation.

In order to understand what information is considered most important from the consumers' perspective when purchasing a connected car, the questionnaire measured the importance the consumers participating in the survey attached to different areas of information (e.g. what data are gathered, how they are used and who they are shared with), through two complementary indicators:

- the **relative** importance for consumers of these topics compared with each other;
- the likelihood that information about these topics would affect their decision to purchase a connected car, as self-reported by consumers.

The survey thus aimed to determine what information consumers found important to know – although without prejudice to the requirements set by the applicable legal framework – and which topics they found more important than others.

In addition, the survey measured consumers' awareness of and knowledge about connected cars, their (known) ownership of a connected car and the importance of connected services compared with other aspects of the car. These indicators were included to assess whether there could be an association between consumers' awareness, knowledge and ownership of connected cars and their perceived importance on the one hand, and what consumers find it important to know about data processing in connected cars on the other hand. Assuming that consumers' ownership, awareness and knowledge of connected cars will increase in the coming years, a difference in attitudes among consumers who currently already score higher on these parameters than the average consumer surveyed could be an indication of possible future shifts in what the average consumer will come to consider material information.

3.3.2.2. Output and use

The survey identified the main areas of information that consumers participating in the survey found particularly important and would therefore expect to receive information about when intending to buy a connected car, and to what extent this differs depending on the sociodemographic profile of the consumer. The results of the survey are presented in Section 4.3.

Tasks 1 and 2 together formed the basis of a detailed overview of what can be considered the obligations that car dealers and manufacturers have to abide by with regard to the provision of information about the processing of vehicle-generated data. This overview is provided in Section 4.4 of this report. It served as an assessment framework against which the findings of the mystery shopping exercise regarding each manufacturer were compared. The results of this comparison were subsequently gathered in comprehensive individual manufacturer reports, included in Annex 1 of this report.

3.3.3. Task 3 – Mystery shopping

3.3.3.1. Design

The mystery shopping exercise consisted of two parts.

1. **In-person mystery shopping visits to car dealers and to manufacturers' websites.** These visits were carried out to assess what information about vehicle-generated data is given to a consumer enquiring about buying a connected car. The visits also allowed the investigation of whether car dealers were able to provide this information proactively, clearly and in such a way that consumers could consult it again if they wished (i.e. in written form), and whether they could point consumers to other relevant sources of information (for instance, the manufacturer's website). For these purposes, the focus of the mystery shopping exercise was to evaluate the information received directly from the dealers during the visits. To supplement this, mystery shoppers also assessed how easily (if at all) they could find further information in the materials that they received from the dealer (such as a brochure or a privacy notice), and whether they could find information on the manufacturer's website based on the dealer's instructions. Both aspects were assessed **from the perspective of the average consumer** in order to accurately measure whether they would be able to retrieve the necessary information and would find that information clearly understandable within the time span that a consumer could be reasonably expected to spend on searching for such information. Multiple shopping visits were made per model/manufacturer, with each model/manufacturer covered in three countries.

   For each visit, mystery shoppers were required to fill in an extensive, structured assessment sheet, to allow consistent data collection and analysis across all models and countries. Mystery shoppers were also required to scan and share with the research team any printed materials they received, so they could be audited in detail (see the next step) and would be available to the research team for further analysis.

   A total of 135 mystery shopping visits took place, divided as shown in Table 3.2 over the different manufacturers and countries.

Table 3.2. Mystery shopping visits per manufacturer and country

Manufacturer	Number of visits in							
	All countries	DE	IE	ES	FR	IT	PL	SE
Volkswagen	20	9	3			8		
Renault	20		3	9	8			
Peugeot	19		3		8	8		
Toyota	19		3		8			8
BMW	21	7	2				6	6

Tesla	16	5	1	5		5		
Hyundai	20		3	9			8	
Total	**135**	21	18	24	24	21	14	14

2. **A detailed audit of printed and online materials made available by dealers and/or manufacturers.** Other than the shopping visits, where the goal was to gather information as provided during a typical vehicle purchase from the consumer's perspective, and with the dealer as the primary source, the subsequent audits aimed to comprehensively evaluate the different documents available to consumers. The audits covered information made available by dealers and manufacturers, in print or online. This information was specifically provided through the following types of media:

    - **printed documents** provided by dealers during the physical mystery shopping visits;
    - the manufacturer's **general website** on its connected services;
    - the connected services' **privacy policy** ([26]);
    - the connected services' **terms and conditions**.

    Each of these types of documentation was audited separately. The audits were conducted by one auditor per manufacturer in the countries in which physical mystery shopping visits took place (for instance, in Germany audits took place for Volkswagen, BMW and Tesla). This resulted in a total of 22 audits.

    Audits were performed through an extensive questionnaire, requiring auditors to check whether, how and where certain information was provided.

3.3.3.2. Output and use

The mystery shopping exercise resulted in a detailed overview of indicators that signalled what information about the processing of vehicle-generated data was provided by dealers and manufacturers, how and where it was provided, and how well the mystery shoppers and auditors understood the information provided. This allowed a comparison of the legal obligations of dealers and manufacturers (Task 1) and

([26]) We deliberately use the term 'privacy policy' where we refer to the privacy statement published by the data controller. The statement is often presented as a privacy policy and is published on a website, made available through a link. Although its primary function is to be an informative statement, the privacy policy is often included by referral in a consumer contract, and the provisions thereof are from a contractual point of view often considered to be 'accepted' by the consumer when the consumer agrees to be bound by the consumer contract.

consumers' expectations (Task 2), which in turn resulted in an analytical report on each manufacturer. These reports are included in Chapter 5 of this report (i.e. Annex 1).

It is important to emphasise that, while the results of this mystery shopping exercise were compared with the applicable legal requirements, this did not constitute (nor was it meant to be) a legal compliance check. Indeed, such a compliance check can only be performed by the relevant competent authorities on a case-by-case basis. Rather, the comparative analysis aimed to identify practices of information provision, and to highlight both best practices and areas where the provision of information seemed to be less than satisfactory. This study was limited to developing industry-directed recommendations that could help manufacturers to improve their performance.

4. Study results

This chapter presents the results of the different tasks of the study.

- Section 4.2 presents the results of the legal mapping exercise (Task 1), and specifically the **regulatory framework** that must be considered when determining what rules car manufacturers and dealers need to abide by regarding the provision of information to consumers about the processing of vehicle-generated data.

- Section 4.3 presents the results of the consumer survey (Task 2), in particular **consumers' expectations** when it comes to what information they should receive, and the likely impact of (not) receiving such information on their purchasing decision, overall and as a function of their familiarity with and interest in connected cars.

- Section 4.4 then merges the results of the legal mapping and the consumer survey to provide a point-by-point **overview of what is required from manufacturers and traders**. This forms the basis of the assessment of their practices in the following section.

- Section 4.5 summarises **manufacturers' practices** in the field (Task 3) when it comes to providing information to consumers, compared with the regulatory requirements and consumers' expectations, providing a legal analysis of these practices (Task 4). This section focuses on the most notable trends across manufacturers. A full discussion of the mystery shopping results and the subsequent **analysis for each manufacturer** is included at the end of this report in Annex 1.

- In Section 4.6 a set of **recommendations** are proposed, aimed at car manufacturers, car dealers and the industry in general, to improve their practices when it comes to providing consumers with clear and transparent information about vehicle-generated data processing, in order to better comply with the regulatory framework and meeting consumer expectations.

4.1. Notes on the interpretation of the results

Every research study is conducted within the boundaries of certain practical and methodological scopes (see Section 3.2). The design and practical implementation of the research then naturally also have implications for the scope of the analysis of the resulting data, and the conclusions that can be drawn from those data. In order to ensure that readers of this report can appropriately interpret the results as presented and appreciate the applicability of the conclusions and recommendations, we discuss below a number of considerations that are important to keep in mind while reading this chapter.

4.1.1. Verifiability of the omitted information

The collection of the data in the mystery shopping exercise focused largely on the **presence (or omission) of information**. As this study concerns **only the pre-contractual phase** of commercial communication, the analysis of the data was necessarily restricted to the presence or omission of information at that point. The veracity of that information, however, could not be verified, as that would require the actual testing of the product and the connected services after purchase to compare them with the information provided before the purchase.

That said, any contradictions found in the information provided were sought to be identified, and conclusions drawn on the basis of the data gathered in the context of this study take this into account. This, to some extent, puts limits on legal conclusions that can be drawn from the available data. This is specifically the case, for some types of information, if they are omitted. For instance, it is possible that neither the manufacturer nor the dealer states that the data collected or generated by a connected car are shared with a third party. This could simply be because in fact no such sharing occurs, in which case there is no wrongful omission. However, sharing data without mentioning this to the consumer could constitute a breach of the legal obligations, in particular where personal data are concerned. This is the case for essential parts of the connected services, as in all the connected cars within the scope of this study some data will be collected that will be stored somewhere and used for some purpose. Consequently, the consumer always needs to be informed about what data are collected, where/how they are stored and what they will be used for. While the veracity of any information about these topics cannot be checked in this study, the presence of information as such is already informative for an assessment of legal compliance. Last but not least, it should also be noted that the impact of the omission of certain information or whether it is provided in a clear and transparent manner requires a case-by-case assessment by the competent authorities.

4.1.2. Availability of materials to audit

As explained above, the audit focused on a diverse set of materials. Initially, it was decided that these would be printed materials provided by dealers during the physical mystery shopping visits. However, such printed materials were offered only very rarely. To maximise the chance that the audit would still cover, to the extent possible, at least all the vital sources of information made available by car manufacturers, additional desk research was performed by the research team to identify these sources. The focus of this research was specifically on the **connected services' website, privacy policy, and terms and conditions**. The aim of the research was to find these sources for the connected services of each manufacturer, and separately for each country in which the audit took place for that manufacturer. The search included a search of the manufacturer's general and connected services' websites, a Google search, links from previously found documentation and/or the information provided by dealers (for instance, a reference to the online privacy policy, if provided).

Not all documentation could be found for all manufacturers in all countries within the scope of this study. We emphasise that this does not mean that these sources are in fact not made available by manufacturers, but rather that an extensive search for them was not sufficient for the study team to locate them. However, the fact that our desk research could not identify these sources is arguably an indication that an average consumer would not be able to easily find them either. Given this, for the purpose of this study, we consider that the sources that could not be located are de facto unavailable, regardless of whether they are simply not freely offered online or are very hard to find/access even if they might be available somewhere.

To offer appropriate context for readers of this report, Annex 2 gives the full details of the scope of the assessment for each manufacturer, including all sources that were audited and where sources could not be located.

4.1.3. Variance in findings between audits/countries

The available sources of information about each manufacturer were audited in at least three of the seven EU Member States included in the scope of this study, to increase the validity of the findings and to keep the results from only allowing the drawing of conclusions regarding one Member State, but also to maximise the volume of documentation that could be audited (e.g. if the connected services' privacy policy could be found only in one country).

At the same time, when sources were identified and audited in multiple countries, the default assumption was that they would be largely identical in content; that is, the privacy policy for the connected services of the same manufacturer was not expected to be very different between Member States.

In the analysis of the audit assessments, it became clear that there were often considerable variances between audits of what had been assumed to be identical local versions of the same document (e.g. the privacy policy or the terms and conditions). The scope of the study did not allow the systematic cross-validation of all these variances, so it is not always possible to say with certainty what caused such differences. This means that such variances could be the consequence either of an actual difference in the content of the documents in each of the Member States, or of a difference in the **assessment by the auditor** (for instance, information was available in two Member States, but the auditor in one Member State could not find the information, while the auditor in the second Member State could find it, or they both found the information but interpreted it differently).

Given that in particular the actual **omission** of information could constitute a breach of the legal obligations of manufacturers and dealers, we have chosen to be conservative in our presentation of results that are not consistent across countries and where one auditor claimed that information was not present, while a second auditor – in another Member State – reported that it was. Specifically, readers should keep in mind that the compliance reports in Chapter 5 reflect the findings of data collection efforts by human subjects, and that, if results are mixed, care should be taken when interpreting reports about the absence of information as indicating that this information is indeed not provided by the manufacturer. Rather, mentions of apparent omissions should in the first place be seen as reflecting the inability of our auditors to find this information.

That said, regardless of whether there is an actual absence/omission of information or whether one or more auditors were not able to find the information that is, in fact, available somewhere, both findings reflect a real issue with access to information that should be addressed. In that regard, even contradictory results between different Member States can still reveal important areas for improvement when it comes to the provision of clear and easily accessible information to consumers.

4.2. Mapping of the relevant regulatory framework

In this section we analyse how EU consumer law is relevant to determining what information consumers need during the marketing and pre-contractual phases of commercial communication, that is, before purchasing a connected car, about the processing of vehicle-generated data by a connected car ([27]). Vehicle-generated data can be linked to car owners or drivers, and may include, for example, location data, biometric data and data linked to possible traffic violations, which can be collected through several means, including vehicle sensors, telematics boxes or mobile applications accessed from a device belonging to a driver. Without clear information, the purchaser of a connected car (who is in most instances the future driver) is not necessarily aware of the processing of personal data, let alone about the way it is processed, the purposes of such processing, the possible transmission of the data to other parties and similar processing operations. Whereas the processing of data may in part be necessary for the performance of the agreed contract, many other purposes can be envisaged by the data collector (controller) beyond the mere performance of the contract, including monetising purposes, such as transferring the data to car dealers (for maintenance), insurance companies, data brokers, advertising agencies and public authorities. There is a risk that the data could be used to the detriment of the consumer; for example, the consumer may be confronted with personalised insurance premiums, the loss of their guarantee, undue influence based on profiling or harassment though personalised marketing that limits the consumer's choices in the future.

The analysis does not focus ([28]) on the consumer's rights as a data subject under the GDPR or the ePrivacy Directive, and, in view of the limited scope of this analysis, concepts of the GDPR are not explained in too much detail ([29]). These specific data protection laws protect the privacy and personal data of the **data subject** as a fundamental right. The main instruments of cross-cutting **consumer protection law**, in this domain mainly the UCPD, the UCTD and the CRD, protect the consumer from a different angle, in their **economic interests**, and do not protect their sociopolitical, moral or ethical values. The two sources of regulation have different objectives, although both aim to protect a weaker party, and both are strongly focused on requirements of informed and clear choice, and information. The question is whether consumer law may provide additional value in view of the protection of the 'data subject' as a consumer ([30]). This is particularly important for transactions related to connected

([27]) That is, a vehicle that has devices that allow communication with other devices within and/or outside the vehicle itself, including other vehicles, infrastructure and the wider internet (European Consumer Organisation (BEUC), 2017. *Protecting European Consumers with Connected and Automated Cars*, BEUC, Brussels, p. 2).

([28]) See, for a comprehensive overview in the field of data protection, EDPB, 2020. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed: 20 December 2022).

([29]) In this context, it is important to consider that terms such as 'consent' and 'transparent information' have different meanings under EU consumer law on the one hand and EU data protection law on the other hand.

([30]) See, for example, Helberger, N., Zuiderveen Borgesius, F. and Reyna, A., 2017. 'The perfect match? A closer look at the relationship between EU consumer law and data protection law', *Common Market Law Review*, Vol. 54, No 5, pp. 1427–1465; Svantesson, D., 2018. 'Enter the quagmire – the complicated relationship between data protection law and consumer protection law', *Computer Law and Security Review*, Vol. 34, No 1, pp. 25–36; Kannekens, E. and van Eijk, N., 2016. 'Oneerlijke handelspraktijken:

or smart products, where the goods, the services and personal data processing are integrated into one contract (or a dispersed set of contracts using referrals). The fairness and desirability of such transactions requires an integrated or at least complementary approach from the two blocks of regulation.

4.2.1. Providing sufficient, clear and correct information – Situation of the unfair commercial practices directive

The UCPD forms one of the cornerstones of European consumer protection law. The UCPD provides a full harmonisation framework ([31]), applicable to all commercial practices that take place before, during and after a business-to-consumer transaction ([32]). Article 2(d) UCPD defines business-to-consumer commercial practices as any act, omission, course of conduct or representation, or commercial communication (including advertising and marketing by a trader) directly connected with the promotion, sale or supply of a product to a consumer. Products include both goods and services (Article 2(c) UCPD). The UCPD aims to afford consumers protection against unfair commercial practices that harm or have the potential to harm their economic interests (recital 6 and Article 1 UCPD). It does not protect human dignity, ethical, sociopolitical or safety concerns. It is important to keep this in mind when looking at the interface between consumer protection legislation and privacy and personal data protection legislation, and when studying dealers' and manufacturers' duty to provide information on the processing of personal data by connected vehicles. This is reflected in the requirement that a practice must have an impact on a consumer's economic behaviour, which ultimately has an impact on their transactional decision. The three pillars of the protection are freedom of decision-making, market transparency and consumer information ([33]).

In order to assess the fairness of a commercial practice, the UCPD takes a **three-pronged approach, including three tests** ([34]). These are not cumulative; if the practice passes any one of these tests it may be considered unfair. The first step consists of verifying whether a certain practice falls under a provision of Annex I of the UCPD, which contains a 'blacklist' of misleading and aggressive practices that are always – that is, without having to assess their impact on the average consumer's purchasing decision in a given case – considered unfair and contrary to the UCPD. In the second test, a practice that does not fall under the practices listed in Annex I can be prohibited because

alternatief voor privacyhandhaving', *Mediaforum*, Vol. 4, pp. 102–109; Ratti, M., 2018. 'Personal data and consumer protection: what do they have in common?', in Bakhoum, M. et al. (eds), *Personal data in competition, consumer protection and intellectual property law*, Springer-Verlag, Berlin pp. 377–393.

([31]) Abbamonte, G. B., 2007. 'The unfair commercial practice directive and its general prohibition', in Weatherill, S. and Bernitz, U., *The regulation of unfair commercial practices under EC Directive 2005/29: New rules and new techniques*, Hart Publishing, London, 14.

([32]) See Article 3(1) UCPD; recital 13 UCPD states that the directive is even applicable to unfair practices that occur outside the contractual relationship between the trader and the consumer or after the contract has been concluded.

([33]) Micklitz, H., 2014. 'Unfair commercial practices and misleading advertising', in Reich, N., Micklitz, H., Rott, P. and Tonner, K. (eds), *European Consumer Law*, Intersentia, Cambridge, Antwerp and Portland, 77.

([34]) See, for a schematic of the steps, European Commission, 2016. Commission staff working document – guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices, SWD(2016) 163 final, p. 49.

it is considered misleading or aggressive, and likely to distort the transactional decision of the average consumer (Articles 6–9 UCPD). The last test assesses whether a practice that is not yet described as unfair under Articles 6–9 UCPD can still be considered to contravene the requirements of professional diligence and is likely to distort the transactional decision of the average consumer (Article 5(2) UCPD). In the pre-contractual phase of commercial communication, the UCPD's provisions on misleading practices and omissions are arguably the most relevant.

4.2.2. The general clause of Article 5 of the unfair commercial practices directive – Professional diligence

Article 5(1) UCPD states the general principle that unfair commercial practices are prohibited. Article 5(2) UCPD specifies that a commercial practice is **unfair** if (a) it is contrary to the requirements of **professional diligence** and (b) it materially distorts or is likely to distort **the economic behaviour** (i.e. with regard to the product) of the **average consumer** whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed at a particular group of consumers. In addition to this general principle, Article 5(4) UCPD refers to the specific provisions concerning misleading practices, as set out in Articles 6 and 7 UCPD, and aggressive practices, as set out in Articles 8 and 9 UCPD.

The 'general clause', which refers to a breach of the **professional diligence requirements**, is an essential element of the UCPD and can be seen as a 'safety net' provision. In addition to the two main categories of unfair commercial practices, misleading practices and aggressive practices, th prohibition works as a self-standing test that can catch certain practices that breach the requirements of professional diligence and are likely to distort the economic behaviour of the average consumer, or an average member of a vulnerable group of consumers, but are not covered by the more specific provisions of the UCPD ([35]). **Professional diligence** is defined in Article 2(h) UCPD as 'the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity'. The idea refers to general notions such as 'honest market practice', 'good faith' and 'good market practice', and 'duty of care', values that apply in the specific field of business activity. The test of professional diligence has to be performed on a case-by-case basis, taking into account all the relevant circumstances of the particular case ([36]). Codes of conduct may be used to indicate the expected professional standard, if they have been developed with due consideration of consumers' interests. The material distortion of the economic behaviour of the consumer is captured by the criterion of impairment of the consumer's ability to make an informed decision, resulting in a transactional decision that would not have been made without the practice (see the definition in Article 2(e) UCPD). While it is exclusively for the competent authorities to assess whether a trader complies with data protection legislation and whether there is (still) room for the UCPD to apply as a safety net in a given case, infringements of the data protection legislation may be regarded as, per se, infringements of professional diligence under the UCPD. If these would have an impact on the consumer's

([35]) Unlike other UCPD provisions, Article 5 considers a specific vulnerability.

([36]) Djurovic, M., 2016. 'The duty to trade fairly', in Djurovic, M. (ed.), *European Law on Unfair Commercial and Contract Law*, Hart Publishing, Oxford, pp. 67–109, 75.

transactional decision, the practice can be assessed as an unfair commercial practice. This principle was applied by certain case-law, for example a judgment of the court of appeal of Berlin in 2014 ([37]). The theoretical question is then whether the practice should not be simply regarded as the omission of material information.

4.2.2.1. Providing sufficient, clear and correct information under the unfair commercial practices directive

To put it in a very general but somewhat simplistic way, the UCPD (and, as we will discuss, the CRD) obliges a trader to provide 'truthful', 'sufficient' and 'transparent' information to a consumer before the consumer enters into an agreement with the trader. The UCPD formulates the requirement in a rather negative manner: the trader should not undertake misleading actions or provide misleading information, nor should they mislead the consumer through the omission of certain information. These requirements apply to all commercial communications, such as general advertising, but are stricter when the trader enters the phase of providing an 'invitation to purchase'. The CRD requires the provision of (largely similar) information 'before the consumer is bound by a contract' (the narrower pre-contractual phase).

4.2.2.2. Misleading actions – Article 6 of the unfair commercial practices directive

A commercial practice is regarded as **misleading** if, based on the consideration of all relevant aspects of the specific case, it involves the provision of **false** information and is therefore **untruthful** or, in any way, including overall presentation, it **deceives** or is **likely to deceive** the average consumer about certain elements, and is therefore likely to cause them **to take a transactional decision that they would not have taken otherwise**, even if the information is factually correct (Article 6(1) UCPD). Article 6(1) lists the elements that can be associated with such information. In our field of study, we refer to:

- the main characteristics of the good or service (including its benefits, risks, execution, composition and accessories, and the results to be expected from its use);
- the extent of the trader's commitments, the motives for the commercial practice ([38]) and the nature of the sales process;
- the nature, attributes and rights of the trader or their agent, such as their identity;
- the consumer's rights or the risks they may face.

([37]) Kammergericht Berlin, judgment of 24 January 2014, *Facebook*, 5 U 42/12 (https://www.vzbv.de/sites/default/files/downloads/Facebook_II__Instanz_AU14227-2.pdf, last accessed: 20 December 2022).

([38]) However, an intention to mislead is generally not required for a practice to be considered unfair under the UCPD.

Article 6(1) UCPD refers to misleading **actions** through which the trader creates an erroneous perception on the part of the consumer. It is obvious that **false** or **untruthful** statements are captured by this provision, for example when it is falsely stated that a certain process does not involve the processing of personal data, that certain personal data will only be processed anonymously, or that personal data will not be shared with certain recipients, will not be transferred outside the EEA or will not be used for commercial purposes, such as targeted advertising. However, even if the information provided to the consumer is truthful, it can still be perceived as misleading when the information deceives or is likely to deceive the average consumer about the product or service, for example when the overall presentation confuses and thus deceives the consumer. When 'blurred' information deceives the consumer, this practice may be considered an action and a misleading omission governed by Article 7(2) UCPD, discussed below.

4.2.2.3. Misleading omissions – Duty to provide material information (Article 7 of the unfair commercial practices directive)

a. General

Whereas Article 6(1) UCPD prohibits the trader from undertaking misleading **actions**, Article 7 UCPD states that a commercial practice is 'regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it **omits material information** that the average consumer needs, according to the context, to take an **informed transactional decision** and thereby causes or is likely to cause the average consumer to take a transactional decision that [they] would not have taken otherwise' (emphasis added). Whereas Article 7 is formulated in a negative manner, prohibiting the omission of certain information, it constitutes in fact a **positive obligation** for the trader to provide all information that can be considered material for the rational decision of an average consumer. The assessment of this obligation is less straightforward than an assessment of misleading actions.

Furthermore, the UCPD is not merely concerned about the simple omission of such information; it takes **insufficiently transparent** information into account as well. Providing material information is not simply a formal matter. Article 7(2) UCPD states that a trader hiding or providing in an **unclear, unintelligible, ambiguous or untimely manner** such material information can be equated to a misleading omission. Under certain circumstances, the presentation of ambiguous or otherwise insufficiently transparent information can be regarded as a misleading action under Article 6 UCPD. In other words, traders need to present to the consumer, in an adequate and transparent manner, all the pieces of information that they may need to make an informed choice.

b. Case-by-case assessment under the UCPD

The assessment of a possible infringement of Article 7 is performed on a case-by-case basis, involving four fundamental elements that are closely interrelated.

- The obligation to provide information relates only to the provision of **material information**, that is, information that can be considered relevant for consumers to make an informed choice.

- An omission would be likely to cause a consumer to take a **transactional decision** they would not have otherwise taken, that is, the failure to provide information must have a significant impact.

- The **average consumer** is the benchmark for the assessment of the significant impact.

- **All circumstances**, and all relevant features, together with any **limitation of the communication medium used**, have to be considered, including any measures taken by the trader to make the information available to consumers by other means (see below).

c. Material information

The idea of material information, although not defined in the UCPD, is essential in order to assess whether the average consumer is in a position (or has the opportunity) to make an informed transactional decision ([39]). In fact, Article 7(1) and (2) UCPD establish in general terms a positive obligation on traders to provide all the information that the average consumer needs to make an informed transactional decision. The requirement of materiality of certain information is thus connected to the concept of the consumer making an informed choice. Material information is the information that has a decisive impact on the average consumer's choice if it is provided, and that is likely to have a decisive impact on their choice if it is omitted or obscured. A practice is only misleading when it influences or is likely to influence the consumer to take a transactional decision they would not otherwise have taken ([40]), or, in other words, it could potentially distort the economic behaviour of the consumer. As stated above, sociopolitical or safety concerns as such are not covered by the UCPD. However, such concerns may influence the consumer's decision on whether or not to purchase a product. Therefore, it cannot be a priori excluded that certain concerns about the capturing and processing of personal data, even if those relate to fundamental sociopolitical or moral rights in the domain of privacy, might also have an impact on the average consumer's decision on whether or not to purchase a car with connected features. This is all the more clear when the risks related to the processing of data can have an economic impact (such as an impact on insurance premiums, or exposure to targeted marketing that may limit the consumer's future choices regarding transactions).

d. Material information in the event of an invitation to purchase

([39]) European Commission, 2016. Commission staff working document – guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices, SWD(2016) 163 final, p. 63; Djurovic, M., op. cit., 118.

([40]) Court of Justice of the European Union (CJEU), judgment of 19 December 2013, *Trento Sviluppo*, C-281/12, EU:C:2013:859, para. 33.

Article 7(1) to (3) UCPD apply to any commercial practices, and hence to general advertising campaigns through any media, and individual offerings to consumers. Material information, as 'key information', must be provided throughout the different phases of commercial communication ([41]). However, Article 7 makes a distinction between a general obligation to provide material information (which is more general in its formulation) and the provision of material information in the event of an 'invitation to purchase', as set forth in Article 7(4) UCPD. An **invitation to purchase** is defined as 'a commercial communication which indicates characteristics of the product[/service] and the price in a way appropriate to the means of the commercial communication used and thereby enables the consumer to make a purchase' (Article 2(i) UCPD).

In short, a commercial communication can be considered an invitation to purchase when it indicates (the most important) characteristics of a product or service and indicates the price, thus providing information that enables the consumer to make a purchase. If the price is not sufficiently clear, there is no invitation to purchase; the trader is merely advertising or promoting the product/service. Therefore, the general provisions of Article 7(1) to (3) UCPD apply. In that case, the obligation to provide material information is still applicable, but this application is less clearly defined and can therefore be interpreted more flexibly. The definition of invitation to purchase, referring to the indication of 'characteristics' and 'the price', has been interpreted very broadly by the Court of Justice of the European Union (CJEU). The wording 'enables the consumer to make a purchase' refers to information that is sufficient for the consumer to make an informed decision about a purchase. It is not necessary for the communication to include an actual **opportunity** to purchase (such as an order form or a buy button) ([42]). Furthermore, the invitation to purchase does not have to be an individual invitation. An advertisement to the general public may constitute an invitation to purchase **if a price is indicated**, even if this is not a fixed final price but a limited indication of a reference price, such as an entry-level price or reference price for a product with different versions. Moreover, 'the characteristics of the product' are already present as soon as there is verbal or visual reference to the product ([43]). An invitation to purchase is a narrower concept than advertising, but does not require the consumer's next step to be to enter into a contract with the trader. The 'final stage' before entering into a contract is the 'pre-contractual information' stage, which is governed by Articles 5 and 6 CRD (see Section 4.2.2.7).

The aim of the specific provision of Article 7(4) UCPD is to provide better protection to consumers when they are at the critical point of entering into the purchasing transaction. Although it is generally stated in the literature that the information obligations are stricter at this stage than in more general advertising stages, Article 7(4) UCPD seems only stricter in its indication of what **must** be regarded as material information, and

([41]) European Commission, 2016. Commission staff working document – guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices, SWD(2016) 163 final, p. 63.

([42]) CJEU, judgment of 12 May 2011, *Ving*, C-122/10, EU:C:2011:299, paras 31–32.

([43]) The characteristics must be indicated in a way appropriate to the medium of communication used. The same degree of detail cannot be required in the description of a product irrespective of the form – radio, television, electronic or paper – that the commercial communication takes (CJEU, judgment of 12 May 2011, *Ving*, C-122/10, EU:C:2011:299, para. 44). It is for the national court to ascertain, on a case-by-case basis, taking into account the nature and characteristics of the product and the medium of communication used, whether the consumer has sufficient information to identify and distinguish the product and the reference to the price for the purpose of taking a transactional decision (CJEU, judgment of 12 May 2011, *Ving*, C-122/10, EU:C:2011:299, paras 40 and 49).

thus **must** be provided ([44]). The CJEU states that the list of topics of requested information is **exhaustive** ([45]).

The key topics are:

- the main characteristics of the product, to an extent appropriate to the communication medium and the product;
- the geographical address and the identity of the trader, such as their trading name, or, where applicable, the geographical address and identity of the trader on whose behalf the trader is acting;
- the price, inclusive of taxes, or, where the nature of the product means that the price cannot reasonably be calculated in advance, the manner in which the price is calculated, and, where appropriate, all additional freight, delivery or postal charges, or, where these charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable;
- the arrangements for payment, delivery and performance and the complaint-handling policy followed if traders depart from the requirements of professional diligence;
- for products and transactions involving a right to withdrawal or cancellation, the existence of such a right;
- for products offered on online marketplaces, whether the third party offering the products is a trader or not, on the basis of a declaration of that third party to the provider of the online marketplace.

4.2.2.4. Transactional decision – Economic behaviour (Articles 5–7 UCPD)

The (likely) **impact** of unfair practices is important, as the UCPD protects consumers' economic interests. Article 5(2) UCPD states that a commercial practice is unfair if 'it materially distorts or is likely to materially **distort the economic behaviour** with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers' (emphasis added). According to the definition in Article 2(e) UCPD, '"to materially distort the economic behaviour of consumers" means using a commercial practice to appreciably impair the consumer's ability to make an informed decision, thereby **causing the consumer to take a transactional decision that he would not have taken otherwise**' (emphasis added).

Similarly, Article 6(1) UCPD states that a misleading action, information or presentation causes, or is likely to cause, the average consumer **to take a transactional decision that they would not have taken otherwise**, and according to Article 7(1) UCPD a

([44]) However, if the information is already apparent from the context (such as the trader's address), it need not be provided.

([45]) CJEU, judgment of 26 October 2016, *Canal Digital*, C-611/14, EU:C:2016:800, para. 68.

commercial practice can be regarded as misleading if it omits information that the average consumer needs in order to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that they would not have taken otherwise. Article 7(2) UCPD, concerning hidden, unclear, unintelligible, ambiguous or untimely information and the hiding of the commercial intent of a certain practice, also refers to a transactional decision that would not have been taken without the practice. The ideas of 'material distortion of the economic behaviour', 'impairment of the consumer's ability to make an informed decision' and the consequential 'taking of a transactional decision that would not be taken otherwise' refer, in fact, to the same concept ([46]). The action, information, omission, ambiguity, etc., must have a level of relevancy and effect that is sufficient to influence the decision-making process of the average consumer.

What is important is that a consumer takes decisions that are related to a certain transaction, for example a purchase, that they may pursue or terminate at some point. Such decisions are the only relevant 'behaviour' in this context. The UCPD is based on the assumption that a consumer is a rational person who will take an informed and efficient decision (a choice) on the market. Through the protection of their informed choice, the provisions on misleading actions and misleading omissions safeguard their economic interests. The UCPD tries to strike a balance between the interests on the market, and this requires that only significant distortions, which impair the average consumer from taking an informed decision, are prohibited. The criterion that is applied in the UCPD is therefore the fact that the action or omission of information is likely to cause the average consumer to take a transactional decision that they would not have taken otherwise. Therefore, not every omitted or even false piece of information is 'material' in terms of relevance.

The prohibitions in Article 6(1) and Article 7 UCPD apply in **all the phases of commercial communication** between the trader and the consumer before, during and even after the conclusion of a contract. They are not limited to the strict pre-contractual phase of negotiations, but apply even during general advertising campaigns providing commercial information to the general public ([47]), for example through websites, brochures and general advertisements across all media. Before purchasing a product, a consumer may undertake a journey on which they are influenced by different kinds of communications. Their appetite may be triggered by a general advertisement on TV, on a website banner, or in an online or paper magazine. Based on this trigger, they may search for further information about the product. They may search for information on websites, contact a manufacturer, or visit a store or, as in our study, a car dealer. During this journey, the consumer builds, or as the case may be, loses an intention to purchase, based on the information that they can find and process, or based on the information provided directly by the trader. The '**transactional decision**' that can be influenced by the presence of certain correct or false information, or by the absence of certain information that they need to take their decision, is not limited to the actual decision on whether or not to purchase the product or service but is broader. According to the definition in Article 2(k) UCPD, a '"transactional decision" means any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting'.

([46]) Micklitz, H., op. cit., p. 92.

([47]) As long as it is 'directly connected with the promotion, sale or supply of a product[/service] to consumers' (Article 2(d) UCPD).

The CJEU stated that any decision related to the decision on whether or not to purchase a product, and in particular the acts that are preparatory to a purchase, such as a visit to a shop, may be regarded as constituting transactional decisions in the context of the UCPD ([48]). This point of view seems backed up by a general belief that a certain mindset created by early steps of a consumer during the purchasing journey may have an impact on the outcome of the journey.

In our context, it could be a decision to purchase or to refuse to purchase a vehicle that necessarily includes connected features. The rational consumer will consider the benefits of the connected car against various risks that they expect to be informed about. Similarly, the consumer will decide whether or not to purchase optional or additional connected services, or to make use of their right to object to their data being processed or to withdraw their consent to their data being processed at any time, a right that they are entitled to under Article 7(3) GDPR. As the impact on the consumer's transactional decision is a key assessment criterion under Articles 5, 6 and 7 UCPD, the idea must be clearly understood. We believe that the issues related to data protection are, in the case of purchasing a connected car, where applicable, part of the consumer's decision to purchase the car (at least insofar as these can be considered material information for that decision). Data processing is part of the functionality of connected products in the sense of Article 5(1)(g) CRD. It is one of the main characteristics of such products in the sense of Article 6(1)(a) UCPD. The Berlin Court of Appeals decided that a consumer's decision to agree to data processing as a precondition for being able to use a service (in this case Facebook) could be considered a transactional decision in the sense of the UCPD. This is particularly the case when a consumer 'agrees' to their data being captured for marketing purposes or the personalisation of services ([49]).

4.2.2.5. The average consumer

The UCPD refers to 'the average consumer' as the benchmark person who (a) is likely to be deceived by the practice and (b) may take a transactional decision that they would not have taken without the deceptive element. The average consumer is the standard of a hypothetical consumer who is reasonably well informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors (in terms of the established case-law of the CJEU ([50])), and who behaves like a rational economic operator based on the information in their possession. Their attention will vary according to the category of goods and services in question. Products perceived as more complex, new, less transparent, comprising certain risks, etc., will require a reasonable consumer to be more attentive. In line with Articles 6(1) and 7 UCPD, national enforcers will have to assess whether false representation, for example the omission of (material) information, is likely to cause the average consumer to take a transactional decision that they would not have taken without the false representation or without the omission. Thus, they must assess (a) whether the average consumer could be deceived (excluding marketing exaggerations, which should not deceive the average, reasonable consumer)

([48]) CJEU, judgment of 19 December 2013, *Trento Sviluppo*, C-281/12, EU:C:2013:859, paras 36–38.
([49]) Kammergericht Berlin, judgment of 24 January 2014, *Facebook*, 5 U 42/12 (www.vzbv.de/sites/default/files/downloads/Facebook_II__Instanz_AU14227-2.pdf, last accessed: 20 December 2022).
([50]) As referred to in recital 18 UCPD. See, for example, CJEU, judgment of 26 October 2016, *Canal Digital*, C-611/14, EU:C:2016:800, para. 39.

and (b) whether the created perception had a significant effect on the average consumer's choice.

4.2.2.6. Case-by-case assessment under the UCPD

Determining whether or not the average consumer may be deceived by a commercial practice requires a case-by-case assessment by the competent enforcement authorities. It requires an assessment *in concreto* of all relevant circumstances of the case, including the overall presentation of the product. Article 6(1) UCPD does not state that the limitations of the medium can be considered in order to justify the practice. False information cannot be justified by the limitations of a medium in time or space, whereas this may be the case for the omission of certain information (Article 7(3) UCPD). Following an assessment of the factual circumstances *in concreto*, the competent enforcement authority must assess whether an average consumer could be deceived and whether their choice is likely to be impaired. This assessment is an assessment *in abstracto*, applying the hypothetical idea of the average consumer as a benchmark. The enforcers will not assess the capabilities of a specific consumer who claims to have been deceived. In performing this 'average consumer test' or 'significance test', the national enforcers will have to exercise their own faculty of judgement, having regard to the case-law of the CJEU, to determine the typical reaction of the average consumer in a given case, according to recital 18 UCPD. This recital states that the 'average consumer test' is not a statistical test. However, it is often acknowledged that, for this assessment, the enforcers can require an expert opinion or a consumer survey, indicating the concrete risk for a sufficiently significant number of consumers ([51]), and that behavioural studies can be helpful in understanding the importance of certain pieces of information ([52]).

The UCPD's provisions concerning misleading (and aggressive) practices do not refer particularly to vulnerable consumers ([53]).

Article 7(4) UCPD provides a list of key items of information that are considered material, and that are therefore needed for the consumer to take an informed decision. However, especially where it refers to the main characteristics of the product, it is still necessary to assess whether a certain characteristic must de facto be considered material. It is not realistic to consider **all** characteristics required (material) information. Thus, the assessment of a possible breach of information obligations does not seem

([51]) Micklitz, H., op. cit., p. 100; this measure was suggested by the CJEU in the 'lifting' case (CJEU, judgment of 13 January 2000, *Estee Lauder*, C-220/98, EU:C:2000:8, para. 31).

([52]) Djurovic, M., 2016. 'The duty of information', in *European Law on Unfair Commercial Practices and Contract Law*, Hart Publishing, Oxford, p. 119.

([53]) The legislation is somewhat ambivalent in this respect, as Article 5(3) UCPD, relating to general unfair practices that are not misleading practices, does refer to groups of consumers who are particularly vulnerable to certain practices (where the benchmark is an average member of that group). Recital 34 CRD ambiguously refers to the needs of vulnerable groups with regard to pre-contractual information, but states that fulfilling these should not lead to different levels of consumer protection. In general, the protection of vulnerable consumers, typically children and older people, is only considered when certain products are particularly appealing to such groups. In our context of connected cars, we believe that we should not focus on specific vulnerable groups.

different from under the other paragraphs of Article 7 UCPD, although they are often considered stricter obligations.

The CJEU stated that the national court, by taking into account, in accordance with Article 7(1) to (4)(c) UCPD, the **factual context** of the commercial practice at issue, the **medium** used to communicate information (in particular the **limitations of that medium**) and the nature and **characteristics of the product** in question, must therefore assess on a case-by-case basis whether the omission of material information caused or could cause the consumer **to take a transactional decision that they would not have taken otherwise** ([54]). Evidently, the benchmark is again the **average consumer**, as explained before, and the competent enforcement authority should assess the likely impact of any omission on the average consumer's decision. The competent enforcement authority should investigate the facts and circumstances of the individual case (i.e. *in concreto*) and assess the **likelihood** of the practice affecting the transactional decision of the average consumer (i.e. *in abstracto*). As stated above, the national enforcers have the power to decide for themselves, although behavioural studies, expert opinions and consumer surveys may be helpful in order to understand what information consumers need to make an informed choice. Similarly, an assessment of whether information is **sufficiently clear and comprehensible** is done with reference to the average consumer ([55]).

Regarding the **limitations of the medium of communication**, the CJEU emphasised clearly that, where the medium is limited in time and space (e.g. a TV commercial, a banner or a classical advertisement in a magazine), these limitations must be considered. The measures that are taken by the trader to make the information available to consumers by other means must also be considered ([56]). Therefore, where, with regard to the intrinsic characteristics of the product at issue and the limitations relating to the communication medium used, it was impossible to provide all the material information for that product, the commercial practice may mention only some of the characteristics, if the trader refers the consumer to its website to obtain the rest of the information. However, that website must contain the material information relating to the main characteristics of that product, the price of the product and other conditions, as required under Article 7 UCPD.

4.2.2.7. Articles 5 and 6 of the Consumer Rights Directive

The obligation to provide material information at the stage of an invitation to purchase, negatively formulated in Article 7(4) UCPD, is also reflected in Articles 5 and 6 CRD, which is another cornerstone of consumer protection under EU law.

The CRD focuses on the trader's **pre-contractual information requirements**. Where Article 7 UCPD requires the provision of material information during the earlier phases of the consumer journey up to the invitation to purchase, Articles 5 and 6 CRD apply to the narrower pre-contractual phase, from the point where the consumer starts the purchasing process until the consumer is bound by the contract or any corresponding

([54]) CJEU, judgment of 26 October 2016, *Canal Digital*, C-611/14, EU:C:2016:800, para. 58.
([55]) CJEU, judgment of 18 October 2012, *Purely Creative*, C-428/11, EU:C:2012:651, para. 55 (in fact, the court referred to the (average) member of the targeted group).
([56]) CJEU, judgment of 26 October 2016, *Canal Digital*, C-611/14, EU:C:2016:800, para. 61.

offer. Article 5 CRD states that, **before the consumer is bound** by a contract or any corresponding offer, the trader must provide the consumer with certain information, listed in the article, in a clear and comprehensible manner, if that information is not already apparent from the context. In our field of study, we consider the following elements of information relevant:

- the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;
- the identity of the trader, such as their trading name, the geographical address at which they are established and their telephone number;
- the total price of the goods or services;
- the duration of the contract, where applicable, or, if the contract is of indeterminate duration, or is to be extended automatically, the conditions for terminating the contract;
- where applicable, the functionality, including applicable technical protection measures for goods with digital elements, digital content and digital services;
- where applicable, any relevant interoperability of goods with digital elements, digital content and digital services that the trader is aware of or can reasonably be expected to have been aware of.

Articles 6 and 8 CRD contain additional information requirements for **distance contracts** and **off-premises** contracts. We believe that we should not focus on these specific types of contracts in relation to the purchase of connected cars and for the purpose of this study ([57]) ([58]).

The CRD refers to the pre-contractual phase as the phase before the consumer is bound by the contract or any corresponding offer. This idea is generally interpreted as narrower and closer to the actual conclusion of a contract than the stage of the invitation to purchase, mentioned in Article 7(4) UCPD ([59]). Article 5 CRD covers all the information requirements under Article 7(4) UCPD, which requires an **invitation to purchase** to contain the information needed by the average consumer to make a fully informed transactional decision. Therefore, when providing pre-contractual information in accordance with the CRD, a trader will, in most cases, also comply with the information requirements under the UCPD ([60]). This is without prejudice to the information requirements under the UCPD regarding the invitation to purchase prior to the pre-

([57]) It is unlikely that the purchase of a connected car would be regarded as an off-premises contract. Cars are certainly purchased at car fairs or 'salons', but even in that case the contract is not regarded as an off-premise contract (European Commission, Directorate-General for Justice and Consumers, 2014. Guidance document concerning Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (https://ec.europa.eu/info/sites/default/files/crd_guidance_en_0.pdf) (CRD guidance), Section 3.2, p. 14).

([58]) Cars are usually purchased after visiting, and discussing them with, a car dealer, and the purchase documents are typically signed on the dealer's premises. However, it may occur that certain connected services are agreed with another, absent, party, through communication media (possibly even the device itself). Investigating this topic would, however, distract from the main purpose of the study.

([59]) UCPD guidance, Section 2.9.5.

([60]) UCPD guidance, Section 1.2.3.

contractual stage, for example at the marketing and advertising stage. It is acknowledged that distinguishing between the stage of the invitation to purchase (in which case the UCPD applies) and the pre-contractual stage (in which case the CRD applies) is not easy ([61]). The distinction is, however, relevant, as consumer associations, enforcement authorities and entities qualified to implement group actions ([62]) have a right to take action in both cases, but only in the event of a violation of the CRD does the consumer have an individual right to be provided with the information or to seek damages if the information is not provided ([63]).

Articles 5 and 6 CRD are more comprehensive than the general provisions of the UCPD and are positively formulated, whereas Article 7 UCPD is formulated as a prohibition.

4.2.3. Recapitulation – Information obligations and data protection: Connected cars

a. General

We have seen that **false** statements or representations should always be deemed misleading if these have or are likely to have a significant impact on the consumer's transactional decision (which we have given a broad interpretation). Regarding information that is **missing**, the CRD can be used to assess the required pre-contractual information, whereas Article 7 UCPD can be used to assess missing material information in earlier marketing phases. Furthermore, the UCPD enables in general a more factual and flexible assessment of misleading omissions of material information. The different legal provisions emphasise that the **clarity** of the information provided must be considered.

Returning to the interface between the consumer and the data protection *acquis*, we stated that the two legal frameworks are different with regard to their purpose / subject matter. Both sources of legislation emphasise the **free and informed manifestation of will** as an important basis for the protection of a weaker party, and both contain **information obligations**. The scope and objective of the data protection legislation is to protect consumers' fundamental rights, whereas the scope and objective of the consumer protection legislation is to protect the consumers' economic interests. However, this does not exclude the opportunity for both legal frameworks to complement each other in certain cases. In particular, the evolutions in the field of social media, connected products and the internet of things indicate that a complementary approach must be followed in order to provide integrated protection against the legal concerns, especially where consumer transactions and personal data processing are equally integrated ([64]). Furthermore, it is a fact that the processing of personal data,

([61]) Tonner, K., 2014. 'The consumer rights directive and its impact on internet and other distance consumer contracts', in Reich, N., Micklitz, H., Rott, P. and Tonner, K. (eds), *European Consumer Law*, Intersentia, Cambridge, Antwerp and Portland, p. 403.

([62]) See the representative actions directive (Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 409, 4.12.2020, pp. 1–27).

([63]) Tonner, K., op. cit., p. 403.

([64]) See, in particular, Helberger Zuiderveen Borgesius, F. and Reyna, A., op. cit., footnote 36, and Svantesson, D., op. cit., footnote 36.

for example for advertising purposes, can have significant economic value ([65]). The violation of information requirements under the GDPR and e-Privacy Directive could, depending on the circumstances of a particular case and under the condition that the requirements for the application of the relevant legal instrument are met, also be considered a misleading omission of material information under the UCPD ([66]). The two regulatory 'blocks' enable different authorities, organisations and individuals to act against infringements and provide different remedies and forms of redress. The UCTD, which we will assess below, is equally important in this respect and possibly even more widely used in practice. Recital 42 of the GDPR refers explicitly to the requirements of the UCTD when a preformulated declaration of consent is submitted to the data subject. The increasing interface between consumer protection and data protection was also highlighted in the recent Digital Content Directive (Directive (EU) 2019/770), which states that non-compliance with the GDPR may constitute lack of conformity of the digital services under the directive, and the remedies of the directive should be available to the consumer in this case (recital 48).

In its judgment of 28 April 2022 in the case *Meta Platforms Ireland* v *Bundesverband der Verbraucherzentralen und Verbraucherverbände* ([67]), the CJEU stated that the infringement of the rules intended to protect consumers or to combat unfair commercial practices – infringement that a consumer protection association aims to prevent and penalise, inter alia, by recourse to actions for an injunction provided for in the applicable national legislation – may be related to the infringement of the rules on the protection of personal data of those consumers (para. 66) and that the infringement of a rule relating to the protection of personal data may at the same time give rise to the infringement of rules on consumer protection or unfair commercial practices (para. 78). The court decided that Article 80(2) GDPR does not preclude a consumer protection association from bringing legal proceedings against a person allegedly responsible for an infringement of the data protection laws, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

The GDPR states which information must be provided to the **data subject**, focusing on safeguarding the fundamental right to personal data protection (Articles 13 and 14), and provides detailed rules on the required clarity of information (Article 12). Article 5(3) of the ePrivacy Directive, which applies when data are stored or accessed on terminal equipment (an idea that includes connected vehicles and every device connected to them, such as smartphones), states that the storage of and access to activity logs through electronic communications networks is only allowed on condition that the subscriber or user (a) is provided with clear and comprehensive information in accordance with the GDPR, inter alia about the purposes of the processing, and (b) is asked for consent to such processing by the data controller, unless it is strictly necessary in order to provide an information society service explicitly requested by the subscriber

([65]) See, for example, UCPD guidance, Sections 1.4.10, 3.4.1 and 4.4 (p. 89); see also, in general, some of the principles underlying the recent digital content directive (Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

([66]) Furthermore, the information requirements of the GDPR and the e-privacy directive may be considered material information under Article 7(5) UCPD; see UCPD guidance, Section 1.2.10.

([67]) CJEU, judgment of 28 April 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322.

or user (e.g. when they request infotainment or other online services under the e-commerce directive ([68])), or for the sole purpose of carrying out the transmission of a communication over an electronic communications network. In the latter case, the processing is based not on consent but on the need to perform a contract (see also Article 6(1)(b) GDPR). In its guidelines concerning connected vehicles, the European Data Protection Board identifies, in relation to the information required under the GDPR, information that should be given as essential first-level information: the identity of the data controller, the purposes of data processing, the data subject's rights, and the names of all the recipients and, if that is not possible, at least a detailed description of the types of recipients. Other information could be provided at a later stage, as a second layer ([69]). This is not necessarily the material information required for a **transactional decision** in the sense of consumer law, but at least gives an indication of the kind of information required.

b. Main characteristics

Article 7(4) UCPD mentions information concerning the **main characteristics** of a product as material information, whereas Articles 5 and 6 CRD list information concerning the main characteristics of a product as mandatory pre-contractual information. Furthermore, Article 6(1)(b) UCPD mentions the main characteristics of the product as an element that must be presented in a way that does not deceive the consumer. The CRD guidance states that the idea is similar to that in Article 7(4) UCPD ([70]), and that a more complex product requires more product information ([71]). In the view of the study team, this also refers to the complexity of all kinds of data processing that may occur with or without the consumer's awareness. This links the issue of complexity with the transparency of the many things going on in a technical environment, which is entirely impenetrable for the average consumer. Article 6(1)(b) UCPD gives an indication of the main characteristics of a product or service, such as its availability, benefits, risks, execution, fitness for purpose and geographical origin. We may assume that this indication is not different under Article 7(4) UCPD, provided that the (potential) impact on the average consumer's transactional decision must always be assessed. It is clear that information on the risks of data processing must be considered as part of the main characteristics. The risks may include the risk that data may be used for profiling, having an impact on automated decisions with regard to the consumer (e.g. personalised insurance premiums, loss of a guarantee if certain behaviour is noticed through data processing, or personalised marketing or influence). The risks in relation to the hacking of data or even the hacking of the entire functioning of a car (which has occurred in practice) are obvious. The UCPD guidance specifies that safety

([68]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, OJ L 178, 17.7.2000, pp. 1–16.

([69]) EDPB, 2020. *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed: 20 December 2022), No 84, p. 18. See, for a detailed analysis of this layered approach, Article 29 Data Protection Working Party, 2018. *Guidelines on Transparency under Regulation 2016/679*, WP260 rev. 01, Nos 35 and following (https://ec.europa.eu/newsroom/article29/items/622227, last accessed: 20 December 2022).

([70]) CRD guidance, p. 22.

([71]) CRD guidance, p. 69.

warnings in relation to products may constitute one of the main characteristics of a product within the meaning of Article 7(4) UCPD. The study team believes that this also applies to the secure processing of data: the consumer must receive clear information on the security of the system, such as the measures taken to protect them against hackers. Article 5(1)(g) CRD requires the provision of information about the functionality of digital content, including applicable technical protection measures.

c. The purposes of data processing and commercial intent

The UCPD guidance contains a section on the possible interface between the data protection legislation and the UCPD ([72]). It states that a trader's violation of the data protection legislation will not, in itself, always mean that their practice is also in breach of the UCPD. Conversely, compliance with the UCPD does not always translate into compliance with the data protection legislation. However, certain violations that occur could be considered part of the overall unfairness of commercial practices under the UCPD in a situation where the trader processes consumer data in violation of data protection requirements, that is, for direct marketing purposes or any other commercial purposes, such as profiling, personal pricing or big data applications. The guidance refers to overall unfairness, which we believe could be based on misleading practices, aggressive practices and the 'catch-all' unfairness provision of Article 5 UCPD (see above). The guidance then refers to misleading practices, stating that the first issue to be considered is the **transparency** of the commercial practice. Under Articles 6 and 7 UCPD, traders should not mislead consumers on aspects that are likely to have an impact on their transactional decisions. Article 7(2) UCPD, concerning hidden or obscured information, and point 22 in the blacklist in Annex I UCPD (falsely creating an impression that the trader is not acting for commercial purposes) prevent traders from **hiding the commercial intent** behind their commercial practice. The guidance states that **the data protection-related requirement** for traders to inform consumers about the processing of their personal data, not limited to commercial communication, may be considered material. Consequently, under Article 7(2) and point 22 in the blacklist in Annex I UCPD, if the trader does not inform a consumer that the data they are required to provide to the trader in order to access the service will **be used for commercial purposes** (e.g. by sharing it with third parties for commercial purposes, such as advertising), this could be considered a misleading omission of material information. Undisclosed or obscurely disclosed monetising of consumers' personal data is clearly covered by the UCPD, depending on an assessment of whether the average consumer would have taken a different transactional decision if they were aware of the use of their personal data for this purpose. We believe that the transactional decision could be regarded as the purchase of the car as a whole, or the purchase of specific optional connected services, which they could have refused or for which they could have negotiated different conditions, if possible. As always, the concrete factual circumstances must be examined, where applicable, on a case-by-case basis, under the UCPD.

Article 5(1)(g) CRD requires information about the **functionality**, including applicable technical protective measures, of **digital content** (which is data produced and supplied in digital form). Recital 19 CRD states explicitly that the term 'functionality' implies that the trader must provide information about the ways in which digital content can be used,

([72]) UCPD guidance, Section 1.2.10.

for instance **for the tracking of consumer behaviour**. The CRD guidance ([73]) provides a non-exhaustive list of the information that may be part of functionality and operability. The list also explicitly mentions any conditions for using the product not directly linked to operability, **such as tracking and/or personalisation**. Furthermore, it is stated explicitly that data processing for tracking or personalisation purposes must be disclosed. Regarding the use of data for profiling and **personalised pricing**, the UCPD guidance states that information on this must be given to consumers ([74]); this information includes material information about the way the price is calculated, as required in Articles 6(1)(d) and 7(4)(c) UCPD, and Article 5(1)(c) CRD. A lack of clear information in this respect could be considered a misleading omission if it could have an impact on the consumer's purchasing decision ([75]).

The link between data protection and consumer protection was often made in the context of **social media services**. The European Consumer Organisation (BEUC) believes that information about the main characteristics of a service should include, for example, a complete explanation of the business model of an app and information on what personal data are collected, processed and transferred to third parties if this is an essential feature of the services provided (as is the case for TikTok) ([76]). A lack of clear and complete information about data processing practices may not allow consumers to take an informed decision on whether to register for a service or app or to understand the functioning of the service and its potential risks. This may result in a breach of Article 6(1)(a) CRD and a misleading omission under Article 7 UCPD regarding the main characteristics of the service in respect of its data collection processes (as well as breaches of Articles 5 and 7(2) UCTD (see Section 4.2.5 for more information)) concerning lack of transparency, due to the contractual nature of the **privacy policies** that are included in a contract by reference ([77]). In 2018, the Italian Competition Authority imposed a fine of EUR 10 million on Facebook based on a misleading omission under the UCPD, because it did not adequately inform consumers during the creation of their accounts that the data they provided would be used for commercial purposes. According to the authority, consumers were persuaded to make a transactional decision that they would not have made otherwise (and in this case the transaction was even 'free' of monetary payment). In particular, the information was too vague and did not make a clear distinction between the purpose of personalising the service and the use of data for personalised advertising campaigns. Furthermore, Facebook **pre-selected** in checkboxes the broadest consent to data sharing, and when users limited their consent they were confronted with severe limitations of use, thus prompting them to maintain the pre-selected choice. This was considered **undue influence**, and thus an **aggressive practice** under Articles 8 and 9 UCPD ([78]). After a joint action by the Consumer Protection Cooperation Network, Facebook committed in 2019 to clarifying its business model, especially how it uses data from users' profiles for commercial

([73]) CRD guidance, p. 67.
([74]) UCPD guidance, Sections 1.2.10 and 4.2.8.
([75]) Helberger, N., Zuiderveen Borgesius, F. and Reyna, A., op. cit., p. 1439.
([76]) BEUC, 2021. *TikTok without Filters* (https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf, last accessed: 20 December 2022), p. 22.
([77]) BEUC, 2021. *TikTok without Filters* (https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf, last accessed: 20 December 2022), pp. 22 and 27, which provide many concrete examples.
([78]) Italian Competition Authority, 2018. 'Facebook fined 10 million euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes' (https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes, last accessed: 20 December 2022).

practices, particularly through targeted advertising services ([79]). In our analysis, we did not overly focus on the prohibition of aggressive commercial practices, prohibited by Articles 8 and 9 UCPD. That was mainly because there are few examples in the field of data protection, we did not reach a clear consensus on this application as undue influence and it would be difficult to test such practices during a mystery shopping exercise. Moreover, unfair practices in relation to data processing have been challenged, focusing on the related **contract terms** under the UCTD, particularly in the field of social media and connected products. We will discuss this further below.

It is therefore clear that information about the **purposes** of data processing, which is also required under Article 13(1)(c) and Article 14(1)(c) GDPR, could, as far as the UCPD is applicable, be considered material information, depending on the circumstances. As more and more sensors in cars, combined with artificial intelligence, are able to provide more and more information for more and more specific purposes, the concerns for consumers are clear. In this respect, information on **the categories of data** that can be collected, processed for specific purposes or shared with third parties is equally important (e.g. technical data, which may reveal certain driving styles, a lack of maintenance, etc.; and geolocation data, which may reveal particular consumer behaviours, biometrics, preferences, etc.). Depending on the circumstances of the case, certain information about recipients **with whom the data will be shared** ([80]) can, where applicable, also be considered material under the UCPD, that is, where such sharing is likely to raise consumers' concerns and may therefore be considered to potentially have an impact on the transactional decision of the average consumer. The categories of recipients and the purpose of data sharing could be of particular importance to consumers in that respect.

d. Specific information topics

Information on the **identity of the trader** is mentioned in Articles 5 and 6 CRD and in Article 7(4)(b) UCPD as material information. For distance contracts, the trader's contact details are also required, as well as information concerning the trader on whose behalf the trader is acting. Under the GDPR, a data controller must provide to the data subject certain mandatory information about the identity (and the contact details) of **the controller** and of their representative, if any. This can be important if the data subject wants to make use of their rights granted under the GDPR. Remarkably, Article 7(4) UCPD does not refer to information on **the consumer's rights** (although the list in this article is deemed exhaustive). However, information on complaint handling can be understood as one of the main characteristics of the product (Article 6(1)(b) UCPD), and, where the processing of personal data is an essential feature of a service, the study team believes that the consumer's rights regarding the correction of data could, where applicable, also be regarded as material under the UCPD. Whether this information may have an impact on transactional decisions is, however, uncertain. Similar remarks can be made about information on the consumer's **legal right to object** to data processing and **to withdraw** their consent to data processing

([79]) European Commission, 2019. *Consumer protection cooperation action on Facebook's terms of service*, factsheet (https://commission.europa.eu/system/files/2019-04/factsheets_on_the_changes_implemented_by_facebook.pdf, last accessed: 20 December 2022). The concerns were mainly based on the UCTD (unclear information, causing significant imbalance).

([80]) This statement under consumer law is without prejudice to the information requirements of the GDPR in the case of data sharing (see Article 13 GDPR).

at any time, as stated in the GDPR ([81]). Article 5(1)(f) CRD refers to information on the **duration** of the contract, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for **terminating** the contract. This information may have an impact on the duration of the data processing and could be material under certain circumstances.

In line with the GDPR, consumers must be informed of whether their data will be processed, including whether it will be shared with companies established in countries that do not offer the same level of protection as in the EEA, and they must be informed about the protection mechanisms that are applied in such cases. In the car industry, it is possible that data are processed in or transferred to organisations (data controllers or processors under the GDPR) based outside the territory of the EEA, and this could be a concern for consumers ([82]).

The information about the functionality of a product, required under the CRD (see 'The purposes of data processing and commercial intent', above), should also include information **on the control** that the consumer may exercise on the extent of data processing, for example through the settings of the devices and the possibility of **deleting** the data. If that is considered material information, it should also be available in easily understandable language in accordance with the guidelines on clarity, set forth in the UCPD, the CRD and the UCTD (see Section 4.2.5).

Article 5(1)(h) CRD requires information about the **interoperability** of digital content with certain hardware and software. It is important for a consumer to know whether certain devices that are supposed to link to the car's system are compatible with that system or not (e.g. the need to use an iOS or Android device). Although a direct link with data protection issues is not obvious, the lock-in to a specific system may have consequences for **data portability**, for example when the owner of a car wants to switch to a different model. This is the subject matter of Article 20 GDPR ([83]).

Information about the functionality of a product or service (Article 5(1)(g) CRD) can include information on a minimum presented (or even warranted) **lifespan** and the availability of software updates ([84]). As the 'premature' **obsolescence** of products has become an important topic for consumer watchdogs, due to strategies of certain manufacturers that have been revealed or presumed over the past years, consumers are becoming more sensitive to minimum lifespan information and/or warranties. The sales of goods directive ([85]) requires the trader to supply updates, including security updates, in the case of goods with digital elements to ensure the continuous supply of the digital content or digital service for 2 years after the delivery of the goods, keeping those goods in conformity. If the contract provides for a continuous supply for more

([81]) Article 13(2) GDPR. Information on the 'right to withdraw' is identified as necessary information in Article 5 and 6 CRD, but this seems to refer to the right to withdraw from a distance contract, according to Article 9 CRD.

([82]) Without prejudice to the information requirements and the application of other measures required under the GDPR in the case of data transfer outside the EEA.

([83]) See also, in relation to data portability, Article 16(4) of the digital content directive and Articles 23 and following of European Commission, 2022. Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (data act), COM(2022) 68 final.

([84]) This may also be considered information on the duration of the contract required by Article 5(1)(f) CRD.

([85]) Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136, 22.5.2019, pp. 28–50.

than 2 years, the trader may be liable for lack of conformity that occurs within the indicated or warranted period (Article 7(3) and Article 10(2) and (5) of the Sales of Goods Directive). Furthermore, several European consumer organisations have undertaken legal actions, including class actions, based on the omission of material information in relation to the policies of updates and obsolescence, as an unfair and aggressive practice under Articles 7 and 8 UCPD ([86]). The premature obsolescence of connected systems may trigger the issues of **lock-in and data portability**, if a consumer is confronted with the need to purchase a replacement product.

e. Assessment of circumstances

It is important to bear in mind that considering the **factual context** and the **limitations of the mediums of communication** that are used is essential when conducting an assessment of the practice (see Article 7(3) UCPD). It is not always necessary to provide all the material information, including the main characteristics of a product or service, in one place. Reference can be made to websites or other sources where more information can be found (including, for example, a visit to a car dealer), as long as the general information is sufficiently clear. This is obviously true of communications in the phases of advertising (Article 7(1) to (3) UCPD), where the UCPD is rather vague and flexible, and the idea of influencing the consumer's transactional decision means intentions that are less clear than those involved in the actual decision to purchase that is influenced at the stage of the invitation to purchase, mentioned in Article 7(4) UCPD, and the pre-contractual phase mentioned in Articles 5 and 6 CRD. But even in the later stages of commercial communication, traders are allowed to refer to additional information that can be obtained, as long as the overall information provided is clear ([87]). However, limited time or space is no excuse for **false** information.

In addition, the use of certain **default settings** in devices may be regarded as a misleading practice, depending on the circumstances, if the presentation is such that the average consumer would unattentively agree to conditions that they could have objected to if they had been more aware of the impact of the settings. Similarly, **information overload** and the presentation of too much and/or too complicated information may equally be considered misleading under Article 7(2) UCPD (regarding hidden or obscured information) and the UCTD (see Section 4.2.5). Even though there are often limitations to disclosing information, information that can have a serious impact on the consumer's choices must be sufficiently prominently displayed and not buried among less important or incoherent information or complex or incoherent document structures.

4.2.4. 'Blacklisted' practices – Article 5(1) and (5) and Annex I of the UCPD

Practices that are included in the list in Annex I UCPD are, according to Article 5(5) UCPD, considered in all circumstances to be unfair ([88]). Unlike the rule of Article 5(2)

([86]) In particular, several class actions against Apple in connection with the iPhone; Euroconsumers, 2021. 'Stop planned obsolescence – the Apple case' (https://www.euroconsumers.org/activities/stop-planned-obsolescence-apple-case, last accessed: 20 December 2022).
([87]) See CJEU, judgment of 12 May 2011, *Ving*, C-122/10, EU:C:2011:299, paras 52–59.
([88]) Article 5(5) UCPD.

and Articles 6 to 8 UCPD, the idea of unfairness does not require a case-by-case assessment of the possible negative impact of the practice on the transactional decision of the average consumer. Most practices in this list are, however, not of direct concern to traders in and manufacturers of connected cars. Nevertheless, the study team refers specifically to **practice No 22, concerning the commercial intent of the trader**, already mentioned above.

4.2.5. Unfair Contract Terms Directive – UCTD

4.2.5.1. Unfairness test

The scope of the UCTD is broad, as it applies to all consumer contracts for the supply of goods and services ([89]). An unfair contractual term is defined in Article 3(1) UCTD as a term that has not been individually negotiated and is contrary to the requirements of good faith, thus causing a **significant imbalance** in the parties' rights and obligations under the contract, to the detriment of the consumer. The UCTD provides protection against unfairness in **pre-formulated** terms and conditions ([90]). A consumer is not bound by a contractual term that, following an assessment by the competent authorities, has been considered unfair.

The general **fairness test** of Article 3(1) UCTD requires the assessment of a violation of good faith causing a significant imbalance between the parties' rights and obligations. Whether a significant imbalance exists must be determined taking into account all circumstances of the case at the moment of the conclusion of the contract and all other terms of the contract (Article 4(1) UCTD) ([91]). In addition to the general test of Article 3(1), Article 3(3) refers to an annex that contains an indicative and non-exhaustive list of contract terms that **may** be regarded as unfair. Furthermore, the UCTD contains **transparency** requirements: standard contract terms must be drafted in plain, intelligible language (Article 5) and consumers must have a real opportunity to become acquainted with such terms before the conclusion of the contract (point 1(i) of the annex and recital 20). Failure to meet the transparency requirements can be an element in the assessment of the unfairness of a given contract term and can even indicate unfairness ([92]). A lack of transparency will normally be considered against good faith, if it causes a significant imbalance. The enforcement practice and case-law indicate that it is indeed an important element. The term 'fairness' may also imply that non-advantageous or unexpected terms should be given appropriate consideration. In summary, the fairness test involves an assessment of good faith, balance and transparency. The fairness test often comes down to the question of whether the trader deals fairly with the consumer, whether they take the consumer's legitimate and foreseeable interests into account, and whether the consumer would have agreed to the term in individual negotiations. If a contract term **deviates from certain binding or**

([89]) European Commission, 2019. Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, OJ C 323, 27.9.2019 (UCTD guidance), 9.
([90]) UCTD guidance, 9.
([91]) A fairness test cannot be related to the 'core terms', that is, the definition of the main subject matter of the contract, or to the adequacy of the price and remuneration (Article 4(2) UCTD). Where the provision of personal data would be considered a main subject matter of the contract or would be considered the price (a controversial issue in legal literature), the test would not be applicable. This study is, however, focused on the purchase of a car, including the payment of a price in currency.
([92]) UCTD guidance, Section 3.1.

even supplementary legislation, or obscures such rules, this may indicate a significant imbalance ([93]). In this context, recital 42 of the GDPR refers explicitly to the UCTD, stating that, in accordance with the UCTD, a pre-formulated declaration of consent must be provided in an intelligible and easily accessible form, using clear and plain language, and it should not contain unfair terms ([94]). Furthermore, the recital states that for the consumer to provide informed consent they require at least information about the identity of the controller and the purposes of data processing. Thus, the GDPR refers to a complementary application of consumer law and data protection law.

A regional court of Berlin ([95]) decided that **privacy policies** are preformulated standard terms and must comply with the principles of consumer law regarding the clarity, specificity and fairness of such standard clauses. A privacy policy is not just a unilateral declaration by the trader. In a case concerning iTunes, the court found that eight clauses caused a significant imbalance between the parties' rights and obligations. Privacy policies that are part of, or ancillary to, terms and conditions, whether or not by referral, have been criticised under consumer law and particularly the UCTD, usually jointly with claims based on the GDPR, in the field of social media and connected products, such as sports wristbands ([96]) and toys ([97]). In the case of connected toys, joint actions were undertaken by several European and US consumer organisations ([98]).

4.2.5.2. Transparency principle

The UCPD requires that consumers must be given the **real opportunity to become acquainted** with contract terms **before** the conclusion of the contract (point 1(i) of the annex and recital 20), meaning that, first of all, the terms (including privacy policies that are considered part of a contract) must be **available** before a contract is signed, and must be easily accessible. **Being available** also means that the consumer must be made aware that certain annexes or ancillary documents (such as terms and conditions and privacy policies that are made part of a contract by reference ([99])) may contain important information about the processing of the consumer's data. The purchase contract terms must refer to such documents, preferably providing a link if the documents are electronic. Such a link, and a real opportunity to read the relevant documents, such as a privacy policy, must be available before the consumer is registered or undergoes any other enrolment process. This also applies to contractual

([93]) UCTD guidance, Section 3.4.2.

([94]) The EDPB *Guidelines 05/2020 on consent under Regulation 2016/679* (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf) also refer to the importance of using understandable language, the absence of legal jargon, the avoidance of overly long privacy policies, and the avoidance of obtaining consent through hidden statements in general terms and conditions (Nos 66 and following).

([95]) Landgericht Berlin, judgment of 30 April 2013, *Apple*, 15 O 92/12 (https://www.vzbv.de/sites/default/files/downloads/Apple_LG_Berlin_15_O_92_12.pdf, last accessed: 20 December 2022).

([96])

([97])

([98])

([99]) As stated previously, we use the term 'privacy policy' to indicate a privacy statement or notice that is made part of a contract by reference. This term is commonly used on traders' websites and in terms and conditions that refer to such documents.

documents of third parties such as other content providers, processors or other suppliers that must be easily available.

If the documents are available, it is expected that by reading the contract an average consumer can decide whether they want to be contractually bound by agreeing to the preformulated terms ([100]). Article 5 UCTD provides that all contract terms must be drafted in **plain, intelligible and unambiguous language**. This is a requirement for all contract terms, but evidently all the more important in view of the significance of the contract terms for the transaction and its economic impact. Consumers must be able to **evaluate the economic consequences** of a contract term or contract. A breach of the transparency requirement of Article 5 UCTD may imply a significant imbalance, as stated in Article 3(1) UCTD. Furthermore, material information may be considered hidden, obscured or unintelligible and therefore considered omitted under Article 7(2) UCPD. A lack of transparency may occur through the use of complicated, vague or abstract terminology; the complicated or incoherent structuring of documents; a failure to highlight important provisions or the hiding of important provisions among other provisions; mere reference to certain laws without providing their text or a reasonable explanation; or the provision of overly long or complex documents that would require an unrealistic time or effort to read (information overload), possibly in combination with a difficult layout ([101]). Examples in the area of social media can be learned from BEUC's analysis of TikTok's privacy policy and terms of use ([102]), concerning, inter alia, the sharing of data.

Relevant terms not being made available in the **national language** of the target audience may add to the lack of transparency and thus contribute to an infringement of Articles 3(1) and 5 UCTD. Although plain English may be understood by a large number of consumers in different European countries, especially by consumers interested in rather sophisticated products such as connected cars, 'legalese' English is usually not sufficiently understandable for consumers. Therefore, the Court of Appeals of Berlin decided that the extensive, complex set of terms and the privacy policy of WhatsApp, only available in English and difficult to understand, were invalid ([103]).

Terms can be presented as pop-ups when devices are started or apps are installed. Because the medium can be difficult to read, and the time available to users is often short, it can be necessary to provide links to websites where the relevant terms can be read or downloaded ([104]). The use of the word 'may' is also criticised as suggesting that the situations in terms are hypothetical, leaving users unclear about what is really happening.

([100]) CJEU, judgment of 23 April 2015, *Van Hove*, C-96/14, EU:C:2015:262, para. 42.
([101]) See, for example, Forbrukerrådet, 2016. *#Toyfail*, p. 12.
([102]) BEUC, 2021. *TikTok without Filters* (https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf, last accessed: 20 December 2022), pp. 23 and following.
([103]) Verbraucherzentrale Bundesverband, 2016. 'WhatsApp must provide terms and conditions in German' (www.vzbv.de/sites/default/files/en_kom_2016-05-13_pm_whatsapp_ibu.pdf, last accessed 20 December 2022).
([104]) See the examples of the confusing inconsistent availability of terms and conditions in relation to connected toys in Forbrukerrådet, op. cit., p. 10.

4.2.5.3. Assessments under the UCTD

The UCTD has often been used by consumer organisations to screen for respect of consumer law in relation to data processing in connection with social media and connected products, such as toys and sports wristbands ([105]).

The **subjects** of unclear terms in terms and privacy policies or, in general, the subjects of significant imbalances between parties (which may still occur if the terms are clearly understandable as such) can be diverse, but in many cases resemble the criticisms in relation to the omitted topics that – irrespective of their assessment under data protection legislation, that is, the GDPR, which is not within the scope of this study – can, where applicable, also be regarded as unfair under the UCPD. These criticisms include the following:

- by signing a contract in relation to a service, a consumer must consent to terms stating that their personal data can be used for targeted advertising;
- recipients with whom data may be shared are indicated vaguely, which is especially a problem if the consumer must consent to such data processing if they want to purchase the product or service;
- the consumer must (automatically) consent to the collection of more data than is necessary for the service ([106]);
- terms state that data can be used 'for several purposes', without limiting the purposes;
- in general, terms in relation to data processing through wristbands are asymmetrical and obscure;
- consumers are provided with insufficient information about their right to withdraw their consent or to delete their data or to request that their data be deleted (which could be important in the event of the second-hand sale of the car) ([107]);
- information regarding security is insufficient or there is no guarantee;
- insufficient information is provided concerning data portability, affecting consumers' decisions to switch to other providers and thereby creating a lock-in effect (through material omission and imbalance);
- the use of pre-checked boxes results in the broad implicit consent of the consumer, etc.

Even if a practice listed above would probably constitute a breach of the GDPR, a national enforcement authority, competent to enforce the applicable national consumer law framework, might also consider that consumer law applies to the case and that such practices might, at the same time and under the condition that the respective legal

([105]) See the references above.
([106]) For example in the wristbands report.
([107]) For example Forbrukerrådet, op. cit., pp. 25–26.

requirements are met, infringe the national laws implementing the UCTD and/or the UCPD ([108]).

The topics listed here can often be qualified under the UCTD as 'unclear' provisions that can create a significant imbalance to the detriment of the consumer, even if the information is provided. These topics can sometimes also be challenged as misleading omissions under the UCPD ([109]), for example if the information is simply not provided or is provided in a hidden or obscure manner, and (more exceptionally) as infringements of professional diligence under Article 5 UCPD. Depending on the circumstances of the case in question, these rules can, where applicable, also intersect with claims based on the GDPR or the ePrivacy Directive.

4.2.5.4. List of unfair terms (UCTD Annex) – Connected cars

Article 3(3) UCTD refers to a non-exhaustive and indicative 'grey list' of contractual terms that may be regarded as unfair, which is set forth in its annex ([110]).

According to point 1(j) of the annex, terms that have the object or effect of enabling the trader **to alter the terms of the contract unilaterally** without a valid reason that is specified in the contract may in principle be considered unfair. However, such terms are allowed for a contract of indeterminate duration, provided that the trader is obliged to inform the consumer with reasonable notice and that the consumer is free to dissolve the contract (point 2(b) of the annex). Furthermore, a change that is not communicated in due time to the consumer results in the consumer being bound by **a term with which they could not become acquainted (an infringement of point 1(i) of the annex)**.

Consumer organisations often complain about contract clauses that allow a trader to unilaterally change the terms of the agreement (including a privacy policy) without specific consent from or informing the consumer, thus giving the trader the opportunity to change the purposes or other features of the processing of data, or the recipients with whom the data is shared ([111]). Such clauses should at least state that the trader will notify the consumer about a change in due time, and that the consumer may terminate the contract (although that is evidently not a realistic option where consumers have made a rather expensive purchase, such as in the case of contracts related to connected cars). Many terms or privacy policies state that consumers should examine for themselves whether the standard documents have changed, which is not realistic, considering the lengthy nature of such documents.

According to **point 1(k) of the annex**, terms that have the object or effect of enabling the trader to **alter unilaterally without a valid reason any characteristics** of the product or service may be unfair.

According to **point 1(b) of the annex**, terms that have the object or effect of enabling the trader to **limit the legal rights** of the consumer vis-à-vis the seller or supplier or another party in the event of the inadequate performance of any of the contractual obligations may be unfair. The GDPR states that data controllers and, in certain

([108]) See Section 4.2.3 of this report, and in particular CJEU, judgment of 28 April 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322.
([109]) UCPD guidance and case-law of the CJEU confirm that the UCPD can be combined with the UCTD (see UCPD guidance, Section 1.4.5, p. 19).
([110]) In the *Matei and Matei* case, C-143/13, para. 60, the CJEU refers to the annex as a 'grey list'.
([111]) See, for example, the Norwegian Consumer Council report in relation to connected toys.

circumstances, data processors are **liable** for any damage to data subjects caused by violations of the GDPR. They can only be exempt from liability if they prove that they are not in any way responsible for the damage (Article 82 and recital 146 GDPR). Therefore, terms that exclude or limit the liability of the trader for violations of the GDPR, or that exclude or limit the trader's liability in general without making an exception for damage resulting from a violation of the GDPR, are illegal. Such terms may even be considered unfair if they exclude or limit the liability of third parties with whom the trader has shared the data ([112]).

([112]) See European Commission, 2019. *Consumer protection cooperation action on Facebook's terms of service*, factsheet (https://commission.europa.eu/system/files/2019-04/factsheets_on_the_changes_implemented_by_facebook.pdf, last accessed: 20 December 2022).

4.3. Consumers' expectations

4.3.1. Introduction

The main objective of the consumer survey was to identify what information about the processing of vehicle-generated data an average consumer considers most important when purchasing a connected car to allow them to make an informed purchasing decision. In order to understand this, the survey measured the importance consumers attach to different areas of information (e.g. what data are gathered, how they are used and whom they are shared with) through two complementary indicators.

- The **relative** importance of these topics compared with each other. That is, respondents were presented with several subsets of topics in several iterations rather than all of the topics at once. They were asked to choose the most and least important factors in each subset (i.e. comparing the relative importance of each factor with the other factors in the list). Based on their responses, a relative ranking of topics in terms of importance could be calculated.

- The (self-reported) likelihood that information about these topics would affect their purchasing decision.

In addition, the survey measured respondents' awareness of and knowledge about connected cars, their (known) ownership of a connected car and the importance of connected services compared with other aspects of the car. These indicators were included to assess whether there could be an association between consumer's awareness, knowledge, ownership of connected cars and their importance to the consumer on the one hand, and what respondents found relatively important to know about data collection in connected cars on the other hand. Assuming that consumers' ownership, awareness and knowledge of connected cars will increase in the coming years, a difference in attitudes among respondents who currently already score higher on these parameters than the average respondent participating in our survey could be an indication of possible future shifts in what the average consumer will come to consider important information.

Finally, the survey also looked at what **sources** respondents said that they would be likely to use to gather information about the connected services of a car they were considering purchasing. While not directly related to the question of what information they find important, the findings for this indicator could contribute to recommendations about how and where such information is best presented to consumers.

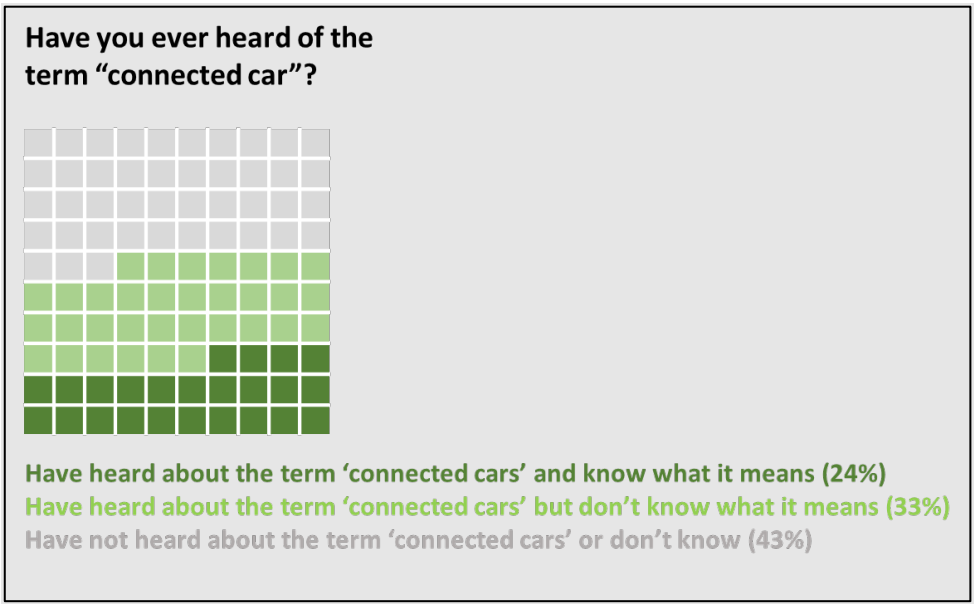
4.3.2. Consumers' knowledge of and attitudes towards connected cars

Just over half of respondents were familiar with the term 'connected car' in the sense that they had at least heard it. At the same time, the measured indicators show that this familiarity is largely superficial, and knowledge about the concept is generally low. This is likely to reflect the fact that connected cars are not yet commonly on people's radars. Most respondents claimed to have never driven a connected car in the 3 years before the survey, and only a small proportion said it was important that their next car had internet-connected services.

Awareness

Almost 6 in 10 respondents (57 %) had heard the term 'connected car' (Figure 4.1). However, awareness among consumers remained superficial, as only 24 % reported knowing what the term meant. This awareness was not related to age.

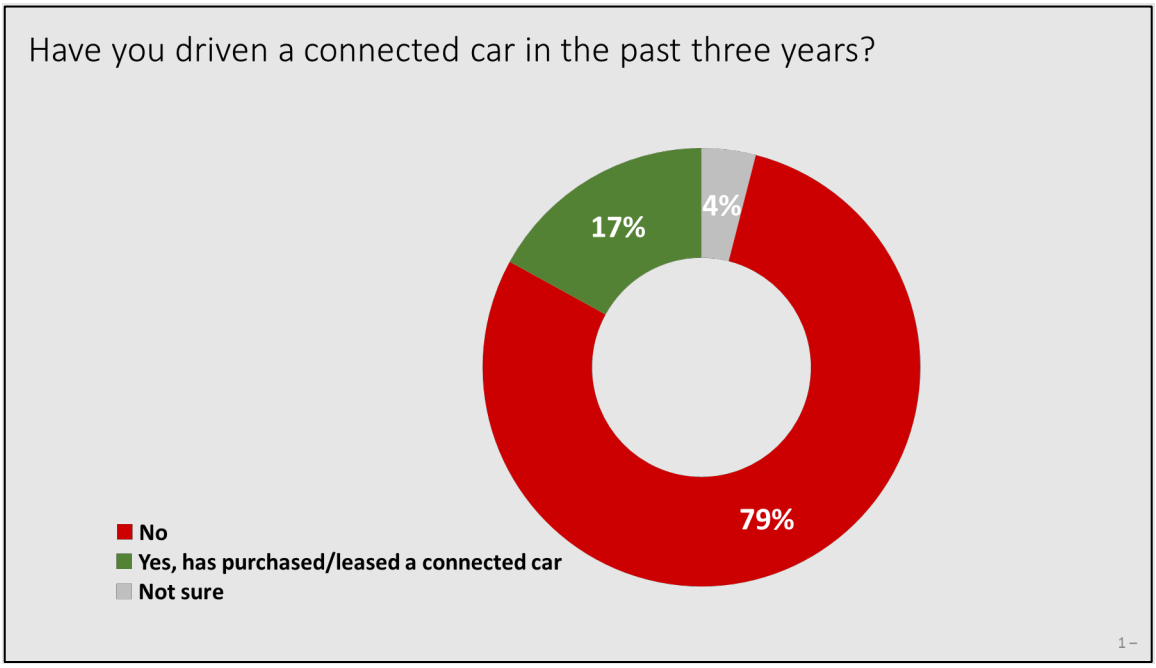
Figure 4.1. Connected car awareness



Ownership

Once the survey explained what the term 'connected car' meant, 17 % reported having bought or leased a connected car in the 3 years before the survey (Figure 4.2). A further 4 % could not tell for sure whether the car they bought/leased was connected or not. The large majority, however, reported not having purchased/leased a connected car (79 %) ([113]).

Figure 4.2. Connected car ownership



NB: Includes all respondents (*n* = 1 438).

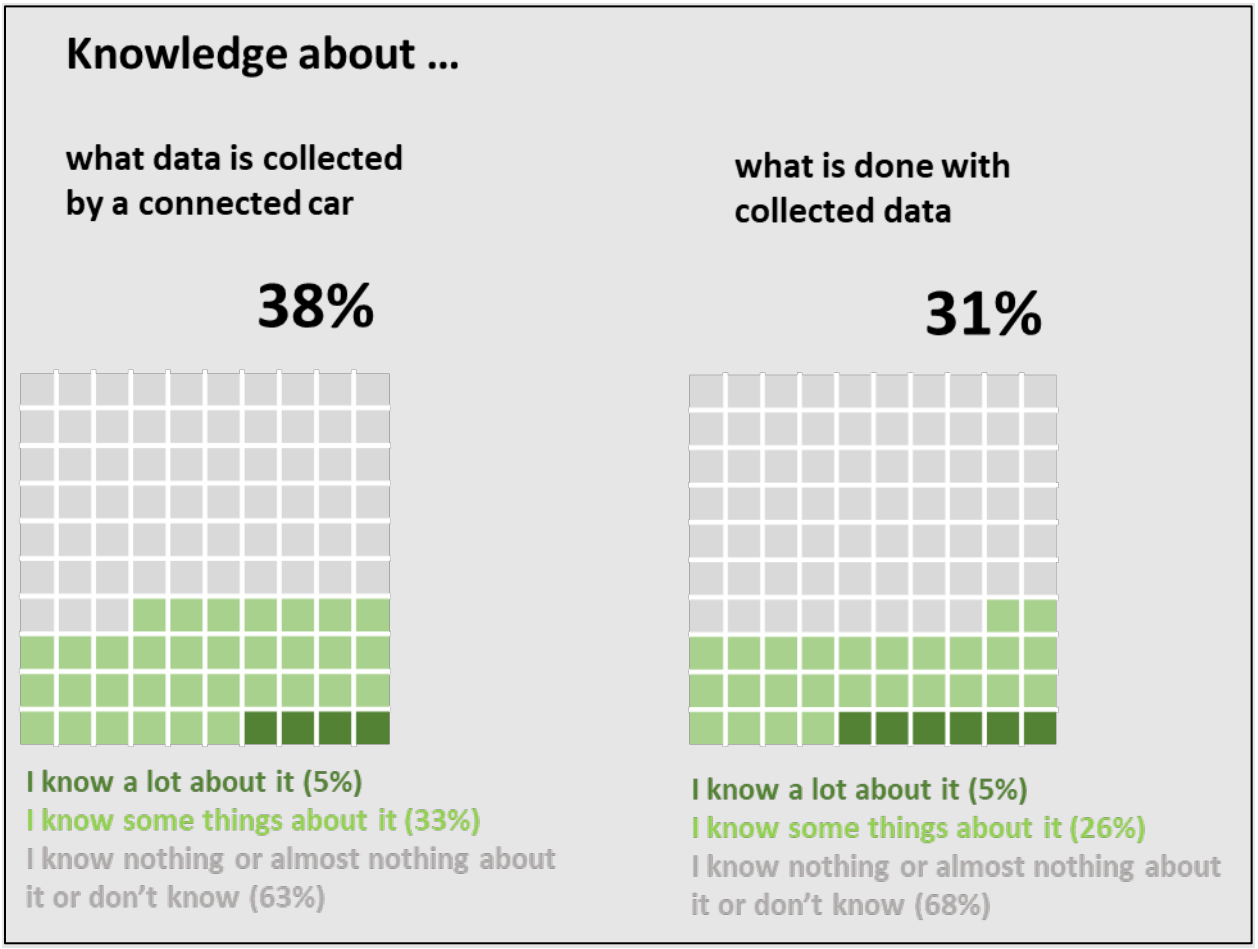
The purchase or lease of a connected car was somewhat more common among the younger cohort. Some 24 % of those under the age of 35 reported that they had bought/leased a connected car in the 3 years before the survey, compared with 15 % among those aged 35 or over.

([113]) Note that this figure includes people who had not bought or leased a car at all in the 3 years before the survey.

Knowledge

Once the survey explained what the term 'connected car' meant, 38 % of respondents also claimed to know at least some things about what data are collected by connected cars, and 31 % reported having the same level of knowledge with regard to what is done with these data (either in the car or externally by the car manufacturer or third parties) (Figure 4.3) ([114]). In total, around 4 in 10 respondents (41 %) reported knowing at least some things about either of these topics. Respondents who reported knowing **a lot** about these topics were, however, very rare, only 5 % for each topic.

Figure 4.3. Knowledge of data processing in connected cars

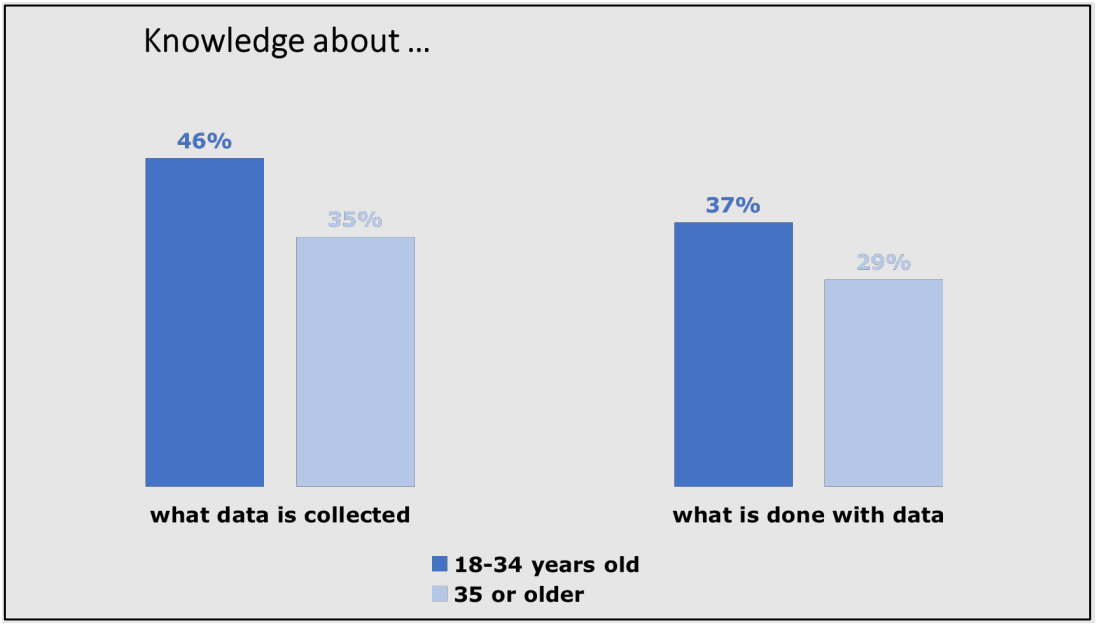


NB: Based on responses to the question 'How much would you say you know about …? What data a connected car collects / How the data collected by a connected car are used (by the car or by third parties such as the car manufacturer)'; includes all respondents (*n* = 1 438).

([114]) Respondents were presented with the following definition: 'A "connected car" is a car that has its own connection to the internet or to other devices. This allows the car to communicate with other devices both inside and outside the car, and also to share data outside the car that has been collected in the car. These data can, for instance, include technical information about the car, your location or your driving behaviour. These data can be used for several purposes, for instance to stream music or videos from the internet, to help you navigate, to monitor the use of the car and driving behaviour, to allow automated driving, to help with the maintenance of your car, etc.'

The younger generation (18–34 years) reported that they knew at least some things about what data are collected (46 % vs 35 % for older consumers (35 years or older)) and what is done with these data (37 % vs 29 %). Notably, for both topics more younger respondents claimed to know a lot about what data are collected and what is done with the data (9 % and 10 %, respectively, compared with 3 % and 4 %, respectively, among older consumers).

Figure 4.4. Knowledge of data processing in connected cars (by age)

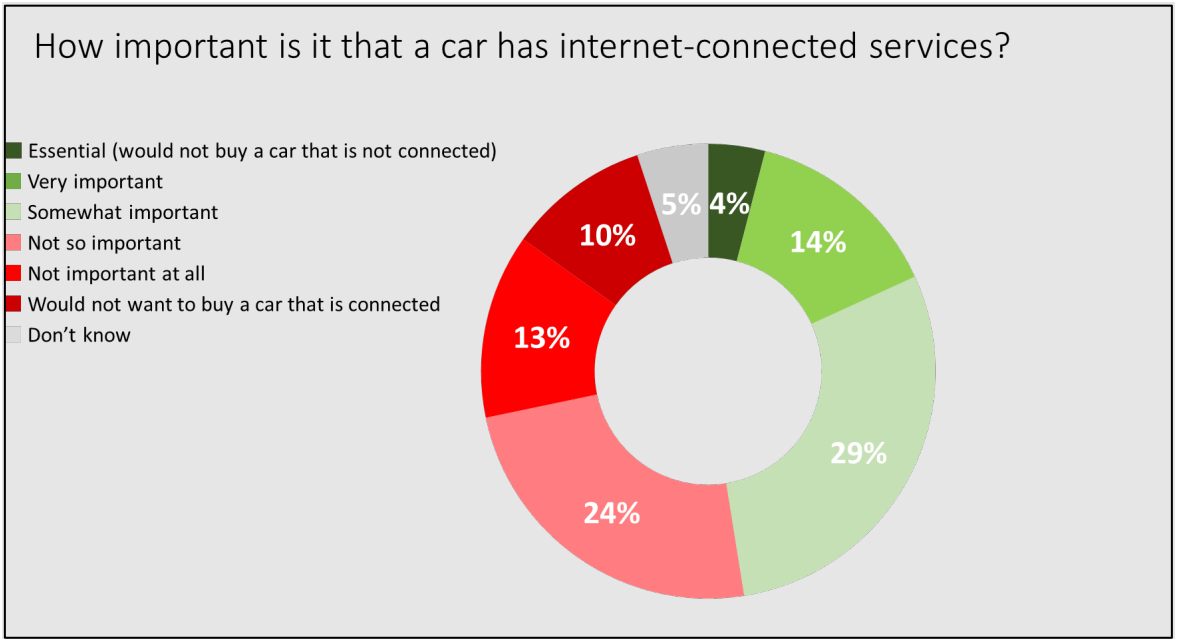


NB: Based on responses to the question 'How much would you say you know about …? What data a connected car collects / How the data collected by a connected car are used (by the car or by third parties such as the car manufacturer); includes all respondents (*n* = 1 438).

Importance

Faced with the scenario of purchasing a connected car in the month after the survey, around half (47 %) of respondents found it at least somewhat important that the car they would buy would have internet-connected services (Figure 4.5). At the same time, an equally large group found this not important or said explicitly that they did not want to buy a connected car. The group of those who would not want to buy a connected car was in itself relatively small, accounting for only 10 % of respondents. This indicated that, while only a small group of respondents was decisively against buying a connected car, the rest of the sample was split on whether or not they found connected services important.

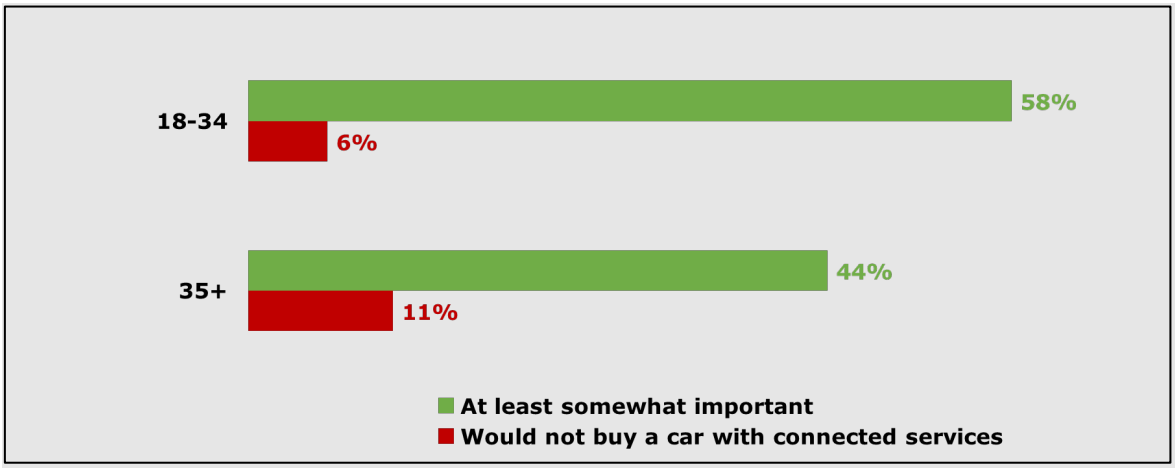
Figure 4.5. Importance of connected services when purchasing a car



Based on responses to the question 'Imagine you will buy a car next month. How important to you is it that this car has internet-connected services?' Includes responses from all consumers (*n* = 1 438).

There was a difference in responses between younger cohorts (18–34 years) and older cohorts. Almost 6 in 10 (58 %) of the younger generation found it at least somewhat important that their next car would have connected services, compared with 44 % of those aged 35 or over (Figure 4.6). Some 6 % would not want to buy a car with connected services at all, compared with 11 % of the older cohort.

Figure 4.6. Importance of connected services when purchasing car (by age)



NB: Based on responses to the question 'Imagine you will buy a car next month. How important to you is it that this car has internet-connected services?' Includes all consumers (*n* = 1 438).

In summary, respondents were not very familiar with the concept of connected cars, and only a small percentage knew what the term 'connected car' meant. There was, however, a considerable minority that had some awareness of the concept and (once it was explained what the term meant) said that they had at least some knowledge of what data are collected by connected cars and what is done with the collected data. Importantly, this awareness and knowledge were higher among the younger cohort (18–34 years). Similarly, while few had bought a connected car in the 3 years before the survey, this was more common among young people,. The younger cohort also generally found it more important that their next car would have connected services. This suggests that the importance of connected services for consumers will grow in the coming years, and is likely to cause a greater need for more and better information on these services.

4.3.3. Consumers' information expectations – Approach

4.3.3.1. Selection of information topics

In a survey, it is easy to ask about what information consumers find important to get when buying a product such as a connected car, but difficult to get good responses. A simple open-ended question where respondents can respond with any answers they could think of would be very likely to lead to responses that would be difficult or even impossible to analyse, as responses to open-ended questions in online surveys are

typically short, formulated ambiguously and not always relevant to the research question. Therefore, we decided to start by presenting an extensive but closed list of topics to the respondent.

The objective of the survey then became twofold: (a) to rank these topics from the topic the average consumer most wants to receive information about to the topic they would least like to receive information about; and (b) to ask consumers regarding each of the topics presented how likely it is that the information they receive about the topic will influence their eventual purchasing decision.

The topics used for this purpose were identified based on the work carried out in the legal mapping phase of the study (see Section 4.2). Using the findings of the legal mapping, 10 topics were defined and then presented to respondents in the survey along with clear examples. The topics and examples used in the survey are as follows:

- what companies collect and use data from the car's connected services;
- your rights as a consumer (how you give consent for the collection and use of your data, whether the car manufacturer can unilaterally change how data are used, etc.);
- what data are collected (technical car data, data about driving habits, geolocation, etc.);
- the purpose of data collection and data processing (navigation, driver's safety, car assistance, car maintenance, entertainment, communication, insurance management, etc.);
- with whom data will be shared (the manufacturer, insurance companies, advertisers, law enforcement authorities, other vehicles, car repairers, etc.) and in which countries they will be stored;
- your control over the collection and use of your data (which data it is optional to collect and for which data it is required, whether you can stop data collection, whether you can decide whom data are shared with, whether data are stored only in the car or also outside the car, etc.);
- the security of your data (protection against hacking, safe storage of data, for how long you will receive security updates for the software, etc.);
- how data are collected (through the Global Positioning System (GPS), sensors in the car, cameras, manual input from the driver, etc.);
- how and when data are shared (live at any time, at regular intervals, only when the car is serviced or repaired, etc.);
- whether you can transfer your data to another car or device (for instance, when you buy a new connected car or want to transfer data from your car to another device, such as your smartphone).

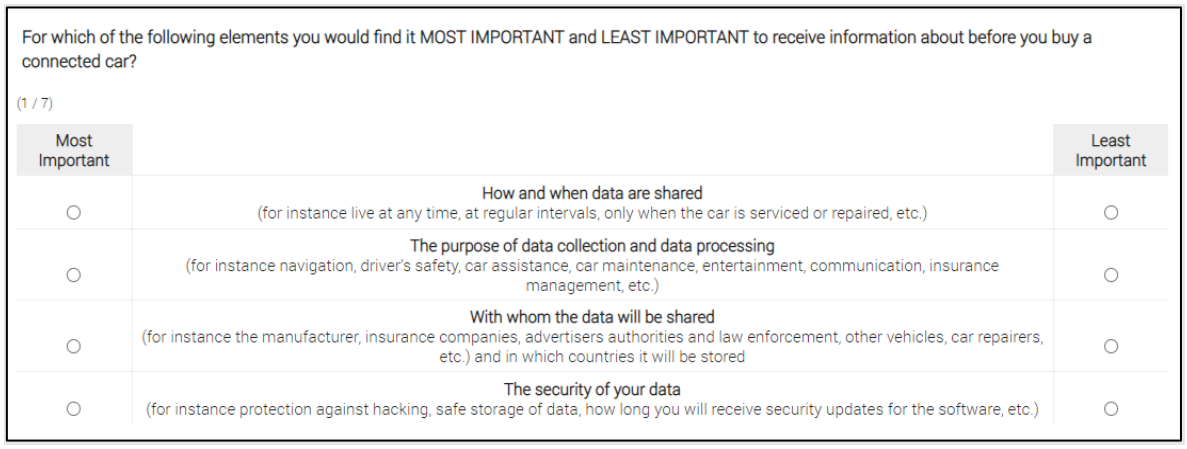
4.3.3.2. Measuring relative importance

Measuring the relative importance of a large set of factors, as was the goal of this survey, can be challenging, as respondents sometimes find it cognitively difficult to rank multiple factors in a list, or simply lack the inclination to do so. Often, they will pick factors placed towards the top of a list, ignoring those further down. Alternatively, they may find it relatively easy to identify the most and least important factors but find discriminating between factors of moderate importance difficult. Multiple choice and grading questions aimed at gauging relative performance can be subject to further response effects, such as response set effects or 'straightlining' (the selection of the same response for most or all topics).

Given these issues, a more sophisticated form of stated importance analysis was used, one that both lowers the cognitive load on consumers and more accurately mimics the decision-making process associated with a purchase. Specifically, we used a maximum difference scaling (**MaxDiff**) approach, sometimes also referred to as 'best–worst scaling'.

Respondents were presented with subsets of the total list of factors considered, rather than all of them at once. They were then asked to choose the most and least important factors in each subset (see Figure 4.7 for an example of one such subset used in the survey. The process was repeated to test numerous combinations of factors being evaluated (and to make sure all topics were included multiple times).

Figure 4.7. Example of MaxDiff question

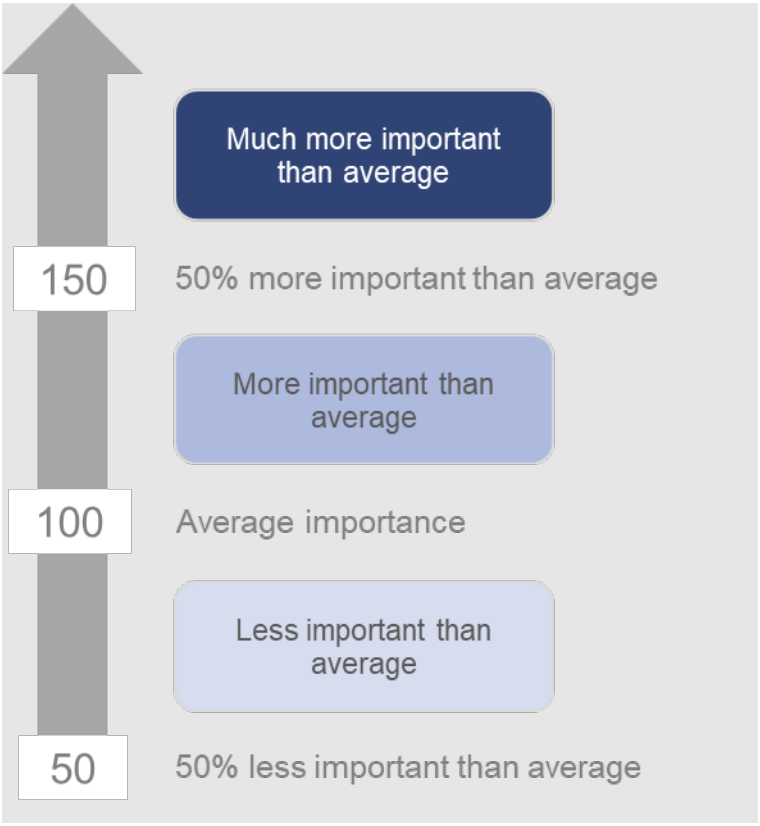

For which of the following elements you would find it MOST IMPORTANT and LEAST IMPORTANT to receive information about before you buy a connected car?

(1 / 7)

Most Important		Least Important
○	How and when data are shared (for instance live at any time, at regular intervals, only when the car is serviced or repaired, etc.)	○
○	The purpose of data collection and data processing (for instance navigation, driver's safety, car assistance, car maintenance, entertainment, communication, insurance management, etc.)	○
○	With whom the data will be shared (for instance the manufacturer, insurance companies, advertisers authorities and law enforcement, other vehicles, car repairers, etc.) and in which countries it will be stored	○
○	The security of your data (for instance protection against hacking, safe storage of data, how long you will receive security updates for the software, etc.)	○

From the resulting data, it is possible to derive an overall ranking of all the topics for the sample as a whole and to arrive at a **relative importance score** for each topic. This score reflects the perceived importance of each topic in relation to the others among respondents. The score revolves around an index of 100, which represents the average of the scores for all items. A score of 150 for topic A and a score of 100 for topic B means that topic A is found to be 50 % more important than topic B. Likewise, a score of 50 for topic A and 100 for topic B indicates that topic A is found to be 50 % less important than topic B (see Figure 4.8).

Figure 4.8. MaxDiff score scale



4.3.3.3. Results

The results of the MaxDiff analysis are shown in Figure 4.9. From the ranking of the topics and each topic's score, it is clear that two topics in particular stood out as being most important for respondents to receive information about when buying a connected car, compared with other topics.

- The **security** of the data processing (protection against hacking, the safe storage of data, how long the consumer will receive security updates for the software for, etc.). With a score of 194, this topic scored almost twice the average score across topics, and 35 points more than the second most important topic.

- The level of **control** that the consumer has over the processing of the data (which data it is optional to collect and for which it is required, whether you can

stop data collection, whether you can decide whom data are shared with and whether data are stored only in the car or also outside the car, etc.).

Figure 4.9. Relative importance of information topics (MaxDiff scores)

NB: Based on responses to the question 'For which of the following elements you would find it most important and least important to receive information about before you buy a connected car?' Includes all respondents (*n* = 1 438).

Other topics were found to be less important than these two by a considerable margin. It is notable from this ranking that several topics that are considered fundamental to inform consumers about under European data protection and consumer rights regulations were found to be of minor relative importance to consumers, most notably what data are collected, and which companies collect and use these data. This is not to say that this information was neither relevant nor important to respondents. It only reflects that it was of less **relative** importance than other aspects that were presented to respondents in the survey.

The ranking of the importance of the topics is very stable across different profiles of respondents. In all sociodemographic subgroups, the security of the data and control over the collection and use of the data were the most important topics. This held regardless of respondents' age, awareness of the concept of a connected car, knowledge of data collection and use in connected cars, purchase/leasing of a connected car in the 3 years before the survey, and how important they found it that a car would have connected services if they were to buy one in the month after the survey.

It is notable, however, that receiving information about the security of the data and, particularly, the control the consumer has over the processing of the data were found

to be considerably more important than other topics by what one could call 'less engaged' respondents, that is respondents who did not own or lease a connected car, who found it less important that their next car would be connected, were less aware of the concept of a connected car, and had less knowledge of what data are collected and what is done with these data. The same holds for the topic that ranked third overall, information about consumers' rights. This is shown in Table 4.1. A possible explanation for this is that among such respondents distrust in data processing in connected cars was higher, and indeed this could be a reason that they were less engaged with connected cars in the first place. As a result of this distrust, it is possible that they were more concerned about the security of their data and wanted to receive more information about how they could control what data is collected, how the data are used and with whom they are shared, or even stop data collection altogether. Their greater interest in information about their rights as consumers could be interpreted in the same way, considering that such respondents would want to make sure that nothing is done against their will and that third parties do not take advantage of them or their data.

Table 4.1. Relative importance of information topics (by consumer subgroup)

Topic	Total	Connected car ownership		Connected car awareness		Connected car importance		Connected car knowledge	
		Yes	No/don't know	High or medium	Low or none	High or medium	Low or none	High or medium	Low or none
The security of your data	194	182	196	188	195	191	194	186	199
Your control over the collection and use of your data	159	145	162	151	162	148	169	150	166
Your rights as a consumer	124	114	127	118	126	116	131	116	130
With whom the data will be shared	122	117	123	119	124	116	128	116	127
The purpose of data collection and data processing	104	106	104	106	104	109	103	107	102
What data are collected	80	84	79	85	78	83	77	82	79
How and when data are shared	61	70	59	63	60	66	55	66	57
What companies collect and use data from the car's connected services	58	61	57	61	57	56	59	59	57
How the data are collected	49	60	46	54	47	56	42	57	43
Whether you can transfer your data to another car or device	49	60	46	56	47	59	41	61	41

Taken together, these results indicate that, the lower a consumer's level of knowledge and/or interest is in connected services of a car, the more important it is for them to receive clear information about how they can ensure that they can shield their data and themselves from what they perceive as potentially harmful risks of that connectedness. This is especially the case because connected services are increasingly included in the standard set of features for cars, making it extra important that less engaged consumers are well informed. This also holds for consumers that are more engaged with the concept of a connected car, for whom information about data security, data control and consumers' rights clearly remain the most important topics.

Among the survey respondents, the majority were 'less engaged' consumers. It is essential that dealers and manufacturers take this group into account, for instance by making sure that they put the topics of data security and consumers' control and rights at the forefront of their communication.

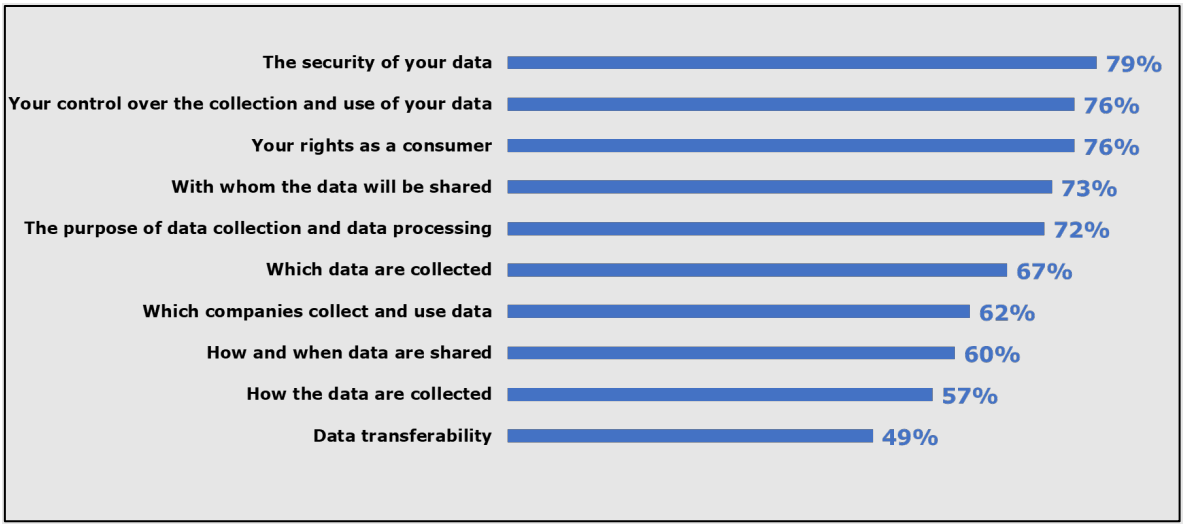
4.3.4. Likely impact of information on consumers' eventual purchasing decision

In addition to the relative importance consumers attach to a wide range of information topics, the survey also measured the likelihood that the information a consumer receives about these topics will influence their purchasing decision. This relates to a crucial aspect of the concept of material information: information is material if the presence or absence of this information is likely to have an influence on the purchasing decision of the consumer.

The results for this indicator, presented in Figure 4.10, closely follow the relative importance ranking presented in the previous section. Information about data security, control over the collection and use of data, and the consumer's own rights were the three topics for which it was most likely that the information provided would influence the respondents' purchasing decisions. Notably, for all but one of the presented topics more than half of respondents thought it was at least somewhat likely that the information they got about it would influence their purchasing decision. The likelihood ranged from 79 % (information about data security) to 49 % (information about data transferability). This suggests that for the average consumer almost any aspect of data collection and use in connected cars might be crucial and a potential deciding factor in whether to proceed with a purchase.

The finding that almost all topics were found to be likely to influence the consumer's purchasing decision by at least half of survey respondents does not contradict the importance scores discussed in the previous section (see Figure 4.9). The importance scores shown in Figure 4.9 reflect the **relative** importance attached to topics **compared with each other**. The results show, for instance, that receiving information about the security of the collected data (importance score of 194) was found to be almost twice as important as receiving information about the purpose of data collection and data processing (importance score of 104). These scores do not reflect the **absolute** importance attached to topics **in their own right**. Indeed, the finding that information about data security was often thought to be more important than information about the purpose of data processing does not mean that the latter topic cannot be considered very important in itself. This explains why there were large differences in the relative importance of topics, while at the same time all or most of these topics were reported by respondents to be likely to have an influence on their purchasing decisions.

Figure 4.10. Likelihood that information will influence purchasing decision



NB: Based on responses to the question 'If you were thinking about buying a car with internet-connected services, how likely is it that your decision to buy the car or not would be influenced by the information you receive about the following topics?' Percentage of those whose decision is very likely or somewhat likely to be influenced by the information; includes all respondents (*n* = 1 438).

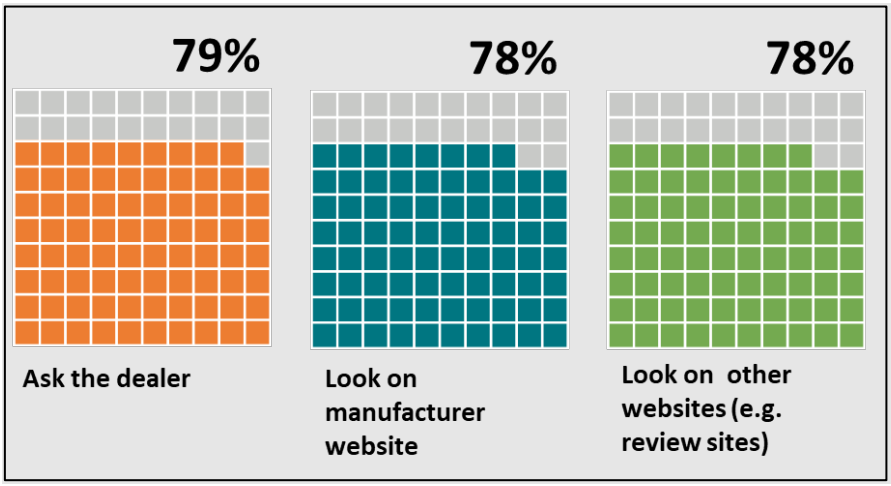
In general, consumers who were less familiar with the concept of a connected car, who had less knowledge about connected cars and who would find connected services less important when buying their next car were less likely to say that the information they got about the processing of data in connected cars would influence their purchasing decision than more engaged respondents. However, among any group of respondents for each of the topics presented, a majority still thought that it was likely that the information would have an influence (Figure 4.10). The sole exception was for the topic of data transferability.

This shows that, while less interest in or knowledge about connected cars among consumers can be linked to relatively less importance of this information to the consumers, all of the topics presented still represent information that, on average, is expected to have an impact on consumers' purchasing decisions, with the possible exception of the topic of data transferability.

4.3.5. Consumers' preferred information channels

The survey also measured what respondents would do to gather information about connected cars if they were interested in purchasing one. None of the potential sources of information asked about in the survey stood out as being clearly more favoured than the others, and each of them was at least somewhat likely to be used by around 8 in 10 respondents (Figure 4.11).

Figure 4.11. Likelihood of using sources

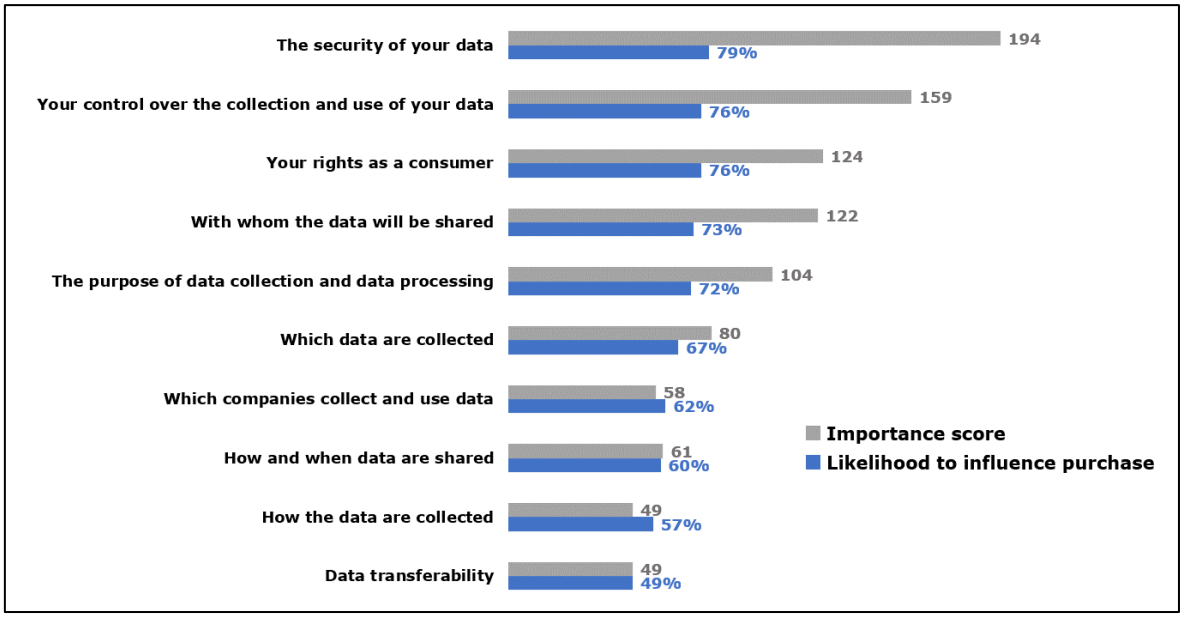


NB: Based on responses to the question 'When thinking about buying a car with internet-connected services, how likely is it that you would do the following things to find out more about how data are collected and used in this car?' Includes all respondents (*n* = 1 438).

4.3.6. Conclusion – What information is important to consumers?

Figure 4.12 shows the relative importance of each of the information topics that relate to the collection and use of personal data in connected cars for the average respondent in the survey, and how likely they thought it was that information about the topics would influence their decision to buy a connected car.

Figure 4.12. Importance of information topics and likelihood of influencing purchasing decision



From these results and the analysis in the previous sections, it is clear that, with the possible exception of the topic of data transferability, each of the topics has the potential to be 'material', in the sense that at least half of the respondents who participated in the survey indicated that their purchasing decision was likely to be affected by what information they received about these topics. This held across different sociodemographic profiles (e.g. age, gender and educational level) and also applied to respondents with less interest in and knowledge about connected cars and connected services. This suggests that respondents believed that they **should always receive information about the 10 topics that were asked about in the survey**.

That is not to say that each of these topics is **equally** important to consumers. The respondents that participated in the survey found it most important, relative to other topics, to receive information about **the security aspects of data processing in connected cars**, and about **the control they have over this processing**. While it would be important to provide information to consumers about any of the topics considered, the survey results suggest that consumers would prefer these two topics in particular to be prioritised in communications from dealers and manufacturers, so that the consumers have easy access to them.

It should also be kept in mind that the importance afforded to the information topics presented in the survey is fundamentally subjective and reflects respondents' own perspectives and priorities. These priorities may not always be fully in line with what are objectively speaking the topics that allow consumers to be maximally empowered

and to make the best purchasing decisions and take action when confronted with unfair practices or a lack of compliance with regulations on the trader's side. For instance, while knowledge about their rights as consumers is arguably fundamental to counter potential issues when purchasing a connected car, the survey shows that respondents found several other topics more important to know about.

Finally, when it comes to the channels via which this information should be communicated, respondents showed no clear preference. Asking a dealer, checking the manufacturer's website or checking a third-party website were all popular means that a majority of respondents reported that they would rely on when looking for information on connected cars. This means that in practice manufacturers and dealers should be ready to provide information both through their websites and during visits to dealerships.

4.4. Assessment framework

4.4.1. Introduction

This chapter provides an overview of the different requirements that connected car dealers and manufacturers are expected to comply with during the marketing and pre-contractual phases of commercial communication when it comes to providing information about the processing of vehicle-generated data. This set of requirements was informed by the findings of the legal framework mapping (see Section 4.2) and the survey gathering consumers' expectations (see Section 4.3). The legal framework that was applied does not include the data protection framework. In other words, the study team did not assess manufacturers' and dealers' performances against the GDPR or the e-privacy directive.

The set of requirements is not exhaustive. That is, a strict and comprehensive application of the legal framework does lead to additional rules and best practices beyond those listed here. Priority is given here to the most important rules and best practices, specifically those where a breach of compliance would probably have most impact on consumers and equate to the most significant breach of EU consumer law.

As discussed at the beginning of this report (see Section 3.2), it is important to keep in mind that traders must always comply with all the legal requirements. This means that any element of information that is legally required must be available to consumers in some form, even if the consumer survey suggests an apparent lack of relative importance attached to some elements by consumers. Information about what topics consumers found most important in the survey can, for example, inform the case-by-case assessment of what information is considered 'material' under the UCPD by the competent authorities.

Keeping this in mind, these topics receive the most attention in this chapter and were most extensively investigated in the manufacturer assessments. Specifically, this concerns:

- the **security** of data processing (protection against hacking, the safe storage of data, etc.);
- the **control** of the consumer over the collection and use of data (which data it is optional to collect and for which data it is obligatory, whether the consumer

can stop the data collection, whether they can decide whom data are shared with, etc.)

In addition, specific attention was paid to information about **data sharing** and where data are stored. This aspect ranked high in the consumer survey in terms of importance among the topics that consumers would like to receive information about. Given the additional risks that come with sharing personal data with certain recipients, especially when the data have a commercial purpose, it is also interesting to identify the quality of information provision about data sharing. The exchange of data and related elements (what data are shared, with whom data are shared and why data are shared) thus also receive close attention in our assessment.

4.4.2. Overview of legal obligations and consumers' expectations

4.4.2.1. Access to information

First of all, it is necessary to have a general overview of the sources of information on connected services and data processing, including verbal information provided by salespeople during dealership visits, printed materials provided during dealership visits, and connected services' websites containing information and/or containing available terms and conditions and specific privacy policies for the connected services. Understanding the landscape is important before focusing on the availability and content of the information as such.

The consumer survey indicated that consumers do not have a preferred channel for obtaining information on connected cars. Verbal information from a salesperson during a visit to a car dealer, written documentation, a dedicated website and general websites are all regarded as potentially valuable sources of information.

Salespeople are the most direct source of pre-contractual information, although they are not necessarily the first source of information that is used by consumers. The obvious importance of this information channel is that it enables (or should enable) interactive information provision through direct questions and answers. Furthermore, they are a classic source of information for less tech-minded consumers, who find it difficult to navigate the internet for online information.

As outlined above, the material information that must be provided is the information that may have an impact on the consumer's transactional decision. The assessment considers the question: 'If the information that was omitted had been provided, would the average consumer still be likely to have made the same transactional decision?' In this regard, it is not necessary that salespeople acting as an information channel provide all the detailed information that is considered material. A trader is entitled to provide additional sources of information, for example in written documents or through a referral to a website where consumers can find more detailed information. But if such additional information is **not available**, or if it is **insufficiently clear or difficult to find**, there could be a misleading omission of material information. As explained in the legal mapping exercise, whether or not there is an omission of information that would mislead an average consumer depends largely on the circumstances of the case.

However, since many topics in the field of data processing may be considered to have a material impact on the consumer's transactional decision to purchase a connected car

(as suggested by the results from the consumer survey; see Section 4.3), it can be argued that a salesperson should at least be able to provide basic verbal information on the material topics or should be able to highlight relevant information in written materials on the spot. As aspects of the security of data processing and the possibility of the consumer exercising a certain degree of control over data processing are clearly considered important information topics by consumers, the salesperson should at least be able to provide basic information on these topics. It is also clear that a salesperson should spontaneously, without being asked, tell the consumer that data processing takes place, that there are certain risks involved in the field of data safety (security), that data can be used for certain purposes and can be shared with certain recipients for purposes that may have an impact on the consumer, that data can be seen by other persons (e.g. other users of the car) and that certain data (such as location data) can be sensitive. These issues are foreseeable risks, and the consumer should therefore be spontaneously informed about such risks, at least with basic information that may be completed by online information.

The provision of false information, including the overall presentation of information that (probably) deceives the average consumer and is likely to have an impact on their transactional decision, may constitute a misleading action (Article 6 UCPD). If a salesperson stated falsely that a connected car does not process personal data, that would be false information, which could have a significant impact on the consumer's transactional decision.

Information in **written** materials, such as leaflets, does not necessarily have to contain exhaustive information about data processing (including the actual collection of the data), but it should point out the information that is considered first-line information, especially when the verbal information is not satisfactory. In accordance with the case-law of the CJEU concerning consumer protection ([115]), such documentation should refer clearly to a website that contains easily accessible information, and a readable and understandable privacy policy and terms and conditions. Consumers should be able to become acquainted with such documents before they are bound to a contract (point 1(i) of the grey list in the annex to the UCTD ([116])), and these documents should be downloadable when the contract or subscription is agreed electronically, enabling the consumers to keep and prove the document that they accepted (Article 10(3) of the e-commerce directive).

If information that can be considered material is hidden or buried in text that is difficult to read, or otherwise difficult to find, or when the phrasing of terms is difficult to understand, ambiguous, unintelligible or presented in a way that makes them difficult to read, the information can be regarded as **insufficiently transparent**, and may be regarded as omitted information (Article 7(2) UCPD). Article 5 UCTD contains a similar legal requirement: when the documents containing information must be considered unilateral terms and conditions binding the consumer (which is obviously the case for terms and conditions governing connected services and, it could be argued, the privacy policies, if referenced), these must be transparent (drafted in plain, intelligible language), and consumers must have a real opportunity to become acquainted with the terms before the conclusion of the contract (point 1(i) of the grey list in the annex to

([115]) As mentioned earlier, compliance with the specific information requirements of the GDPR was not assessed.

([116]) The annex to the UCTD contains an indicative and non-exhaustive 'grey list' of clauses in consumer contracts that may be regarded as unfair.

the UCTD and recital 20 UCTD). A lack of transparency should be considered an act against good faith, if it causes an imbalance between the trader and the consumer. The terms might then be considered unfair under Article 3(1) UCTD and consequently not binding on the consumer.

Furthermore, if a contract term would deviate from certain binding or even supplementary legislation in the field of consumer protection, or would obscure such rules, this may indicate a significant imbalance, according to the UCTD guidance, and thus an infringement of Article 3(1) UCTD.

In the end, the most important question is whether the consumer is sufficiently informed on the topics that are considered material for their transactional decision, considering all the available sources of information.

4.4.2.2. Basic information on connected services and data processing

It is crucial that the consumer is made aware that personal data are processed as part of the connected services, and that they understand the basic implications of this. False information relating to this elementary issue should be considered misleading.

Information on the **main characteristics** of products must be given as material information (Article 7(4) UCPD). The more complex products are, the more detailed information the consumer should be given about characteristics that may have an impact on their transactional decision, in particular concerning **risks** (see Article 6(1)(a) UCPD). The fact that personal data are collected and processed implies certain risks linked to hacking, leakage, or the use of this information for profiling, the personalisation of services or pricing, automated decision-making, direct marketing, etc.

The following could be considered first-level material information ([117]).

- Information on **who** collects/processes data. The identity of the trader that the consumer is dealing with is deemed material information (Article 7(4) UCPD and Article 5 CRD).

- **What data** are collected. These include, in particular, biometric and location data, which can be considered sensitive.

- The **purposes** of data processing. The UCPD guidance ([118]) states that certain uses of data must be considered material information, which cannot be omitted, such as the use of data for commercial purposes, marketing, profiling, personal pricing based on data on consumers' behaviour or automated decision-making. It can be argued that an exhaustive overview of the purposes of data processing is material information, providing the consumer with a better view of the risks involved and the opportunities they have to exercise control over the use of their data. Furthermore, a trader hiding the commercial intent of a certain practice, may be considered a breach of point 22 in the blacklist in Annex I UCPD. Furthermore, Article 5(1)(g) CRD requires information about the functionality of

([117]) This is also provided in the information obligations in the GDPR.
([118]) UCPD guidance, Section 1.2.10.

digital content, for example when it is used for the tracking of consumer behaviour and personalisation (recital 19 CRD and CRD guidance ([119])). See also, in this regard, references to case-law in Section 4.2 above.

The study examined three specific topics of first-level information that should be considered material, and that were particularly highlighted in guidance documents, case-law and the consumer survey conducted as part of this study (see Section 4.3). These are:

- information on the control that a consumer may exercise over data processing, including information on the rights of the consumer;
- information on the general issue of the security and safety of data processing and connected services;
- the fact that data are shared with certain recipients and related information.

Other topics of information, while they may not be considered first-level information, may also be considered material.

In some contexts, information on **how data are collected** (e.g. through sensors or GPS) could be considered material, but this depends on what data are collected and is in general less relevant (as responses from consumers in the consumer survey show).

4.4.2.3. Information on data security

The security of connected services and data processing were considered the most important topic to receive information about by respondents in the consumer survey (see Section 4.3), considerably more so than other topics. As a consequence, we consider this a key topic that cannot be omitted.

This implies that at least the issue of risks and security should be spontaneously brought up during dealership visits, and the provision of false information must evidently be avoided (Article 6(1) UCPD). Further information should be easy to obtain through verbal information, written documentation or sufficiently clear information on websites (possibly a dedicated privacy policy). The topics that the study reviewed relate to general information in the field of security, and more specific issues regarding detailed information, for example where data are stored, how this information can be found and the clarity of the information.

The study also focused on the question of whether, where there are multiple users of a car, users would be able to see the data related to other users. Such data can be sensitive (e.g. location data may reveal sensitive information about a person). It can be argued that this is a concern that consumers are not necessarily aware of when they have not encountered connected services before.

([119]) CRD guidance.

4.4.2.4. Consumers' control over data processing

The control that consumers have (or, on the contrary, do not have) over the processing of their data is a second important topic identified in the consumer survey as being of key importance to consumers. It is clear that consumers want to know, for example, whether they can limit the scope of data that are processed, the purposes of data processing, the duration of data processing or the sharing of their data, and whether they can delete data, or whether they have to accept the process as it is once they have signed a contract. We believe that basic information should be provided **spontaneously** during dealership visits and more detailed information should be found **easily and in clear language** in written documentation, such as brochures, or online on web pages, in dedicated privacy policies or in dedicated terms and conditions.

The possibility of exercising control over data processing is linked to the **legal grounds** of the processing. When the processing is **necessary** for the performance of the connected services or even the (correct and safe) functioning of the car, the consumer is not always entitled to object to, limit or stop or withdraw their consent to certain aspects of data processing. If data processing is based on the consent of the consumer, the consumer can have more flexibility to be able to accept, reject or stop or withdraw their consent to certain aspects. If data processing is necessary for a particular reason, the reason should be real and correct (see above).

The consumer has **specific rights** under the GDPR, such as the right to have an overview of their data, or demand rectification. These rights should not be obscured by misleading information. Moreover, given the important concerns of consumers in this field, material information relating to the possibility of having control (or not having control) over their data and the rights of consumers should not be omitted.

A specific topic is the possibility of **disconnecting** the services in order to stop data processing. Consumers should be informed about whether or not they are able to do this (and, if possible, how they can do this).

4.4.2.5. Data sharing

The sharing of personal data with certain recipients, while not among the top three topics consumers participating in the consumer survey considered important to know about, may still be considered material. Indeed, both the European Commission and case-law consider this topic vital, especially (but not exclusively) when the data are shared with third parties for commercial purposes, the data can be monetised, or data sharing will have an impact on the consumer through targeted marketing, the personalisation of services or pricing, or automated decision-making.

Consumers should be **spontaneously** informed that data sharing will occur – if this is the case – and whether or not they can refuse to share their data. They should be informed of the identity of the recipients, preferably by name, or if this is not possible at least the categories of recipients ([120]). They should also be informed of the scope of

([120]) Without prejudice to the information requirements of the GDPR in this respect.

the data that are shared and the purposes of data sharing (with a specific focus on commercial use, marketing and other uses that may have an impact on the situation of the consumer), and the possibility of consenting to or refusing data sharing. This information can be regarded as information about certain risks that the consumer must be aware of, and that may influence the consumer's decision to purchase the car. The information about the recipients, the scope of the data and the purposes of data sharing should be exhaustive and should not be extended unilaterally without the consumer's consent. Where consumers are not informed spontaneously about these topics, at the very least clear information should be available online as text on a website or in the relevant privacy policies. The importance of this information has been confirmed in case-law and guidance documents ([121]).

If the shared data relating to the consumer are anonymised, there is no risk of this affecting the consumer and the obligation to provide information is therefore less relevant. This is also true of certain pseudonymised data, depending on the circumstances and in particular the techniques used for pseudonymisation.

With regard to the information that is provided, the study assessed whether this information was clearly presented in the relevant sources of information, whether it could be found easily and whether it was understandable for the average consumer.

4.4.2.6. Specific uses of data

The use of personal data for **profiling**, **personalisation** of services (and pricing) and **automated decision-making** creates specific risks for consumers, and when such uses occur they should be clearly indicated as material information.

Furthermore, the consumer should be informed about the purposes and the consequences of these specific uses. The GDPR provides the consumer (data subject) with certain rights in this respect. In the case of automated decision-making that produces legal or significantly similar effects (e.g. when insurance premiums are calculated by automated systems based on data related to the consumer's behaviour), the consumer should be able to challenge the consequences, and to request a human review of the process. The study team considers the information about these rights to be of material importance, as manufacturers should not obscure the legal rights of the consumer.

4.4.2.7. Changes to privacy policies or terms and conditions

According to point 1(j) of the annex to the UCTD, terms that have the object or effect of enabling the trader to alter the terms of the contract unilaterally without a valid reason that is specified in the contract may be considered unfair. However, such terms

([121]) See, for example, UCPD guidance, Section 1.2.10; and the action of the Italian Competition Authority against Facebook in 2018 (Italian Competition Authority, op. cit.). See also, within the framework of the GDPR, Article 29 Data Protection Working Party, 2018. *Guidelines on Transparency under Regulation 2016/679* (https://ec.europa.eu/newsroom/article29/items/622227, last accessed: 20 December 2022) (WP260 rev. 01), especially the annex, p. 37.

are allowed for a contract of indeterminate duration, provided that the trader is obliged to inform the consumer with **reasonable notice** and that the consumer is **free to dissolve** the contract (UCTD annex, point 2(b)). Furthermore, a change that is not communicated in due time to the consumer results in the consumer being bound by a term with which they cannot become acquainted (an infringement of UCTD annex, point 1(i)).

Consumer organisations have, in the past, complained about contract clauses that allow a trader to unilaterally change the terms of the agreement (including a referenced privacy policy), thus providing an opportunity for them to change the purposes or other features of data processing, the sharing of data with certain recipients, etc., without specific consent from or informing the consumer. Such clauses should at least state that the trader will notify the consumer about a change in due time, and that the consumer may terminate the contract (although that is evidently not a realistic option for contracts involving rather expensive products, such as contracts related to connected cars). Considering the lengthy nature of privacy policy documents and terms of service, it is not realistic to expect consumers to monitor themselves whether and where changes are made to these documents.

According to point 1(k) of the annex to the UCTD, terms that have the object or effect of enabling the trader to alter unilaterally without a valid reason **any characteristics of the product or service** may be unfair.

4.4.2.8. Exclusion or limitation of liability

According to point 1(b) of the annex to the UCTD, terms that have the object or effect of enabling the trader to limit the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of the inadequate performance of any of the contractual obligations may be unfair. The GDPR states that data controllers and, in certain circumstances, data processors are liable for any damage to data subjects caused by violations of the GDPR. They can only be exempted from liability if they prove that they are not in any way responsible for the damage (Article 82 and recital 146 GDPR). Thus, terms that would **exclude or limit the liability** of the trader for violations of the GDPR, or that would exclude or limit the trader's liability in general without making an exception for damage resulting from a violation of the GDPR, would be illegal. Furthermore, such clauses may be regarded as obscuring the consumer's rights as a data subject under the GDPR and could even be regarded per se as infringements of professional diligence (Article 5 UCPD).

Therefore, when any exclusion or limitation of liability regarding damages was mentioned we examined whether this also applied to damages caused by non-compliance with data protection regulations.

4.4.2.9. Termination and lock-in

The duration of the contractual rights and obligations in the context of connected services and the duration of data processing should be clear. Overall, consumers should be informed about how long they will have to respect obligations and how long they can expect to rely on the services. We consider this to be material information. Some

information is indirectly linked to the lifespan of the services (such as information on software updates, which we review as a separate issue).

Furthermore, consumers should be informed about whether or not the termination of data processing has an impact on the performance of the car as such, and whether or not such termination has a direct or indirect cost impact on the further use of the car. They should also receive information about whether they are locked in to the services.

In addition, the possibility of obtaining the data after termination and/or of transferring the data to other systems (data portability) may have an impact on the consumer's opportunities to terminate data processing, or to switch to another provider, and thereby escape the lock-in effect. This is a transactional decision that is affected by the opportunities that are available. Furthermore, data portability is a right under Article 20 GDPR that should not be obscured by misleading information or otherwise unfair terms and conditions. Furthermore, it cannot be ruled out that a forced lock-in would be regarded as a general unfair practice (an act against professional diligence or good faith) under Article 5 UCPD.

4.4.2.10. Software and security updates

The sales of goods directive requires a trader of a product to supply updates, including security updates, in the case of **goods with digital elements** for a continuous supply of the digital content or digital service, to keep those goods in conformity for 2 years after the delivery of the goods. Article 5(1)(g) CRD requires the provision of information about the functionality of a product or service, which may include information on the minimum presented (or even warranted) lifespan and the availability of software updates. Information on the expected lifespan through updates can be considered material information. Furthermore, the early obsolescence of connected systems may trigger the additional issues of lock-in and lack of data portability, which may be regarded as general unfair practices (infringements of professional diligence and good faith) under Article 5 UCPD.

Security updates are also related to the issue of security, which, as discussed in Section 4.4.2.3, consumers consider it highly important to receive information about.

4.4.2.11. Codes of conduct and external supervisory authorities

As part of the study, this review examines if manufacturers mention whether or not they follow any codes of conduct, and whether or not they mention any external supervisory authorities that can be contacted to raise questions/complaints.

This may not be considered material information, depending on the code of conduct. However, it is interesting to know whether this information is provided in the general framework, and certain well-known codes of conduct may provide specific safeguards or benefits that consumers may be aware of, in which case such information could possibly be regarded as material.

4.4.2.12. Basic information on contracting

It should be clear to consumers **when** they are bound by rights and obligations in relation to connected services and data processing and/or **which formalities** are needed for them to be bound or to give their consent to the processing of their data, which can be explicit or implicit.

It is at least necessary to provide consumers with basic information on this contractual process. The omission of information in this respect or the provision of obscure information may be regarded as a misleading practice under Article 7 UCPD or unfair contracting on the basis of unclear information (Articles 3 and 5 UCTD), depending on the circumstances.

4.5. Traders' practices

In this section, we present general trends across manufacturers and indicate some best practices from specific manufacturers when it comes to the provision of information about data processing in connected vehicles, as encountered during the mystery shopping visits to dealers and manufacturers' websites.

Detailed analyses of individual manufacturers (see Annex 1) uncovered important differences between manufacturers, and a lack of uniform practice in the sector. However, when it comes to the basic provision of information to potential car buyers two consistent trends were observed by the study team across all manufacturers.

- The verbal information provided by salespeople during dealership visits was usually not satisfactory under the requirements of legal obligations.

- Printed documentation was only rarely provided and usually did not contain information about data processing (if documentation was provided, it was typically not very helpful in terms of information about data processing within connected services).

The differences between the manufacturers appeared more obvious when it came to the more dedicated online sources about the connected services, that is, websites about the connected services and their specific privacy policies and terms and conditions.

4.5.1. Information provided during dealership visits

Salespeople at dealers' sites are generally expected to act as the first source of information about the connected services of a car, the related data protection issues and in particular the issues in this context that may have an impact on the transactional decision of a consumer, particularly their decision on whether or not to purchase a certain car model (i.e. the material information). Although it is likely that at least some consumers will conduct their own research online before or after a dealership visit, salespeople are still the most direct point of contact.

Since connected services and the processing of personal data in the context of the services create certain risks for consumers, consumers should be made aware of those risks early in the purchasing process. This concerns, in particular, risks in relation to security (the hacking of software, of the data or even of the car as such; data leaks and

data theft; and the sharing of data with other users of the same car and subsequent purchasers of a car), and in relation to profiling, the personalisation of services or prices, automated decision-making, targeted marketing and other commercial uses of data. In the first place and at a minimum, consumers must be informed about the existence of such foreseeable risks. Only when they are aware that there are risks can they reasonably be expected to try to collect further information about how those risks are dealt with. Their purchasing decisions may be affected by that additional information. The consumer survey conducted as part of this study found that the information concerning these topics is regarded by consumers participating in the survey as information that may be considered material, with a high likelihood of having an impact on their transactional decisions.

In stark contrast with the needs and reasonable expectations voiced by consumers in the survey, we observed that salespeople only rarely mentioned the existence of connected services in the car spontaneously. Typically, mystery shoppers had to ask for this information. It is obvious that, when the connected services are not even mentioned, consumers' overall risk awareness will be seriously hampered, and this may restrict the consumer's ability to make a well-informed purchasing decision. A minimum amount of risk-related information should be given spontaneously. All manufacturers performed below a satisfactory level in this respect.

Building on the previous observation, it was also common that, when mystery shoppers mentioned the topic of connected services themselves, salespeople were not sure whether personal data would be collected, or would even contend that no personal data would be collected. If a salesperson says that personal data are not collected when the contrary is in fact true, this can mislead the consumer, which may have an impact on their transactional decision. Even if connected services are not activated by default in a car and are to be installed or activated separately after purchase, it is necessary for car dealers to be able to communicate that these services will, once activated, generate and process personal data.

When salespeople are not able to provide unambiguous information themselves, a second line of recourse is other sources, printed or online. False information that is provided as being certain, however, may result in more direct detriment if the statement is believed to be true. In any case, we believe that, given the fact that this information may be considered material, consumers should have the opportunity to discuss the main issues interactively with salespeople who are sufficiently knowledgeable about the connected services and the important questions relating to data protection. In that sense, it is significant that the knowledge of the salespeople encountered in the mystery shopping exercise regarding connected services was generally found to be below the level that would be needed to inform consumers satisfactorily (the only exceptions being BMW and Volkswagen).

When the issue of connected services is brought up by a visiting consumer, salespeople should, likewise, be able to at least respond by providing certain material information verbally, even if this information is at first not provided spontaneously. During the mystery shopping exercise, there were primarily issues in providing such basic information in response to consumers' inquiries about security (the hacking of the services, the data or the car, and data leaks; the storage of data inside or outside the car; and the protection of users' personal data from disclosure to other users and second-hand purchasers of the car); the fact that data are used for certain purposes that may have an impact on the consumer (personalisation, profiling, automated decision-making, commercial use, marketing); the fact that data may be shared with

certain recipients; and whether or not the user of the car can object to, control, limit or stop the processing/sharing of their data, or control the purposes that the data are used for. These topics were not mentioned very often by salespeople during mystery shoppers' visits, either spontaneously or after probing by the shoppers, and in particular the topic of data sharing was only touched on rarely. Moreover, if information about data sharing was provided it was most often regarded as unclear. Mystery shoppers also reported that they felt in general not well informed about the possibility of controlling and limiting the data processed, and to a lesser extent about data security. The study team, however, believes that these topics should at least be touched on by a salesperson in order to raise consumers' awareness. More detailed information and answers to questions can be presented online, but in that case salespeople should refer to them clearly, to ensure that consumers can find this information.

Printed documentation was rarely given to mystery shoppers during dealership visits. Furthermore, the topics of information included in such documentation seemed rarely helpful in the context of the material information that we considered important – information about consumers' concerns related to personal data processing – and such information rarely contained references to online sources. Rather, information was almost always limited to the presentation of the connected services themselves and the benefits of these services for consumers. In the study team's view, this is a missed opportunity, as printed documentation could be a helpful substitute for or complement verbal information provided by salespeople, especially if they are unable to provide detailed information themselves.

Likewise, it would be useful for salespeople **to refer consumers by default to the dealer's or manufacturer's website** for more detailed information on the car's connected services. However, this did not occur systematically during the mystery shopping visits either.

4.5.2. Online information

Typically, the studied manufacturers had pages on their websites dedicated to the connected services (or often a collection of various connected services and applications). These usually contained some basic information about the functionality/usefulness of the services, occasionally with a short online video or with links to more detailed information. More rarely, these web pages contained detailed information about the data that are processed. The study team believes that BMW's website can be considered an example of good practice in this regard, with clearly visible data protection topics allowing users to navigate through the privacy policy. The study team also considers Renault France's website a good example, although it provides more limited information. Sometimes there was a clear link to a **specific privacy policy** for connected services. Again, the BMW and Renault France websites were good examples of the provision of dedicated privacy policies, with very prominent links to the relevant web pages. Tesla's privacy policy was also well designed, with the main information presented under a clear heading and hyperlinks that could be clicked to find out more details under each heading. Such clearly visible links raise the awareness of the consumer, who can find detailed information in the privacy policy. However, the mystery shopping exercise revealed that there were different approaches between the manufacturers and even between the different national websites of the same manufacturer. Some manufacturers did not provide a specific privacy policy, only offering a small-font standard link at the bottom of their website referring to a general privacy policy that applied to their entire

undertaking. For Hyundai and Peugeot, it was not possible for the study team to locate a privacy policy dedicated specifically to connected services in any of the countries where these manufacturers' websites were visited by our mystery shoppers.

It is good practice for **online privacy policies** to be downloadable so that a consumer can easily consult the version that they had agreed to when they started the service, and so that this document may serve as proof of what was agreed between them and the manufacturer / service provider. This is especially the case when no privacy policy or terms and conditions are signed as paper documents (in which case the e-commerce directive requires that the contract documents be downloadable). In practice it was not always exactly clear during the mystery shopping exercise when the consumer would be bound by an agreement (e.g. when an app was used for the first time, whether or not jointly with the explicit acceptance of terms and conditions through the click of a button on the website, or after continuing to use a downloaded app on a smartphone). For instance, a few manufacturers seemed to make their app only downloadable through Google Play or Apple's App Store, whereby the applicable terms and conditions and privacy policies were not visible before the app was downloaded and installed. The pre-contractual legal documentation is often not sufficient in those cases, and in some cases the consumer would not be able to become acquainted with the terms and conditions before the conclusion of the contract, even though this is a requirement under the UCTD.

The topics concerning **security** should be found easily online. Most mystery shoppers, however, either could not find this information or found it with (great) difficulty. These topics should be found easily and presented as an intuitive design of web pages with layered information (e.g. clear headings and links, and key information highlighted) ([122]). The study team believes that it would suffice to summarise key information in an easily visible and accessible way, and to refer users to the privacy policy for further information. In particular, information on the possibility that users of the car could see the personal data of other users was rarely provided. Furthermore, if information was provided it was not always found to be clear by mystery shoppers. Only BMW, Volkswagen and Tesla demonstrated satisfactory practices in this respect.

Mystery shoppers found it in general difficult or impossible to find information on topics concerning the possibility of exercising **control** over data collection and data processing. In a minority of cases, mystery shoppers found it easy to find such information. Again, BMW, Volkswagen and Tesla were found to be examples of best practices in this respect ([123]). Overall, information on the possibility of asking for data collection to be stopped was found most often, and information about the possibility of limiting the data that are processed and deleting the data was available less often. Information on the opportunity to decide on the purposes of data processing was only rarely found. However, this topic is important, as it can enable a consumer to limit the use of their data for certain purposes, such as commercial use, profiling, personalisation and

([122]) See, for a good approach, BMW's ConnectedDrive privacy policy (as assessed for Ireland), which is available on its website and provides tiles with the main themes that consumers can click on (such as 'How is your data stored?'). By clicking on this tile, the consumer can read basic information about encryption, secured IT systems and monitoring. This information is easily found but is still high level.

([123]) BMW was found to offer a good example in its privacy policy, where a consumer can click on a tile labelled 'How to change your privacy preferences' to obtain contact details and suggestions about the control that a consumer can exercise; for example, they can restrict or cease the use of certain data, delete data or demand portability.

automated decision-making. Consumers should have a clear view of their opportunities in that respect.

The majority of mystery shoppers also indicated that it was difficult or impossible to find online information about **data sharing**. Information on the possibility of refusing to share data was least often found. Information on the possibility of avoiding data sharing and on the recipients of the data was found somewhat more often. According to the mystery shoppers, quite a number of privacy policies also contained insufficient information on data sharing, in particular in relation to who could be recipients, for which purposes data are shared, and whether or not the consumer could object to or avoid data sharing. The feedback of mystery shoppers varied considerably in this respect. The exclusive use of anonymised or pseudonymised data for sharing was occasionally found in privacy policies.

In general, the mystery shoppers indicated that the information they could find was rather clear and understandable. This may, however, be a consequence of the fact that they would typically only access high-level, general information provided on manufacturers' websites rather than in-depth, complex documents such as privacy policies and terms and conditions. Still, even at that higher level of introductory information, clarity is of course crucial. The review of the privacy policies indicated that the language of the privacy policies was often also found to be clear, but a number of mystery shoppers found that some terms or phrasings were difficult to understand. The information that seemed more difficult to understand was often related to legal concepts, such as the 'legal grounds' of data processing. The analysed privacy policies did not always explain what such concepts meant. For instance, some only mentioned the legal grounds of the processing of certain data together with the listed purpose, without an explanation of what this meant in practice and the impact of the indicated legal grounds on the possibility of the user limiting, changing their preferences for or withdrawing their consent to the processing of certain data. In other cases, the legal ground concepts were not described at all; they were only mentioned in relation to the relevant article of the GDPR, which is evidently not understandable for the average consumer. Topics that have an impact on the consumer should not be mentioned as a legal formality (i.e. a 'ticking the box' approach to legal compliance), but should be explained in clear terms, with a description of the consequences for the consumer. For instance, when the processing of certain data is regarded as a necessity by the manufacturer, such as because it is necessary for the provision of the services (the performance of the contract), for the (safe) use of the car itself or to meet legal obligations, this should be explained in a clear way, and it should be explained whether or not the consumer can limit or terminate data processing under the circumstances. The mystery shoppers found some positive examples in this respect but in other cases indicated that the phrasing of the information was difficult to understand.

Furthermore, the privacy policy presented by the manufacturer in the context of connected services should be a **dedicated privacy policy**, tailored to these services, and not a general privacy policy that is used for the entire business of the manufacturer. A dedicated privacy policy should consider more specific privacy concerns, for example by providing a warning about the visibility of users' data to other users or a warning about what should be done with the data if the car is sold as a second-hand car, or specific information about the storage of the data inside the car system. General privacy policies usually did not contain this specific information or these warnings. Mystery shoppers could also (albeit rarely) find more tailored information about the liability of the manufacturers in the event of breaches of the data protection legislation in specific privacy policies or specific terms and conditions. The study team identified the privacy

policies of Volkswagen and BMW as good examples of detailed, dedicated and extensive privacy policies.

In the privacy policies, mystery shoppers could typically find information on who collects which kinds of data. Sometimes not all data collectors or controllers were indicated by name, but usually these could at least be identified (for instance, certain company group members). Whether or not lists of controllers and processed data were exhaustive or they could only be extended with the consent of the consumer was much less clear to a number of the shoppers.

4.5.3. Specific topics of information

Information about **automated decision-making** was rarely found by the mystery shoppers in the privacy policies. When it was found, the rights of the consumer (as the data subject) were usually described as required by the GDPR. Information about **profiling** and **personalisation** was found more often.

Mystery shoppers were divided in their feedback when it came to information and clauses about **unilateral changes** to the privacy policy or the specific terms and conditions. In many cases, they could not find any indication that they would be informed about changes **before** these would become effective, and a right to object to the changes or to terminate the contract was also rarely found. Some privacy policies, however, did indicate which elements could be changed, and for what reasons, which the study team considers a good practice. In general, however, it seemed from the feedback of mystery shoppers that the information on the rights of consumers was not well covered in a number of documents that the study team reviewed.

An explicit statement that **liability** for breaches of data protection legislation is not limited was also rarely found.

Across manufacturers, information about a guarantee concerning the length of time for which users would receive **software and security updates** was not found by the study team. However, this is important information because it gives an indication of the life cycle of the apps or services, and there is a link with the sales of goods directive.

4.5.4. Consumers' information levels

Considering all sources of information (verbal, printed and online), a majority of mystery shoppers felt that they were not well informed about **security issues**, the **possibility of having control over data processing** and **issues relating to data sharing**.

The assessment was overall more negative than positive for all three of these topics.

Table 4.2 summarises the main findings sorted by phase of the consumer purchasing process, from receiving verbal information from dealers, through consulting other (written) sources, to obtaining the most detailed relevant documents (terms and conditions and privacy policies).

Table 4.2. Summary of main findings

Phase/area	Main findings
Verbal information	• Connected services were rarely mentioned spontaneously by salespeople during visits to dealerships. • Mystery shoppers typically evaluated salespeople as not very knowledgeable about any of the key data processing topics.
Other sources	• Printed documentation about connected services was only very rarely given (and often focused on service characteristics and benefits for consumers rather than on data processing practices). • Mystery shoppers were not systematically referred to online information.
General online information	• Most manufacturers have a dedicated website for their connected services, but the level of detail of the websites visited seemed to differ (including between the same manufacturer's versions for different countries). • Websites rarely contained details on data processing (but if available the information was generally understandable). • A link to a dedicated privacy policy could not always be (easily) found by the mystery shoppers.
Privacy policy	• Not all manufacturers offered a dedicated connected services privacy policy. • The privacy policy, if available, was not always downloadable. • Legal concepts, such as 'legal ground', were not always clearly explained. • Between manufacturers there were considerable differences in the availability of key information. If information was available, this information was not always easily found or well understood by the mystery shoppers.
Terms and conditions	• Terms and conditions were not always (easily) accessible to the mystery shoppers. • Information on liability related to data protection breaches was rarely found.

4.6. Recommendations

Below, we present, based on the findings of the mystery shopping exercise and the subsequent analysis by the study team, a set of recommendations that could be helpful to improve the provision of clear and transparent information during the marketing and pre-contractual phases of commercial communication when it comes to the processing of vehicle-generated data.

Our recommendations outline concrete best practices (rather than focusing on the development of abstract policies) that could realistically be expected to be implemented by manufacturers and dealers.

- The first line of weakness seems to be the attitudes (and probably the knowledge) of salespeople at dealerships. **Manufacturers** could consider establishing a programme for car dealers and their salespeople to ensure that salespeople are trained and have a better understanding of the risks and issues related to the functioning of the connected services and personal data processing, enabling them to point out the main issues spontaneously and to have an interactive discussion with consumers. **Dealers** could ensure that at least certain salespeople have deeper knowledge and can assist their colleagues and consumers where more detailed questions arise during the sales process. Furthermore, salespeople could be trained to refer systematically to where the relevant information can be found, for example which of the materials provided by the manufacturer, including brochures or specific sections on their websites, may be helpful. **Manufacturers and dealers** should ensure that printed documentation about the connected services is available and points out the main issues involved, focusing on security; the possibility of controlling data processing (and the limits of that freedom where data collection is deemed necessary); the specific purposes that involve risks (the personalisation of services and pricing, automated decision-making, targeted marketing and commercialisation); with whom data are shared and why, and whether or not the consumer may change that; and practical issues such as how to prevent users' data against disclosure to other users of the car and how to delete data or disconnect the car. Where more detailed information is necessary or useful, the printed documentation may refer to dedicated web pages of a manufacturer's or dealer's website.

- A web page dedicated to connected car services should already point out basic information, such as the data that are collected, by whom they are collected and with whom they are shared (and why), and an overview of security issues and practical, functional information (possibly with a short video). The main risks should be immediately clear to consumers. The same page should contain a clear hyperlink to the dedicated privacy policy where users can find more information and their commitments and should invite the consumer to read it. In particular, BMW was found by the study team to provide a very good example of how such a page could be designed.

- **Manufacturers** should draft a dedicated privacy policy for the connected services that focuses on the specific privacy issues and security aspects associated with these services. A general privacy policy often contains too much general information that is either not relevant or less relevant than in specific policies. Specific information could focus on how data are stored in the systems of the car itself or on distant servers, how data can be deleted, how user data are protected against disclosure to other users, what should be done with the data when a car is sold as a second-hand car, the cases where data processing is deemed necessary (see below in this list), and the specific sharing of data with the service providers involved, insurance companies, etc. The privacy policy should also be downloadable.

- If changes are made to the terms and conditions and privacy policies, consumers should always have the opportunity to terminate the contract if they do not agree with them, within clear time frames or notice periods.

- Specific terms and conditions for the connected services should be available through the connected services' web page and should be downloadable. It should be made clear on the website when the consumer and the dealer or manufacturer are bound by an agreement. The terms and conditions should deal with unilateral changes in the course of the agreement and make clear that there is no limitation of liability in the event of breaches of the data protection legislation.

- The wording of the privacy policy should not be obscured by a formalistic and sterile use of terms such as 'legal ground', 'legitimate interest' and 'portability', or simple referrals to legal provisions (such as articles of the GDPR), without explaining in clear words what these ideas mean and how they affect the rights of the consumer ([124]). If certain data processing is necessary for the (safe) use of the car, for the connected services, for safety reasons (such as location data for SOS intervention), to meet legal obligations, etc., that should be explained in clear wording and the consumer should understand whether or not they can stop or limit data processing in view of the related concerns.

- Information about software and security updates should warrant a minimum time span for which these updates will be provided for the car model. Consumers should have a realistic view of the life cycle of the car and the connected services in connection therewith, especially when major investments would be necessary to make outdated and unusable systems interoperable.

Table 4.3 summarises our recommendations, again ordered by area of the consumer purchasing process.

Table 4.3. Summary of recommendations

Phase/area	Recommendations
Verbal information	• Better training should be provided for salespeople on data processing in connected services and they should be trained to mention key information spontaneously.
Other sources	• Train salespeople to more systematically refer to online sources. • Develop printed documentation about data collection as part of connected services, containing key information and

([124]) Without prejudice to the controller's information obligations under the GDPR, for example Articles 13(1)(d) and 14(2)(b) GDPR, concerning the indication of legitimate interest.

	referring to dedicated online information with more details.
General online information	• A dedicated connected services website should be easily accessible and contain basic information about key topics, with reference to the privacy policy or terms and conditions for more details. • The main risks should be immediately clear to consumers. • Clear links to the privacy policy and terms and conditions should be provided.
Privacy policy and terms and conditions	• There should be a privacy policy specifically for connected services. • The privacy policy should not be obscured by technical/legal terminology. • In the event of changes to the terms and conditions and privacy policy, consumers should always have the opportunity to terminate the contract, with clear time frames or notice periods. • The terms and conditions should contain clear information on how long users will receive software updates for.

5. Annex 1 – Feedback on each manufacturer

In this chapter we present the feedback on each of the seven manufacturers in the scope of this study, based on the assessment framework developed in Chapter 4. Each feedback report follows the same structure, discussing on the basis of the feedback from the mystery shoppers the extent to which the manufacturer complies with the relevant requirements. Note that the extent of the evaluation depends on the information available, meaning that, if certain sources of information (in particular connected services privacy policies and/or terms and conditions) could not be located by the mystery shoppers or the research team, some topics could not be assessed. See Annex 2 for a full overview of the assessed materials from each manufacturer.

The findings of our manufacturer assessments concern the provision of information on the processing of vehicle-generated data compared with the requirements in this respect under EU consumer law, and not under EU data protection law. Furthermore, it should be noted that the findings presented here were gathered solely for the purpose of this research project and that they by no means constitute or pre-empt the assessment by the relevant competent authorities of whether or not a practice is considered to be in compliance with the applicable legal framework, as such an assessment remains the responsibility solely of these competent authorities.

5.1. BMW

5.1.1. Access to information

During mystery shoppers' visits to the car dealers, salespeople rarely spontaneously mentioned the car's connected services, and aspects of data processing such as security or the sharing of data with third parties were mentioned even less. When the subject of connected services was brought up by the mystery shopper, they usually mentioned that the car collects personal data. Some salespeople, however, did not seem sure about it, and sometimes (albeit rarely) mystery shoppers were told that no personal data are collected, which may be considered misleading information that may have an impact on the consumer's decision to purchase the car. Still, BMW provides examples of best practices in the scope of this study when it comes to the provision of key verbal information, and mystery shoppers generally felt that salespeople were able to always provide some kind of useful information about the connected services. The same applies when it comes to describing the services during sales visits, although this occurred only rarely, including at BMW dealerships. In line with these findings, **mystery shoppers considered the BMW salespeople generally to be knowledgeable about the connected services**. This does not mean that mystery shoppers felt overall well informed about topics related to security, control over data processing or data sharing after their visits: the results reported by the mystery shoppers were evenly distributed between feeling sufficiently informed and insufficiently informed.

In contrast to verbal information, written documentation (specific terms and conditions and privacy policies) was only provided to mystery shoppers occasionally, and rarely spontaneously. Dealers did not provide a specific leaflet or brochure about the car model or the connected services.

A website dedicated to BMW's connected services is available, but not all mystery shoppers were referred to this website by salespeople. Still, such referrals occurred more frequently for BMW than for other manufacturers. Mystery shoppers who were referred to the dedicated website typically received a specific URL (rather than a general instruction or suggestion to visit the manufacturer's website), which is good practice. Not all mystery shoppers found the information on the website to be very detailed, possibly because a substantive part of the information was only

accessible by clicking through and opening other pages beyond the main page. Nevertheless, clear links to specific terms and conditions and a specific privacy policy could typically be found.

The privacy policies were downloadable in some countries, but in others they were not (where they were not downloadable, they were presented in the form of a web page). The privacy policy should be downloadable if the subscription is agreed electronically, to enable consumers to keep and prove the document that they accepted (Article 10(3) of the e-commerce directive). When the contract is signed as a paper bundle and the privacy policy is a printed version within the bundle, this is less strictly required. However, the study team considers it good practice to make the privacy policy downloadable, as this makes the printing and studying of the policy easier.

5.1.2. Basic information on connected services and data processing

According to the mystery shoppers' feedback, **the web pages and/or linked privacy policies contained at least some information on the important topics that could in general be considered material**: the data that are processed, the purposes of data processing, who processes the data, whether data are shared with third parties, how data are kept secure, the control the user has over the scope of data processing or the recipients of data, the control the user has over the use of their data, whether the user can disconnect the car completely, how the user can review and control what data are collected, and whether and how the user can delete stored data. Only rarely did mystery shoppers find no information about these issues. In these cases, the lack of information may be considered an omission of material information, if the relevant information is not provided through a different channel. Considering the fact that, as discussed above, salespeople rarely provided detailed verbal or written information during store visits, it can be reasonably doubted that information not available on the website would be covered by the salespeople.

Mystery shoppers' feedback on the availability of information about who is involved in the processing of data was mixed. Some mystery shoppers reported that the privacy policy stated explicitly that no organisation other than the manufacturer processes the data, but others reported that they were provided with a list of names of companies and some mentioned a list with categories of companies that were not named specifically. This indicates at least that it was difficult for the mystery shoppers to unambiguously determine what information was provided on this topic, potentially signalling some lack of clarity. If mystery shoppers found a list of data processors, it was typically not stated explicitly that this list was exhaustive, despite this being required. Mystery shoppers also did not always find it clear which other companies were involved in the provision of the connected services and whether or not these process data. Typically, some information was found on this topic, but it was often considered by mystery shoppers to be rather general or unclear. Finally, mystery shoppers were unable to identify the responsible data protection officer.

Regarding the scope of the data that are processed, some shoppers reported that the privacy policy listed the exact data types (e.g. 'fuel level'), while others found a mix of exact data categories with more general descriptions (e.g. 'technical car data'). **Not all privacy policies appeared to state sufficiently clearly whether the list of data types that is collected was exhaustive and/or whether the list can only be extended in agreement with the consumer.** This should be clear, as consumers

must always be aware of the data that are processed, whether the processing is based on their consent or another legal ground. This is particularly relevant to more sensitive data, such as location data, which can normally only be processed with the explicit consent of the consumer (this was not always found in the privacy policies of BMW). The list of processed data was found easily in the privacy policy, and was, overall, described as sufficiently clear by mystery shoppers.

Information on the purposes of data processing was found to be given in general, but not always specifically in connection with the data types that were covered by a specific purpose. Most mystery shoppers found that the purposes were defined in rather general terms, but this was in most cases an acceptable practice unless the overall picture of the purposes of data processing was too vague (which does not seem to have been the case for BMW). The information could be found easily in the privacy policy and was considered clear overall, although for some mystery shoppers certain phrasings were more difficult to understand.

According to most mystery shoppers' feedback, the fact that some data can be used for marketing and commercial purposes and/or can be shared for such purposes was mentioned with a sufficient explanation of the meaning of this. Rarely, it was not found to be mentioned anywhere, which one might not expect if the company's strategy in this field were uniform. If the data is used for commercial purposes in these cases, the omission of this information might be considered a misleading and unfair practice in a case-by-case assessment.

Regarding information about the duration of the data retention, shoppers' feedback was mixed. Mystery shoppers found most often that data are kept until the user deletes the data (or requests that their data be deleted). Some, however, reported that data are kept as long as necessary, but it was not always clear to them what this would mean in practice. Furthermore, it was not always found to be clear what happens with the data when they are no longer needed; only some mystery shoppers found that the information clearly stated that the data would be deleted.

Mystery shoppers provided varying feedback about the provision of information on the issue of the data retention after the sale of the car as a second-hand car. According to some, the privacy policy stated that the users should delete their data themselves; others reported that all data are deleted automatically, or, on the contrary, that users must ask the manufacturer to delete the data. In rare cases, mystery shoppers could not find any information about this. According to the GDPR, the company acting as a data controller should delete the personal data when data processing is no longer necessary. From the point of view of the company's duties to inform consumers, the different options reported by shoppers are acceptable, as long as consumers are informed about what they can or cannot expect. However, if this information was indeed (as in some cases) entirely omitted it might be considered an omission of material information, as consumers should feel sufficiently safe about the invisibility, or on the contrary concerned about the visibility, of their data to other users, such as second-hand car purchasers. Moreover, the various reports from shoppers might also indicate that the information was difficult to interpret accurately, which would suggest that more should be done to provide this information in a clear and unambiguous way.

In general, the legal grounds for data processing were found to be mentioned, but mystery shoppers did not find this to have a clear link to the specific types of data processing that are covered by the legal grounds. 'Legitimate interest'

was usually mentioned (but in rare cases it was not found by mystery shoppers). **Where legitimate interest was mentioned, mystery shoppers found that it was not explained in detail what this means.** That said, data that would be collected based on legitimate interest were mentioned. **A statement that some data processing is 'necessary' was also typically identified, but this was assessed to be referred to in rather general terms.** However, when the collection of data is indicated as necessary there should be clear information on the type of data and why they are considered necessary. If this information is not provided, the consumer's rights to exercise control over data processing may be minimised by a general, unjustified 'axiom' that processing is necessary and that the consumer cannot decide on the scope, the purposes or the termination of the processing. The need to process data for the performance of the contract and to meet legal obligations are usually indicated as legal grounds. In general, mystery shoppers considered the explanation of the legal grounds/reasons for data collection clear.

5.1.3. Information on data security

The consumer survey indicated that the security of data processing is by far the most important concern of consumers, and information relating to security may have a significant impact on the consumer's decision on whether or not to purchase a connected car. We indicated that salespeople should spontaneously mention the issue of security, as this includes information about foreseeable risks that are usually considered important. However, **BMW's salespeople did not mention the topic of data security spontaneously**. When the issue was brought up, issues such as protection against hacking and data leaks, and secure access were only occasionally mentioned. Where and how data are stored was mentioned slightly more. The verbal information provided on the different security topics was in general considered sufficiently clear. However, not all mystery shoppers felt well informed about the security of data processing, based on the verbal information received during their visits to the dealer, and some reported that they felt that they were not informed at all, indicating a large variety in the extent and quality of information provided by salespeople.

While several mystery shoppers reported that they could easily find information about security aspects of data processing online, a considerable number stated that they could not find any information on this, or that the information was hidden in unstructured text. Given the importance of this information (and the fact that the provision of verbal information on this topic by salespeople was not always sufficient), this could suggest that, at least in some cases, information may be omitted that may be considered material. On the other hand, **the information that was found by mystery shoppers was in general considered sufficiently clear**. The security topics that were mentioned were mostly complete, except regarding the question of whether all users can see the data of other users. This topic can be considered important, as it involves a direct privacy risk to the users of a car, in particular where sensitive data such as location data can be seen. As a consequence, it can be argued that it should be more clearly covered. Most shoppers, however, did not find information on this topic. We believe that this could potentially be an indication of an omission of information that might be considered material.

Taking into account all verbal, written and online information they could retrieve, **most mystery shoppers felt sufficiently well informed about the security aspects of**

data processing. However, a considerable number of mystery shoppers felt that they were not informed about this aspect at all.

The information on security in the privacy policy was found to be diverse and there were differences between policies in different countries. Some shoppers reported that they found more detailed information in the privacy policy text or in referenced documents, even sometimes including security standards. Most often, however, **shoppers reported having found at most a basic statement that protection of their data was guaranteed**, without further information, or even no information about this aspect at all. Given the important impact that this information might have on the average consumer's decision to purchase a connected car, its absence might be considered an omission of material information. If information was available but not found by shoppers, this still indicates the need to make the information easier to find.

Information on where data are stored (in or outside the car, on servers, in the EU or EEA, etc.) could only rarely be found by the mystery shoppers in the privacy policy.

5.1.4. Consumers' control over data processing

Salespeople usually did not spontaneously provide information about the control that the consumer, as a user of the connected car, can exercise over data processing. When the issue was brought up, not all key topics were mentioned. While the possibility of stopping data collection was usually mentioned, other topics were mentioned less often (e.g. the possibility of deleting or requesting the deletion of collected data and the possibility of having control over the scope of data that are processed or the purposes of processing). Whether all users of the car can see the data of other users was also only occasionally mentioned, although this subject should be mentioned because this potentially constitutes a privacy risk for the consumer.

In general, the verbal information about the possibility of having control over data processing (the scope of the data processed and the purposes of processing, and the possibility of stopping data processing) was considered sufficiently clear. Nevertheless, not all mystery shoppers felt well informed about these issues based on the information they received from salespeople.

With regard to the online information about the control of the user over data processing, the feedback of mystery shoppers was mixed. Most of them found it rather easy to locate the information online, but a considerable number could not find any information about this issue. The information that was found was overall considered to be sufficiently clear, though not always complete. Information on topics such as whether the user can decide on the scope or the purposes of data collection and whether they can request the deletion of data could sometimes be found, but sometimes it could not (more or less in equal parts). In combination with the limited spontaneous verbal information provided, this is not good practice. However, information on the possibility of stopping data collection was generally available.

Taking into account the verbal, written and online information they could retrieve, most mystery shoppers felt sufficiently well informed about the aspects of controlling data processing. However, there was still a considerable number of mystery shoppers who felt insufficiently informed. Given the importance of

these issues for consumers, indicated by the consumers participating in our survey, and the possible impact on their transactional decision, there might be cases where this information could be considered material, and the fact that consumers would feel not well informed might therefore be problematic.

The possibility of disconnecting the car to make data transmission impossible was typically found to be mentioned in the privacy policies. Some shoppers found a detailed explanation of how to do this, but not all of them could locate this information. The possibility of disconnecting and thus stopping data transmission might be regarded as material information because consumers might find it important that they are not locked in against their will. The information is only useful if the consumer can find out how to disconnect their car to stop the data transmission, which may have an impact on their transactional decision. If a user manual explains this, the omission of this practical information would not have an impact. Whether or not the lack of a practical explanation is considered an omission of material information thus depends on the circumstances.

The privacy policies were found to state that the withdrawal of consent for data processing is possible, and mystery shoppers also generally found that the policies explained how the consumer can do this. Furthermore, information was found on the time frames that allow the consumer to withdraw from the contract. The provision of this information in particular is considered good practice by the study team from the point of view of consumer law.

Regarding consumers' rights to access their data, get an overview of the data collected and request that the data be deleted or changed, mystery shoppers' assessments differed. These rights were only sometimes found to be mentioned. Consumers indicated in the survey that receiving information on their rights is very important. The GDPR also requires that consumers be informed about these rights. Therefore, the omission of information on the existence of these rights might also be regarded as an unfair, misleading practice.

Mystery shoppers also provided mixed feedback on the presentation of the information. In some cases, the information was deemed easy to find, in a dedicated section of the document, while others found it difficult to access and buried in other text. This is an additional indication that BMW's practice in this field could sometimes create confusion among mystery shoppers. However, the content of the information provided, if it was found, was in general considered very clear by mystery shoppers.

5.1.5. Data sharing

Salespeople usually did not spontaneously provide information about the subject of the sharing of personal data with third parties. When the topic was brought up by mystery shoppers, salespeople rarely provided information about the possibility of refusing or avoiding data sharing. Regarding information about the recipients of the data, the results were evenly mixed: some dealers provided this information and others did not. Furthermore, the quality of the information about (possible) recipients was uneven: this information was sometimes considered clear and sometimes considered unclear, more or less in equal parts (and the results were similar for other topics related to data sharing). We consider this topic important, and the basics should be sufficiently clear during a visit to a dealer. **Overall, mystery shoppers had**

mixed feelings about being well informed about data sharing after their visits to the dealer.

Information on data sharing was generally easily found in the written materials given during a visit (notably the privacy policy and terms and conditions). This information was also found to be quite clear by mystery shoppers, and the relevant topics were mentioned.

Regarding the ease of finding information online, the feedback from mystery shoppers was mixed. While a considerable number found it rather easy to find the information, several others that could not find any information. In situations where the verbal information provided was insufficient and no additional information could be found online, this might constitute a misleading practice. If the information was available, the mystery shoppers could in general find information about the recipients of the data and the possibility of avoiding (or permitting) data sharing, but information on the possibility of refusing data sharing with specific types of companies was only found occasionally. **The information that was found was in general considered sufficiently clear.** Online information about the possibility of consenting or refusing to share data with third parties and about the recipients of the data must be available and must be sufficiently clear (especially where it is a substitute for verbal information). The omission of information in relation hereto might therefore be considered an unfair, misleading practice.

Shoppers were typically able to find an indication that only anonymised or pseudonymised data are shared. Doing so reduces the manufacturer's obligation to provide information, because the risks to the consumer are minimised. In rare instances, mystery shoppers were not sure whether data are shared in non-anonymised or pseudonymised form. Those shoppers described being provided with a list of the types of entities that receive data, which did not actually mention their names. It was not clear to them whether that list was exhaustive or not. To these shoppers, it was also not clear which data are shared.

Most shoppers described having found a general list of purposes for which the data are shared, but these were not specifically linked to types of data or certain recipients. Commercial or marketing purposes were not found to be mentioned as purposes. Notably, in countries where shoppers found that documentation stated that only anonymised or pseudonymised data are shared, information about the purposes of data sharing was easily found under a specific heading and the text was deemed very clear, whereas, in countries where policies indicated that non-anonymised data could be shared, this information seemed to be more difficult to find, and mystery shoppers deemed the terms used to be more difficult to understand. Therefore, where transparency was more important it was less strictly observed. In accordance with case-law and guidance, when non-anonymised data are shared with third parties the related information on their identity, the scope of the data and the purposes of data sharing should be as clear and specific as possible.

5.1.6. Specific uses of data

Automated decision-making was only sometimes found to be mentioned in privacy policies. When it was mentioned, the policies stated that it would occur only with the consent of the consumer, and the shoppers considered the consequences of

automated decision-making to be appropriately described. Furthermore, the policies **affirmed that the consumer has a right to challenge the automated decision and to ask for a review by a human.**

The use of data for profiling was not found to be mentioned. The use of data for the personalisation of services was only occasionally found to be mentioned. If the latter was found to be mentioned, shoppers reported that it was indicated appropriately that the consent of the consumer would be needed for this.

5.1.7. Changes to the privacy policy or terms and conditions

Only rarely could shoppers find mention of the fact that unilateral changes could be made to the privacy policy. If it was found to be mentioned, there seemed to be a lack of commitment to notify the consumer of such changes, and no opportunity for the consumer to object to the changes. These practices could be considered unfair.

No shoppers reported having found mention in the specific terms and conditions for connected services that BMW would be entitled to unilaterally modify the terms and conditions. This was unusual. The fact that shoppers could not find this information could therefore indicate that it was not clearly provided in an accessible and understandable way.

5.1.8. Exclusion or limitation of liability

In some countries, the shoppers found that the terms and conditions of BMW contained a liability clause, with an exclusion or limitation of liability. Some shoppers reported that it was stated that this limitation of liability would not apply to damage caused by failure to comply with data protection laws (which is the correct practice), but this information could not be found in all countries. Since liability for breaches of data protection legislation cannot be limited or excluded, there might be cases where this would mean that the terms and conditions would obscure the legal rights of consumers.

5.1.9. Termination and lock-in

Shoppers were typically, but not always, able to find a disclaimer that the termination of data processing can have an impact on the usability or quality of certain connected services. Some policies stated that a notification period is necessary to stop the processing when it is based on a contractual agreement; other policies did not appear to contain that information. Privacy policies usually referred to a direct or indirect cost impact when data are no longer collected, processed or shared, but some policies were not found to contain information on this topic.

The possibility of transferring the data to other systems (portability) or obtaining the data was only sometimes found to be mentioned. When it was mentioned, it was often not explained how this can be achieved.

The information on the impact of terminating or refusing data processing was in general regarded by shoppers as somewhat clear, with some unclear phrasings. In general, information on this topic seemed less clear to mystery shoppers than other information provided by BMW.

5.1.10. Software and security updates

Information on software or security updates was not found in the evaluated BMW documentation. It was not clear for how long the consumer can expect to receive such updates. Where this information may have an impact on the consumer's concerns regarding the security of the data, it might be considered material information. Software updates as such may have an impact on the lifespan of the services and should be warranted in accordance with the consumer sales directive (see Chapter 4, item 4.11).

5.1.11. Code of conduct and external supervisory authorities

It was found that BMW referred mostly to an internal code of conduct (without a link to access it). Usually, a reference to an external supervisory authority was not found.

5.1.12. Basic information on contracting

Most shoppers found some description of the assumed acceptance of the specific terms and conditions. An explicit act of acceptance was, however, only found to be mentioned occasionally. This is acceptable if the consumer has an opportunity to read and become acquainted with the terms and conditions before their subscription to the service is activated and they begin to use it. Given the availability of the terms and conditions and the privacy policy on BMW's website, this seems to be the case.

The actions needed to be able to use the connected services seemed to differ depending on the country examined: while some shoppers did not report that a specific action was needed, others reported that it was required to enter into a separate subscription for the services (besides the car sales contract), or to register on a website, to download a mobile application and/or to install a SIM card. All of this information is useful for consumers. It is positive that the connected services are not active by default without a contractual framework.

5.2. Hyundai

5.2.1. Access to information

The salespeople in Hyundai dealerships visited by mystery shoppers rarely talked spontaneously about the connected services of the car. In addition, not all salespeople could confirm that data were processed by the connected car when asked about this, and some contended explicitly that no data were processed. The latter, as all the models/trims in which mystery shoppers showed interest process at least some (personal) data, could possibly be misleading information. Key information concerning security, control over data processing and data sharing was only provided by salespeople when brought up by the shoppers. A substantial number of mystery shoppers stated that salespeople did not give any verbal information at all about connected services and could not refer them to other sources of information, leaving them to find such information themselves online. As a consequence, **mystery shoppers considered the knowledge of salespeople in relation to connected services to be limited**. This suggests that consumers visiting these dealerships run a considerable risk of receiving incorrect or insufficient information about the (possible) processing of personal data. Furthermore, none of the mystery shoppers were given demonstrations of the connected services. Although a dedicated website about Hyundai's connected services is available, salespeople usually did not refer the shoppers to this website for further information.

Some mystery shoppers received a general leaflet about Hyundai car models, or a leaflet about the specific car model, but salespeople did not go through these materials with the shoppers to highlight relevant information. One such leaflet contained **some limited information on security aspects**, but no information about data sharing or about the control that the consumer may have over data processing. None of the leaflets referred to a privacy policy or terms and conditions. Some of the leaflets contained a link to visit the manufacturer's website, but this was not found to be helpful by the mystery shoppers to retrieve additional relevant information about data processing. None of the mystery shoppers received written terms and conditions or a privacy policy.

A dedicated website for Hyundai's connected services is available. As salespeople and leaflets (when these were given) generally did not refer to a specific URL, most mystery shoppers had to try and locate the manufacturer's website or found it through a search engine. When they found the website, most **mystery shoppers could not find any information** on the topics of security, the control that a consumer may have over data processing or data sharing. They could also not identify a privacy policy or terms and conditions document dedicated to Hyundai's connected services. Mystery shoppers could find a general Hyundai privacy policy, although with considerable effort. However, this document did not seem to contain information about data processing through connected services. On some country websites, a leaflet could be found with general information about the possibility of disconnecting the car and deleting and resetting the data.

The above indicates that mystery shoppers could only retrieve very limited verbal, printed or online pre-contractual information about Hyundai's data processing activities in the context of its connected services.

5.2.2. Basic information on connected services and data processing

Most mystery shoppers were unable to find information on Hyundai's website about the topics relating to data processing (the scope of the data processed, the purposes of the processing, who collects the data, with whom the data are shared, etc.). In only a few cases, mystery shoppers reported that terms and conditions mentioned

elements that could possibly have contained information about these topics. However, as in these cases there was no actual link to the terms and conditions, this could not be verified by the study team.

Most mystery shoppers found no information on key topics such as who processes data, what data are processed, the purposes of data processing, data sharing and consumers' control over data. This lack of first-line material information could be considered an infringement of the UCPD. While we cannot rule out that certain information may be made available after the connected car is purchased (e.g. when the consumer downloads an app or sets up the connected services), based on the study team's assessment it seems likely that it is in general difficult to access this information prior to purchasing the car.

5.2.3. Information on data security

Salespeople did not spontaneously provide information about the security aspects of connected services. When the issue of security was brought up by mystery shoppers, the salespeople could typically provide some information, specifically on hacking, data leakage, storage or access protection. Overall, however, mystery shoppers did not find this information to be very clear. One exception was the information on the protection of users' data against disclosure to other users of the car, which mystery shoppers found most of the time, when it was provided, to be clear. In general, most shoppers felt not well informed about data security based on the information they received during their visits to the dealer.

Some mystery shoppers received a leaflet about the car model they wanted to purchase, which contained limited information about security (specifically about hacking).

Most shoppers could not find information on data security on the manufacturer's website, and those who did generally considered the information to be insufficiently clear. Specifically, information on where data are stored was only scarcely provided, although the study team expects that consumers should at least be informed whether their data are stored within the EEA.

Overall, considering all sources of information (verbal information during dealership visits, printed materials and online information), mystery shoppers felt not well informed about security aspects of connected services.

5.2.4. Consumers' control over data processing

Salespeople did not spontaneously provide information to mystery shoppers about the control that the consumer may or may not exercise over data collection or data processing. When the topic of having control was brought up by mystery shoppers, some information was discussed. However, information was lacking on some key topics. Information was particularly lacking on the possibility of deleting personal data (or asking for the data to be deleted), the possibility of deciding which data are processed and the purposes for which data can be processed, and the possibility of stopping data processing.

If information was provided on the possibility of having control over data processing, mystery shoppers overall found this information not very clear, especially when it came to information about the possibility of deciding which data are processed and of stopping data processing. In contrast, information about the possibility of deleting the data and of deciding on the purposes for which data are collected was considered sufficiently clear. However, it must be noted that this concerns only a very small number of mystery shoppers' feedback, as most often this information could not be provided in the first place. As a consequence, most shoppers felt not well informed about the control they can have over data processing based on the information they received during their visits to the dealer.

Only a very small number of shoppers received printed information. In addition, they always only received a general leaflet about the car model, which did not contain any information about the control that the consumer may have over data processing.

Most mystery shoppers were unable to find any online information about the control that a user may have over data processing, and the information they did find was considered very difficult to locate and overall not sufficiently clear. Exceptionally, some shoppers did report that they could find online information about how they could disconnect the car and delete their data.

Overall, considering all sources of information (verbal information, online information and written documents), almost all shoppers reported that they felt not well informed about the control that a user of the connected services may have over data processing.

5.2.5. Data sharing

Salespeople did not spontaneously provide information about data sharing. Moreover, even when the topics were brought up by mystery shoppers, information about the recipients of the data or the possibility of refusing or avoiding data sharing was almost never provided verbally. Furthermore, when such information was mentioned, mystery shoppers considered it not very clear. Almost all shoppers did not feel well informed about the issues of data sharing based on the information received during their dealership visits. This cannot, according to the study team, be regarded as good practice and, depending on the circumstances of a case, may even constitute a misleading practice.

A few mystery shoppers received a leaflet about the car model but did not find information about the sharing of data with third parties in it.

Very few shoppers could find information on the sharing of data online. That said, in the rare cases that they found information they considered it somewhat clear.

Almost none of the shoppers felt well informed about the sharing of data based on the information they received during their dealership visits, or obtained from written documents or online. Given the risks involved and the importance of this material information, the study team cannot rule out that this lack of information may constitute a misleading practice.

5.2.6. Specific uses of data

Mystery shoppers could not find information in relation to profiling, the personalisation of services or automated data processing.

5.2.7. Changes to the privacy policy or terms and conditions

As neither a privacy policy nor terms and conditions were found, mystery shoppers could not find information in relation to what happens if changes are made to the privacy policy and/or terms and conditions.

5.2.8. Exclusion or limitation of liability

As mystery shoppers found neither terms and conditions nor a privacy policy, this aspect could not be evaluated.

5.2.9. Termination and lock-in

No terms and conditions or privacy policy could be found, meaning that this aspect could not be evaluated.

5.2.10. Software and security updates

A website was identified with general information about updates. While no contractual guarantee regarding the provision of software and security updates was found, a statement was found saying that there are 'usually' two updates per year.

5.2.11. Code of conduct and external supervisory authorities

No information could be found.

5.2.12. Basic information on contracting

No information could be found.

5.3. Peugeot

5.3.1. Access to information

Salespeople from the Peugeot dealerships visited by our mystery shoppers did not mention the topic of connected services spontaneously during any of the visits. When the topic was brought up by the mystery shopper, a considerable proportion of salespeople confirmed that personal data were processed. However, it was also relatively common that salespeople were not sure about this or that they stated that no data were collected (which, because all the models/trims in which mystery shoppers showed interest during their visits process some (personal) data, creates a risk of providing misleading information. **Salespeople were generally regarded by the shoppers as not very knowledgeable or not knowledgeable at all about the connected services and/or the data processing happening as part of these services.** Furthermore, salespeople did not demonstrate the connected services during the visits. In addition to this lack of verbal information, mystery shoppers only rarely received printed materials and were only sometimes referred to a dedicated website.

Mystery shoppers were unable to find a dedicated connected services website. Peugeot's website provides general links to terms and conditions and to a privacy policy, but these are not dedicated specifically to connected services. The privacy policy, for instance, does not apply to data processed by the car, and the purposes of the data processing mentioned in the policy are not linked to connected services.

Only with some difficulty could mystery shoppers find a web page on the MyPeugeot app. While this page contained some basic information about the app and referred to a YouTube video, mystery shoppers could find a link neither to a dedicated privacy policy nor to dedicated terms and conditions. Further research revealed that these documents only become accessible to consumers after they subscribe to the connected services and download the app. The app can be downloaded from Google Play and Apple's App Store, and the respective download pages stated explicitly that no information about data safety was available (at least before downloading the app).

During one dealership visit (in France), a mystery shopper received a printed bundle of terms and conditions and privacy policies from the salesperson. Later in the purchasing process, the implied intention seemed to have been that parts of this bundle would be signed as a contract. Some of those documents related to basic connected services (some of which were not available), specifically tele-maintenance services and SOS and assistance services, and a specific privacy policy was provided to the shopper as part of the bundle.

5.3.2. Basic information on connected services and data processing

Overall, mystery shoppers reported that they could find some of the first-line information on data processing online (what data are collected, by whom and for which purposes) and other material information (whether data are shared, whether data are kept secure, whether the user can decide on which data are shared, and with whom and for which purposes the data are shared). Information on the possibility of disconnecting the car (and how this can be done) was also most often found.

The tele-maintenance privacy policy provided in France (see Section 5.3.1) identified the dealer as the data processor and controller for tele-maintenance data; for the SOS and assistance services, Peugeot was identified as the data controller. In the policy, data that are processed and the purposes and the legal grounds of the processing were mentioned in detail, but it was not explicitly indicated that these were exhaustive or that the consumer's consent was required to extend the scope of data processing. Furthermore, the policy was found to describe how some data processing was necessary

for the provision of the services, while other data processing occurred based on consent. It was also found to say that users may exercise control over the processing of those data. However, the description of the data categories that are processed and the purposes of processing (and which category was used for which purpose) were not always clearly understood by the mystery shoppers. The use of location data for the SOS and assistance services was found to be appropriately described.

Mystery shoppers found that the specific tele-maintenance terms and conditions and privacy policy stated that consumers must give their consent for data to be used for direct marketing. However, marketing purposes were not explicitly indicated as purposes in the documents.

In the tele-maintenance privacy policy provided in France, the legal basis of data processing was found to be indicated, although only by referencing the relevant GDPR article, rather than by providing a description of the legal grounds in language that could be understood by a layperson. The data that were considered necessary for the services (and where the control of the consumer is therefore limited) were found to be marked with an asterisk. The study team considers this a good practice, as this is key information for a consumer as far as the impact of the legal grounds goes. The duration for which the data are stored was also found to be indicated in detail in this policy, with several different terms for different data, varying from 6 months to more than 10 years.

5.3.3. Information on data security

Salespeople did not mention the security aspect of connected services spontaneously. When the subject was brought up by mystery shoppers, not all relevant aspects of security (hacking, data leaks, storage of data, secure access to services, etc.) were covered, but mystery shoppers found the information that was provided to be generally rather clear. Nevertheless, most shoppers did not feel well informed about data security after their dealership visits.

Most mystery shoppers could not find online information about the security aspects of connected services, or could find only limited information with great difficulty. Shoppers were able to find only partial information on topics such as protection against hacking, protection against data leaks, where data are stored, protecting access to the services and whether car users can see the data of other users. As information received verbally from salespeople was also limited, it was not at all evident to the study team that shoppers could collect key information, which might in certain cases be considered a general breach of the obligation to provide material information. Furthermore, **the information that mystery shoppers could find was overall not considered very clear**. As a result, most of the shoppers felt that they were not well informed on data security aspects based on verbal and online information. On the whole, this is not an example of good practice and in certain cases might constitute a breach of the obligation to provide consumers with material information.

The specific terms and conditions for tele-maintenance received in France mentioned the fact that users of the service must warn other users of the car that personal data can be disclosed. The fact that users were responsible for the deletion or resetting of their data was also mentioned. The terms and conditions also contained detailed information about the countries to which the information can be transferred. However,

some basic information about the security of the processed data (protection against hacking, data leaks and protected access, etc.) was not provided.

5.3.4. Consumers' control over data processing

The topic of consumers' control over data processing was not mentioned spontaneously by salespeople during dealership visits. When the topic was brought up by mystery shoppers, the salespeople were unable to provide detailed information; they could typically provide information only on some key topics. In particular, the possibility of deciding on the purposes of data processing was never mentioned. A majority of mystery shoppers felt that they were either not well informed or not informed at all about exercising control over data processing after their visits to the dealership.

Most shoppers could not find any information at all about the possibility of controlling which data are processed and how they are used, or could find only some information with great difficulty. Opinions also differed considerably between shoppers on the clarity of information that was found, with shoppers commonly reporting that they found the information insufficiently clear. Most topics were usually only found to be partially mentioned. Information about the possibility of stopping data processing was, however, typically provided. The possibility of exercising control over which data can be processed and for which purposes and whether the user can ask for the data to be deleted were only occasionally mentioned.

In general, based on the verbal and online information mystery shoppers received, most felt that they were not well informed or not informed at all about the possibility of having control over data processing. The study team believes that in some cases this lack of information could be considered an omission of material information.

The specific privacy policy for tele-maintenance provided in France mentioned that consumers have control over which data are processed, except those data necessary for the performance of the tele-maintenance services. It explicitly mentioned that, if a user were to limit the processing of certain data, this might impede the provision of the services. The different rights of the consumer (to access, correct, delete, limit the data processed or object to data processing, to data portability, to object to the use of the data for direct marketing, etc.) were mentioned, although without much detail, and mystery shoppers did not always understand them. The policy also mentioned that consumers could at any time disconnect the service, but did not include information on how to do this.

5.3.5. Data sharing

The topic of the sharing of data with other parties was not spontaneously mentioned by salespeople during mystery shoppers' dealership visits. When mystery shoppers brought up this topic, only some salespeople could provide information about the recipients of the data and/or whether the consumer can object to or avoid data sharing, but often this information was partial and mystery shoppers did

not find it very clear. As a result, **most mystery shoppers felt not well informed or not at all informed about data sharing after their visits to the dealership.**

Most mystery shoppers could not find any online information about the sharing of data. Given that information received verbally from salespeople was also limited, it was not easy for shoppers to collect key information. This might in certain cases result in a breach of the obligation to provide material information. Information about the recipients of users' data and the possibility of avoiding data sharing was found by only some shoppers, and whether the consumer can refuse to share their data was even less frequently mentioned. Mystery shoppers were, however, divided on the clarity of information on these topics.

In general, shoppers felt not well informed about the issue of data sharing based on the verbal and online information they received.

However, the assessment is more positive when it comes to the specific case of the privacy policy for tele-maintenance services obtained in France. This policy did describe the data that were shared, with whom these were shared and for what purpose. Furthermore, mystery shoppers found that the policy indicated that some data were pseudonymised (especially those collected to improve services). The policy did not explicitly indicate that the list of recipients was exhaustive, and it did not state that the list could be extended unilaterally either. In addition, the policy was found to mention that the data is not processed for commercial or marketing purposes. Despite the provision of these details, shoppers sometimes felt that the terminology used was not always easy to understand.

5.3.6. Specific uses of data

Information on the use of data for automated decision-making, profiling or the personalisation of services could not be found.

5.3.7. Changes to the privacy policy or terms and conditions

No information was found about this topic online.

The specific terms and conditions obtained in France for tele-maintenance services mentioned that they can be changed unilaterally. Specific reasons for such changes were also detailed: in order to include regulatory changes, to incorporate more kinds of technical warnings and to reflect the technical developments in the market. However, no information was given on whether consumers would be notified of such changes or whether consumers would have a right to cancel the services in the event of changes. If indeed no such notification or opportunity to cancel the services would be provided, this could, in certain cases, constitute a violation of the UCTD.

5.3.8. Exclusion or limitation of liability

No information was found about this topic online.

The specific terms and conditions concerning tele-maintenance services obtained in France did not contain a clause on a general limitation of liability that would limit the liability for data breaches.

5.3.9. Termination and lock-in

No information was found about this topic online.

The specific terms and conditions concerning tele-maintenance services obtained in France mentioned a minimum contract duration of 3 years from the registration of the car. The consumer can end the contract at any time after that period, with a notice period of 30 days. The right to data portability was also found to be mentioned in the terms and conditions, although this information was difficult to find and the document did not explain what this means in practice (i.e. the right of consumers to obtain their data after termination of the contract). The policy also stated that stopping the processing of certain data that is necessary (indicated with an asterisk) could have an impact on the services, which the study team considers a good practice. However, the cost impact of terminating data processing was not specified.

5.3.10. Software and security updates

No information was found about this topic online.

The specific terms and conditions concerning tele-maintenance services obtained in France do not mention software or security updates explicitly, but, as mentioned above, the service was described as being guaranteed for a period of 3 years from the registration of the vehicle as a new vehicle.

5.3.11. Code of conduct and external supervisory authorities

Mystery shoppers did not find any references to codes of conduct. The specific terms and conditions concerning tele-maintenance services obtained in France referred to supervising authorities, which is a good practice.

5.3.12. Basic information on contracting

No information could be found online about how consumers are bound by the connected services contract. The Peugeot website allows the creation of a connected services account, but there seems to be no opportunity to read the applicable terms and conditions, or privacy policy, prior to subscribing to the services.

The specific terms and conditions concerning tele-maintenance services obtained in France had to be signed as paper documents, which, de facto, made it possible to read these terms and conditions before accepting them.

5.4. Renault

5.4.1. Access to information

Salespeople at Renault dealerships usually did not talk spontaneously about the connected services of a car during dealership visits by the mystery shoppers. When the topic was brought up by the mystery shoppers, salespeople often said that no personal data are collected, which, in the light of the fact that all the models/trims in which mystery shoppers showed interest during their visits process (some) personal data, the study team considers misleading first-line information that may have an impact on the transactional decision of a consumer.

Mystery shoppers generally considered the knowledge of salespeople to be less than satisfactory. Typically, they did not receive much verbal information or written documentation, and were only sometimes referred to a dedicated website. Demonstrations of the connected services occurred only occasionally. In a considerable number of cases the shoppers did not receive any information at all. As the limited verbal communication was in many cases not complemented by referrals to printed or online information, there may have been cases where the obligation to provide material information was not respected.

Renault has a dedicated web page for connected services in several evaluated countries, where a number of diverse connected services were found to be described. **A general, downloadable privacy policy for connected services was also identified, albeit difficult to find** (i.e. at the bottom of the main Renault website home page, in small font). Although the document is intended as a general privacy policy for Renault's services as a whole, it did mention the processing of data in the event that the consumer would have to use connected services (services mentioned were remotely controlling the vehicle, monitoring the battery, controlling the driving mode, etc.). However, more details on data processing were not provided and the policy did not mention specific key topics related to data processing that consumers participating in our survey considered important (such as the security of connected services).

As an exception to this, on the Renault website in France it was possible to find a specific page on data processing in relation to connected services, where the processed data are listed, along with how long they are retained for. Mystery shoppers found this page to be somewhat more specific than the information provided by Renault in the other countries that the study team evaluated, but, according to the study team, it still did not contain much of the information considered material with regard to data processing by connected cars. At the same time, the French website contained a much more visible link to the privacy policy than other countries' websites.

Mystery shoppers could not find specific terms and conditions for connected services online. When registering for the My Renault app, mystery shoppers were able to access terms and conditions for the use of that app. However, this app is only one aspect of Renault's connected services, with limited services. Therefore, the study team considers that these terms and conditions do not cover Renault's connected services in their totality, leaving a considerable amount of information unmentioned.

5.4.2. Basic information on connected services and data processing

National Renault websites and/or privacy policies (if found) contained at least some information on the processing of key data, such as information on who processes which categories of data and for which purposes, data sharing, data security, the extent of control over what data are processed, how the data are used and with whom they are shared, the possibilities of disconnecting the car and deleting stored

data, and contact details. Only in one of the countries covered by this study could the mystery shoppers not find information on the possibility of having control over the purposes of data processing, and the possibilities of disconnecting the car and deleting stored data. This may indicate that there are issues with presenting information in an easily accessible and consistent way across the different countries covered by the study.

The privacy policy identified different (potential) data controllers, including the parent company Renault SAS. In some countries this could also include the national Renault branch and sometimes individual dealerships. However, mystery shoppers did not find it clear whether this list of data controllers was exhaustive. Specific names of the controllers were provided, and mystery shoppers were also able to identify the data protection officer for Renault SAS. The privacy policy was also found to contain a list of the exact data that are processed and an indication that this list would not be extended without the consumer's prior agreement. Appropriately, it also explicitly stated that location data could only be processed with the consent of the user except where another legal ground applied.

The privacy policy contained a detailed list of the purposes of data processing and the related legal grounds, but the mystery shoppers found differences between the policies in different countries, and the structure and accessibility of the documents themselves were found to be rather complex (for instance, shoppers had to click drop-down menus to open text boxes with more information). As a result, some shoppers might have missed some key information. For instance, it was mentioned that data processing could be done for marketing purposes, but because shoppers had to click a link to access this information it was not found by all of them. The same occurred regarding the purpose of profiling, information on which was hidden in a large amount of text and could consequently not be found by some mystery shoppers. Information on the purposes of data processing was typically found but did not seem to be linked to the specific types of data processed.

Furthermore, when it comes to the information that could be found, opinions among the shoppers were divided on whether this information was clear, with some shoppers reporting they found the information sufficiently clear and others mentioning that they did not find this to be the case. This could potentially be linked to the complex presentation of the information, which might not have allowed all shoppers to access and read the information in a sufficient way.

The legal grounds for the different types of data processing were found to be mentioned in the privacy policies. These legal grounds were linked to individual purposes but not in appropriate detail to the types of data, so it was **not clear to mystery shoppers which types of data could be processed on which legal grounds**. Specifically, for instance, 'legitimate interest' was found to be mentioned as a legal ground in relation to specific purposes of processing but not to specific data categories that the ground would cover. Mystery shoppers also did not find this idea to be clearly explained. **Whether the processing of certain data was necessary was also not indicated explicitly**; rather, it was specified implicitly (for instance by mentioning 'the performance of the contract' and 'legal obligations' as legal grounds). This implicit indication was not well understood by mystery shoppers.

The privacy policies stated that the data are retained for as long as necessary, and some indication was found on how to assess this time frame. The data were said to be removed from Renault's systems or anonymised when no longer needed. As the privacy policy did not specifically discuss the storage of data in the car, no reference was made

to the removal of data from the car. Moreover, mystery shoppers did not find information on what Renault or the consumer would or should do with data when no longer using the car or when selling the car.

5.4.3. Information on data security

Salespeople generally did not mention the aspect of security of connected services spontaneously during dealership visits. When the subject was brought up, not all relevant aspects of security (hacking, data leaks, storage of data, secure access to services, etc.) were mentioned, but information that was given was generally considered sufficiently clear. **Nevertheless, most mystery shoppers felt not well informed about the security aspect of connected services after their visits to the dealership.**

Most shoppers either could not find online information about the security aspects or could only find some information with difficulty. Given the limited information received through verbal communication, it was not at all evident that consumers could find additional information. **Furthermore, mystery shoppers overall did not consider the information they found to be very clear**, and they only found information on some of the topics, such as protection against hacking, protection against data leaks, where data are stored and the protection of access to connected services. Information on whether car users can see the data of other users could only be found occasionally.

In general, based on the verbal and online information, shoppers felt not well informed about the security aspects. The study team considers that this could, in some cases, lead to a breach of the obligation to provide consumers with material information.

The privacy policies that were reviewed did not contain detailed information about data security, such as about the hacking of connected services and data leaks. Furthermore, no information could be found about the protection of the data of the car users against disclosure to other users, or what happens to the data when the car is sold as a second-hand car. A positive exception was the fact that the privacy policies did state that some data are transferred outside the EU/EEA, which is relevant and important information to consumers. However, other than this exception, the general statements made about data security could not be considered to have much informative value for consumers wanting to purchase a connected car.

5.4.4. Consumers' control over data processing

Information about consumers' control over data processing was not mentioned spontaneously by salespeople during dealership visits. When the topic was brought up, the salespeople were generally unable to give comprehensive information on the risks and policies involved. For instance, the fact that car users would have the opportunity to decide what data are processed, and for what purposes, was only mentioned by some salespeople. Similarly, the possibilities of stopping data processing or deleting data were almost never mentioned. **As a result, most mystery shoppers**

felt that they were not well informed about their opportunities to exercise control over data processing after their visits to the dealership.

A considerable number of shoppers either could not find information about the possibility of controlling which data are processed and the use thereof online, or could only find some information with great difficulty. However, those that did find information reported that they found it to be generally rather clear. Still, different key topics were usually only partially covered. For instance, information about the possibility of stopping data processing was usually provided, but information on the possibility of exercising control over which data can be processed and for which purposes, and whether the user can request that the data be deleted, was only occasionally provided.

In general, based on the verbal and online information mystery shoppers received, they felt not well informed about the issue of having control over the data processing. In some cases this lack of easy access to information may be considered an omission of material information.

In the privacy policy, mystery shoppers were generally able to find key information about the rights of the consumer to access, delete or correct their data and to withdraw their consent for data processing. The right to data portability was also typically found to be mentioned but not always understood. Only one shopper was able to find information in the privacy policy about the possibility of disconnecting the car. The impact of terminating data processing on the functioning of the car was rather implicitly indicated, in a section where the purposes of data processing was set out, and not explicitly stated. Not all mystery shoppers found this element easy to understand, indicating that the clarity of the information could be improved. A mention of any direct or indirect costs of the termination of data processing was also not found.

5.4.5. Data sharing

Information about the sharing of data with third parties was not spontaneously mentioned by salespeople during dealership visits. Even when the topic was brought up by the mystery shoppers, they were not able to provide information about the recipients of the data, or whether or not consumers can object to or avoid data sharing. **Most mystery shoppers felt that they were not well informed after their dealership visits about the issue of data sharing.**

A considerable number of shoppers could not find any information about the sharing of data online, or could only find this information with great difficulty. Given the limited provision of verbal information during dealership visits, the difficulty in finding additional information online might cause issues for consumers in accessing key information, and consumers might conclude that this information is simply not provided. **Furthermore, shoppers had mixed opinions about the clarity of the information that was found**: about equal numbers of shoppers found the information either rather clear or rather unclear. Information on the different key topics related to data sharing was not always found. Specifically, while information about the recipients of the data seemed to be readily available, information on the possibility of refusing or avoiding data sharing was found less often.

In general, shoppers felt not well informed about the issue of data sharing based on the verbal information they received and information they received online. The study team considers that this could be perceived as material information not being available to consumers in some cases.

Shoppers' assessments of privacy policies differed between countries in terms of what information could be found about data sharing. In general, however, the information was not provided under a very clear heading, making the **identification of the information by mystery shoppers more difficult**. The policies referred most often to the sharing of data with broad categories of service providers and companies, such as financing companies, without naming individual companies. In Spain and France, it was reported that the policy stated that data can be shared with other 'partners' 'for their own purposes', without any further explanation. However, it was stated that the consent of the consumer would be required for such sharing to occur. The privacy policies were also found to state that data can be shared with service providers 'for the dispatch of commercial offers', but it was not clear whether this referred to marketing on behalf of Renault only or whether this could include marketing by third parties (e.g. through brokers). **Perhaps as a consequence of this lack of concrete detail, the mystery shoppers differed in their interpretations of this information.** It was not clear whether only anonymised or pseudonymised data would be transferred. In summary, these findings indicate that the information on data sharing was not entirely unambiguous for an average consumer, creating a risk that important information might not be understood or found, even when searched for explicitly.

5.4.6. Specific uses of data

Information about automated decision-making was not found in the privacy policies. Profiling and the personalisation of services were found to be mentioned, but were hidden in text that was difficult to navigate. Mystery shoppers, however, typically did find it clearly explained that the consumer must give their consent to the use of their data for profiling and personalisation.

5.4.7. Changes to the privacy policy or terms and conditions

The privacy policies stated that changes were possible and that Renault would either notify consumers of changes (meaning that unilateral changes were possible) or ask them to agree to changes. Mystery shoppers often found this to be ambiguously stated, as it was not clear in what cases consumers would be given the rights to object to changes and to terminate the agreement if they did not agree to any changes.

5.4.8. Exclusion or limitation of liability

Mystery shoppers could not find clauses dealing with liability.

5.4.9. Termination and lock-in

The privacy policies indicated, although in rather implicit wording, that the termination of certain aspects of data processing may have an impact on the usability of the car. Not all mystery shoppers understood the implications of the information in the way it was provided. Direct or indirect costs of such termination were not explicitly indicated.

Data portability was indicated as a right of the consumer, but the meaning was not always understood. This leaves room for consumers to misinterpret the options for portability and therefore they might not make full use of the options available to them.

5.4.10. Software and security updates

Some information on software updates and how to install them could be found by the mystery shoppers, but they could not identify a notification of a binding guarantee in relation to the duration for which updates will be available (which should cover a minimum period of 2 years).

5.4.11. Code of conduct and external supervisory authorities

An internal code of conduct was found to be mentioned. Furthermore, a referral was found to a supervising authority in France (the French privacy authority Commission Nationale de l'Informatique et des Libertés).

5.4.12. Basic information on contracting

The Renault connected services in totality seemed to cover a combination of different, services and applications. However, **in terms of contracts for these services it was not clear how a consumer would be bound by an agreement to any or all of these services/applications**. For instance, if a consumer was to register to use the My Renault online service, they would have to indicate that they had read the terms and conditions, which can be read before registering, and would therefore be deemed to have accepted them. However, these terms only partially cover the connected car services (although this was not clear to all mystery shoppers). Therefore, in general mystery shoppers did not find it clear how an agreement was established in order to provide the connected services. Moreover, shoppers did not find information on whether consumers can withdraw from the contract.

5.5. Tesla

5.5.1. Access to information

During dealership visits by the mystery shoppers, salespeople usually did not talk spontaneously about connected services, and they never spontaneously mentioned security, data sharing or the issue of having control over the data processing related to these connected services. When the subject was brought up by the mystery shoppers, most salespeople said that data are collected. However, a considerable number of salespeople either were not sure about this or said that no data are collected (which, because all the models/trims that mystery shoppers showed interest in during the dealership visits process at least some (personal) data, the study team considers potentially misleading for consumers). Salespeople who were able to give information did so mostly verbally or by referring to Tesla's website, but never through written documents. The connected services were also demonstrated occasionally. However, a considerable number of salespeople could not give basic information in any form. As a result, mystery shoppers found **salespeople overall not to be very knowledgeable about Tesla's connected services**. **Still, most mystery shoppers after their dealership visits felt at least somewhat informed about data security and the possibility of having control over data processing**, but less so about the issue of data sharing.

However, the lack of verbal information provided during dealership visits could be compensated for to a large extent by the information shoppers were able to find online. Shoppers usually received a specific URL for Tesla's dedicated website from salespeople, and most shoppers found key information about the connected services on that website (for instance, in relation to security issues or control over data processing). Not all mystery shoppers were able to find this information with the same ease. **Most shoppers were able to find a specific connected services privacy policy and specific terms and conditions**, which were available through a link on the website (though the privacy policy could not be downloaded).

5.5.2. Basic information on connected services and data processing

Mystery shoppers were typically able to find key information about what data are processed and by whom, the purposes of data processing, whether data are shared with third parties, how data are secured, whether and how users can see and decide what data are processed, whether users can disconnect the car completely and whom users can contact if they have further questions or complaints. They usually found this information in the privacy policy document available online, and in some cases directly in the text on Tesla's website. **Shoppers found the information to be quite detailed**, although there were some differences in this feedback between countries.

Based on the information that was found by the mystery shoppers, it does not appear that Tesla provides very clear information on **who** processes the data. The information found stated that 'different companies' can do this, usually without further explanation. While Tesla was found to provide a list of types of companies that may process data, this was understood not to be an exhaustive list. The list also contained no specific names or contact details, or details for contacting the relevant data protection officer. In general, the list was not always found to be easy to understand. Overall, it appears that **Tesla was insufficiently clear on the topic of who processes data**. Similarly, mystery shoppers also reported that it was not clear what other companies are involved in the **provision** of the connected services (some of which may also act as data processors).

In the documents available online, mystery shoppers could find information about what data are processed but could not find confirmation that the list was

exhaustive. **Assessments differed regarding the clarity of this information**: some shoppers found the information very clear, while others found some parts of the text rather difficult to understand. In general, shoppers indicated that they were able to find information on **how** data are processed. Specifically regarding the processing of location data, they found that Tesla indicated that this was only done with the consent of the consumer, which the study team considers to be the correct practice.

Most often, detailed information on the purposes of the data processing was found, linked to the data that were covered by the purposes mentioned. Again, however, this information was **not always clearly understood** by the mystery shoppers.

Some shoppers found that the information available mentioned that data can be used for marketing/commercial purposes or can be shared for these purposes. **Most mystery shoppers were, however, unable to locate this information**, and where it was found it was typically not well understood. If data are processed for commercial purposes but information on this is indeed not provided or is very difficult to locate, this might constitute an unfair, misleading practice.

Mystery shoppers' assessments varied with regard to the availability of an indication of the legal grounds for data processing. Some reported that the legal basis was provided and well linked to the types of data that are covered by the purposes, but several shoppers were not able to find such information. As it is unlikely that there would be such a variety between privacy policies in different countries, this variety in the shoppers' assessments could be a result of differing interpretations of the information provided, or an indication that information was difficult to find, leading some shoppers to overlook it. Either way, it does indicate a difficulty in consistently finding and/or correctly interpreting the information provided.

Some shoppers found that legitimate interest was mentioned as a legal ground, and where they found this they were typically also able to identify the types of data to which this applied. However, an explanation of the concept of legitimate interest was not always found. Shoppers also often found that the available information stated that data could be collected because it was **necessary** to collect certain data for the performance of the contract or to meet legal obligations, or to protect the vital interests of the consumer. In general, this information was found to be at least somewhat clear, although some mystery shoppers reported having difficulty understanding certain technical terms.

Some shoppers found an indication that certain data are only processed with the consumer's consent. This applied, for instance, to location data. However, where data processing based on consent was found to be discussed, shoppers did not always clearly understand when and how the consumer is expected to give consent. While shoppers were typically able to find confirmation that the consumer can withdraw their consent, they could not find information on how this can be done in all countries covered by the study.

Mystery shoppers' evaluations also varied when it came to information on the deletion of unnecessary/excessive data. Overall, mystery shoppers found that it was **not entirely clear what happens when data are no longer needed**. Some shoppers reported that they found information stating that data are kept for 'as long as necessary' but could not find an explanation about what this means. Others found that this was explained. Information on how long data are kept for or when they are deleted

was also not always found. Similarly, some shoppers reported that the information they found stated that consumers must delete any personal data themselves when the car is sold as a second-hand car or when it is returned to a leasing company, while others said they could not find any information on this.

5.5.3. Information on data security

Salespeople never provided spontaneous information about security aspects during mystery shoppers' dealership visits. When the topic was brought up by the mystery shoppers, not all key aspects of the topic were discussed. Specifically, information about the risks of hacking was typically not provided, although when information was provided shoppers found it overall sufficiently clear. Nevertheless, in general **shoppers did not feel well informed about data security aspects based on the information received during their visits to the dealership.**

Shoppers were often referred to a website for information on data security, usually with a specific URL, which the study team considers good practice. Most shoppers also found information on Tesla's website with relative ease, and they tended to find the information provided very clear. Detailed information on where and how data are stored was often found, but **information on the possibility that personal data of users of the car could be seen by other users of the car seemed to be missing** (and not very clear). The latter topic is an important concern and should be explained more extensively. In addition, not all shoppers could find detailed information on security-related topics such as hacking, data leaks or theft, and secure access to services. Still, **considering information received during mystery shoppers' dealership visits and online information, overall they felt that they were well informed about data security.**

Most mystery shoppers found that the information available stated that the data cannot be completely secured from cyberattacks or cybertheft. This is good practice, as it warns the consumer about the risks involved in connected services. However, the study team believes that legal implications may be linked to such a statement, if it is used to limit the manufacturer's liability if a security breach occurs. But, given this, it is considered fair and appropriate to warn consumers that risks to data security, in particular resulting from illegal conduct, cannot be fully eliminated, even when all appropriate means of protection are applied.

Some shoppers found detailed information about the security protection techniques applied. Others, however, reported that they could only find a general statement describing the presence of such protection without further details. No references to specific security standards were found.

Most shoppers reported that they found a general statement on where or in which country/continent data are stored. It was, however, not always clear to shoppers whether data are stored outside the car.

5.5.4. Consumers' control over data processing

Salespeople did not spontaneously provide information about the control that users can have over data processing during dealership visits. When the topic was brought up by the mystery shoppers, **salespeople were only able to offer limited information** on the possibility of having control over data processing, the scope of the data, the purpose of data processing, and the possibility of consumers asking for the processing of their data to be stopped or for their data to be deleted. However, when information was given, it was overall considered sufficiently clear by the mystery shoppers, except in relation to the possibility of controlling the purposes of data processing. **In general, shoppers did not feel well informed about the control they could have over data processing based on the information they received during their visits to the dealership.**

Shoppers did find mostly complete information online about the possibility of controlling data processing. This information was considered at least rather clear, although some shoppers indicated that they faced difficulties in finding the information because it was included in a larger body of text and not clearly indicated. In any case, Tesla seemed to perform very well compared with other manufacturers as far as online information on the topic of consumers' control over data processing is concerned. Probably as a result of this, **mystery shoppers in general felt well informed based on the information they retrieved from dealership visits and online**.

Most mystery shoppers received or found at least some information about consumers' rights to obtain an overview of their data, access their data, or have their data deleted or changed. If these rights are not clearly guaranteed, this may constitute an omission of material information under Article 7 UCPD and an unfair practice under Article 3(1) UCTD, as it would mean that the rights of consumers are being obscured.

Some shoppers found clear information on how consumers can disconnect their car to stop data processing. However, most others were unable to find such information and could not, based on the information they found, say for sure whether such disconnection would actually be possible. The possibility of transferring data to another system (portability) was often but not always mentioned. This might again constitute an omission of material information.

The possibility of withdrawing consent for the processing of certain data was typically mentioned, although it was not always clear to shoppers how this could be done.

5.5.5. Data sharing

Salespeople did not spontaneously provide information about the topic of sharing data with third parties. When the topic was brought up by mystery shoppers, most often salespeople were unable to provide clear information on data sharing (such as the recipients of data and the possibility of objecting to data sharing). In the rare cases where any information was provided about the recipients of the data, mystery shoppers found this information to be rather unclear. **A vast majority of shoppers felt not well informed about data sharing after their dealership visits.**

Shoppers could overall easily find online information related to data sharing, and this information was also generally considered clear. In the study team's view, Tesla outperforms other manufacturers in this respect. Considering all sources of information, most shoppers felt sufficiently informed, and a considerable number of visitors felt very well informed about data sharing, although they tended to feel somewhat less informed about this topic than the topics of data control and data security (see Sections 5.5.3 and 5.5.4).

The connected services privacy policy was found to contain information about the fact that data can be shared with third parties. Information about data sharing was found easily, in a dedicated section of the policy. Shoppers typically found the information to be sufficiently clear, although some found parts of it difficult to understand. Information about whether data are anonymised or pseudonymised before sharing was only rarely found. When data are transferred in a non-anonymised or non-pseudonymised way, the manufacturer's information obligations are strict. Therefore, the privacy policies that do not mention anonymisation or pseudonymisation must observe strict information obligations. The privacy policy was found to mention categories of recipients but did not name the specific parties in these categories (which is not best practice). The policy duly mentioned that the list of parties with which data are shared can be extended, but only with the consent of the consumer. In addition, shoppers did not always find it clear which data are shared. However, the purposes of data sharing were mentioned, sometimes clearly linked to specific categories of parties with whom data could be shared but sometimes only in general without linking to specific categories. Most shoppers found mention of the fact that data can be shared for commercial or marketing purposes. The policy was also found to state that data sharing for marketing or commercial purposes would only be done with the consumer's consent, which is the correct practice.

5.5.6. Specific uses of data

Most shoppers could only find an indication that the use of data for the personalisation of services may occur. In addition, some found that the consent of the consumer is required. Consumers have the right to know that their consent is needed for personalisation practices. This is material information about the rights of the consumer, so, regardless of whether the information is indeed missing in some countries or whether it was not always easy to find, further steps could be taken to increase the accessibility of this information.

5.5.7. Changes to the privacy policy or terms and conditions

Shoppers' feedback varied when it came to the provision of information on changes to the privacy policy for connected services. Some found a concrete list of changes that can be made (which the study team considers a good practice), but others reported that they only found a general statement that Tesla can make unilateral changes to the privacy policy without specifying the changes, or that they could not find any information at all. If unilateral changes are not mentioned, the rights of the consumer seem protected, as this implies that such changes would never take place. However, the study team finds it hard to believe that in practice changes would not be made unilaterally during the life cycle of the services. The study team therefore believes

that the lack of indication about unilateral changes might be an omission of material information, if it is indeed missing, and that at the very least this information should be more clearly indicated to consumers.

Shoppers' feedback also varied when it came to information about the notification that would be given about such unilateral changes. Some shoppers reported that they could find detailed information on this, including an indication that notification would be provided within a specific time frame. Others, however, could not find information on the time frame. Again, on the likely assumption that this does not reflect the real variety between different policies in individual countries, the study team believes that the variation in reports from shoppers indicates a need for clearer and more accessible information on this topic.

Only rarely did shoppers find a statement providing that a consumer may object to changes to the privacy policy (in specific circumstances). Statements to the effect that the consumer could withdraw from the services if they disagreed with changes were not found. Therefore, it seems to the study team that Tesla is not sufficiently clear about the rights of the consumer in this respect: it should be clearer that consumers may object to changes that have a negative impact on the services or their contractual rights, and that they can terminate the contract in such a case (UCTD annex, point 1(j)).

No information on the possibility of changing specific terms and conditions unilaterally was found.

5.5.8. Exclusion or limitation of liability

Information about the manufacturer's liability was not found in the specific terms and conditions.

5.5.9. Termination and lock-in

Most shoppers could not find information on the fact that objecting to or stopping the collection of certain data could affect the usability or quality of certain connected services. However, some shoppers reported that they did find information on this and/or that objecting to or stopping data collection may have an indirect cost impact for the consumer ([125]). A statement that a waiting or notice period would apply when the user wants to stop data processing was also not found.

Shoppers' assessments of the availability of information varied regarding the opportunity for the consumer to obtain the processed data after data processing

([125]) While Tesla does not provide an explicit warning that stopping data collection could have an indirect cost impact, some shoppers found this message to be implicitly present in the information provided by Tesla. Tesla states that it is as much a software company as it is a car manufacturer, and that it optimises the driving of its cars with big data and artificial intelligence, including an optimised autopilot feature. Furthermore, the optimisation of the energy use of the car is said to rely heavily on collected data. Some shoppers reasoned that the advantages of artificial intelligence would be lost if such services were terminated, creating a higher cost.

terminates. Some shoppers found that it was clearly mentioned as a right, and that the information explained how the user can do this. Others, however, reported that no information could be found on returning data to consumers.

In general, shoppers found the information about the impact of stopping data processing somewhat clear, although they considered some parts difficult to understand.

5.5.10. Software and security updates

Most shoppers reported that they did not find it clear how long a consumer would receive software and security updates to the connected services for. Some, however, could find some information, for instance stating that there is only a guarantee for paid updates. The study team believes that a failure to provide information on this (or to make it clearly and easily accessible to all) might breach the obligation to provide material information or the requirement to act with professional diligence under Articles 7 and 5 UCPD, respectively, and Article 5(1)(g) CRD and the sales of goods directive.

5.5.11. Code of conduct and external supervisory authorities

Some shoppers found a reference to an internal code of conduct, but a link to a specific document was not provided. No external code of conduct was found to be mentioned in any of the audits. However, in some of the countries covered by the study a reference to the Dutch supervisory data protection authority was found in the privacy policy.

5.5.12. Basic information on contracting

There are specific terms and conditions for the connected services, but it was generally not clear how consumers are deemed to have accepted these, how they are bound by any agreement regarding connected services (apart from an agreement to purchase the car) or whether they can withdraw from the agreement.

5.6. Toyota

5.6.1. Access to information

Toyota salespeople rarely talked spontaneously to mystery shoppers about the connected services of the car during dealership visits. When the subject was mentioned by the mystery shoppers, most salespeople said that personal data are collected. Some, however, explicitly reported that this was not the case (which, because all the models/trims in which mystery shoppers showed interest during their dealership visits process (some) personal data, the study team considers potentially misleading information) or that they were not sure about this. The connected services were rarely demonstrated to the shoppers.

Mystery shoppers' assessments of the knowledge of the salespeople about connected services varied, about equally divided between positive and negative. Nevertheless, based on the feedback provided by mystery shoppers, the study team considers Toyota among the better-performing manufacturers in this respect. Furthermore, **while information was only rarely provided spontaneously, Toyota salespeople did so considerably more often than other manufacturers when it came to information about data security and exercising control over data processing**, the two topics that were regarded as most important to consumers during the consumer survey. Information on data sharing was less frequently provided.

The information that was provided by salespeople was mainly verbal, with occasional referrals to a website. Written documentation (e.g. a leaflet) was rarely provided, and did not contain information on the main topics of security, controlling data processing and data sharing. In addition, the documents did not contain a reference to a website, privacy policy or terms and conditions.

Online information was found to be limited. Some details on the practical use of the services could be identified, but only limited details were found on other aspects of information that are considered to be important or material when it comes to data processing in connected services. **Neither the mystery shoppers nor the project research team were able to find a specific privacy policy or specific terms and conditions for the connected services in the countries covered by the study.**

5.6.2. Basic information on connected services and data processing

Most mystery shoppers could retrieve at least some information on who collects which kind of data and for which purposes, data sharing, data security, the extent of consumers' control over the processed data and over the use and the sharing thereof, the possibility of disconnecting the car and deleting stored data, and contact details.

5.6.3. Information on data security

Salespeople did not often mention the aspect of security of connected services spontaneously during the dealership visits, although Toyota still performed better than other manufacturers in this respect. When the subject was brought up by mystery shoppers, not all relevant aspects of security (hacking, data leaks, the storage of data and secure access to services) were mentioned. Notably, information on the storage of data was only rarely provided. However, if information was received from salespeople on security, it was generally perceived by mystery shoppers as sufficiently clear. In addition, a leaflet that a few shoppers received did not contain information on security. In summary, most mystery shoppers felt not well informed on the topic of security after their dealership visits.

Not all mystery shoppers were equally successful in finding online information on data security aspects of connected services, and a considerable number of shoppers could not find such information. However, those who could find information found that it was in general sufficiently clear. **Taking together both the verbal information from salespeople and the online information that could be found (if any), only some shoppers felt sufficiently informed.**

5.6.4. Consumers' control over data processing

Salespeople did not often spontaneously mention the topic of control over data processing during the dealership visits. Nevertheless, the study team considers that Toyota performed better than other manufacturers in this respect. When the subject was brought up by mystery shoppers, not all key aspects were discussed. Specifically, information regarding the possibility of stopping data processing, deleting the data or limiting the purposes of the processing was rarely mentioned. Information on the possibility of limiting the data that are processed, and in particular the possibility of keeping the data of car users secure from other users, was provided more often. **If information was received, it was also not always found to be clear.** In particular, information about whether the user can limit the scope of the data that are processed was found to be rather unclear. Information on the possibility of stopping data processing and deleting the data was considered somewhat clearer, although it was still reported as unclear by many shoppers. Information on the possibility of limiting the purposes of data processing was considered sufficiently clear. A leaflet that a few shoppers received during their dealership visits did not contain information on the topic of controlling data processing. **All in all, a clear majority of the shoppers felt not well informed about the topic of controlling data collection after their visits to the dealership.**

Most mystery shoppers either could not find any information online about controlling data processing or could only find it with great difficulty. The information that was retrieved was found to be rather unclear by most mystery shoppers. Overall, taking together verbal and online information, most mystery shoppers felt not well informed about the topic of controlling data processing, with a considerable group feeling not at all informed.

5.6.5. Data sharing

Salespeople rarely mentioned the subject of data sharing spontaneously during dealership visits. When this topic was brought up by mystery shoppers, the information provided (if any) was not always found to be clear, specifically when it came to the recipients of the data, and the possibility of objecting to or avoiding data sharing. A leaflet that a few shoppers received during their dealership visits did not contain information on data sharing. All in all, a clear majority of the shoppers felt not well informed about the topic of data sharing after their visits to the dealership.

A majority of shoppers reported that they either could not find online information on data sharing or could find only some information with great difficulty, although the information that they did find was typically regarded as rather clear. Information on the companies that data are shared with was rare. Other topics,

such as whether a consumer can avoid or object to data sharing, were better covered. **Overall, taking together verbal and online information, a majority of shoppers felt not well informed about the topic of data sharing.**

5.6.6. Specific uses of data

Mystery shoppers were asked to search for information about profiling, the personalisation of services and automatic decision-making in the privacy policy. However, as a specific privacy policy could not be identified, no such assessment could be made.

5.6.7. Changes to the privacy policy or terms and conditions

As no dedicated connected services privacy policy or specific terms and conditions for connected services could be identified in the countries covered by the study, the possibility of changing the provisions of such documents could not be assessed.

5.6.8. Exclusion or limitation of liability

As terms and conditions could not be identified, this issue could not be assessed.

5.6.9. Termination and lock-in

As a privacy policy could not be identified, this issue could not be assessed.

5.6.10. Software and security updates

No guarantee could be found concerning software or security updates.

5.6.11. Code of conduct and external supervisory authorities

Mystery shoppers could not find information on a code of conduct, or supervising authorities.

5.6.12. Basic information on contracting

Mystery shoppers could not find information on how the contract concerning connected services is concluded. An app used for the connected services can be downloaded on

Google Play or Apple’s App Store, but no terms and conditions are clearly visible before downloading.

5.7. Volkswagen

5.7.1. Access to information

During mystery shoppers' dealership visits, the salespeople for Volkswagen usually did not mention the connected services of a car spontaneously. The key topics of security, exercising control over data processing and data sharing were only very rarely mentioned spontaneously. When the topics of connected services and data processing were brought up by the mystery shoppers, salespeople typically did confirm that personal data are collected, although a considerable number of them stated that this was not the case (which, because all the models/trims in which mystery shoppers showed interest during their dealership visits process some (personal) data, the study team considers potentially misleading information), or that they were not sure about this.

On all visits, salespeople could at least provide some information on the connected services and related data processing. This was done most often verbally, although a number of salespeople also referred mystery shoppers to a website. According to the mystery shoppers, most salespeople were at least somewhat knowledgeable about connected services. Volkswagen is one of the best performers among the manufacturers studied in this respect. Demonstrations of the connected services were, however, rare. Printed documentation was provided occasionally (in particular, a leaflet and a registration document for connected services with terms and conditions). The printed documentation contained some detailed information about data processing (the scope of processed data, the purposes of data collection, the data controller, data sharing, the disconnection of connected services and contact details) but did not provide information about data security and control. The documents also contained links to specific terms and conditions and a specific privacy policy.

A connected services website is available, with links to a downloadable privacy policy for connected services and specific terms and conditions. Some detailed information on certain aspects of the connected services is available through links on the website.

5.7.2. Basic information on connected services and data processing

In general, mystery shoppers were able to find key information on the scope of processed data, who collects these data, the purpose of the processing, the sharing of data with third parties, the security of the data, the possibility of limiting the scope of the data collected, the recipients and the use of the data, the possibilities of disconnecting the car and deleting stored data, and contact details.

In the connected services privacy policy, the names of the companies that collect and process the data were clearly provided and easy to locate in the text. Most shoppers found that the privacy policy clearly stated that the list was exhaustive. Similarly, most shoppers reported that the contact details of the data protection officer were given for all companies involved in data processing. The terminology used in these descriptions was overall considered clear, with only a few phrasings that were difficult to understand.

In the privacy policy, a detailed list could be found of the data types that are processed, and the descriptions of the data types were overall found to be clear. However, this list is embedded in an extensive policy, which sometimes made it difficult for shoppers to locate. Some shoppers failed to properly locate and/or understand the information. Whether or not the list was exhaustive was also not always clear to mystery shoppers.

Mystery shoppers could find an indication that location data could only be collected with the consent of the consumer, although exceptions were also listed (for instance, in the

case of urgent SOS services). The available information also stated that biometric data could be processed with the consent of the consumer, which the study team considers a good practice. Volkswagen is one of the few manufacturers that point this out.

Mystery shoppers found information on the purposes of data collection to be rather general but overall clearly explained. Purposes were found to be not systematically linked to specific types of data. Marketing and commercial purposes were generally found to be mentioned, but not all mystery shoppers found that they were well explained.

The legal ground of data processing was found to be indicated for each type of data. 'Legitimate interest' was identified as a legal ground, but most mystery shoppers found that the concept was not well explained (leading one shopper to assume that legitimate interest was not mentioned at all in the privacy policy). Assessments of the provision of information on the need to process any data as a legal ground were more varied. Some shoppers reported that it was mentioned and clearly explained, while others were unable to find any information. This indicates at least a lack of easy access to information about the topic and a lack of clarity, as confirmed by the fact that several shoppers said that they did not find the information provided to be very clear.

Most shoppers found that the privacy policy mentioned that data are kept for 'as long as necessary', but not all of them found this idea to be clearly explained. That said, they did typically report that the policy stated clearly that data are deleted when no longer needed. Information about what happens to the data if the car is sold as a second-hand car (specifically, users must delete the data themselves) seemed more difficult to locate, as only one shopper was able to find this information.

5.7.3. Information on data security

During mystery shoppers' dealership visits, salespeople almost never talked spontaneously about data security issues. When the subject was brought up, they mainly talked about the storage of data and occasionally spoke about protection against data leaks and secure access to services, but very rarely mentioned car or software hacking or the protection of users' data against disclosure to other users. **Notably, shoppers found the verbal information they received about protection against hacking to be generally unclear.** In contrast, the information provided about protection against data leaks or theft, where and how data are stored, and secure access to services was usually found to be rather clear. **All in all, most mystery shoppers indicated that they felt at least somewhat informed about security after their dealership visits.** Still, a considerable minority of mystery shoppers reported that they felt not well informed.

Mystery shoppers could find information about the security aspects of the connected services online with varying degrees of success. While several of them could find this information easily, most shoppers either could not find the information or could only find it with great difficulty. Most shoppers who were able to find the information felt that it was at least somewhat clear. Information on where and how data are stored was most prevalent. Information about secure access to the services and how data are protected against data leaks or theft was found less often. Information about car or software hacking and about the protection of the data against disclosure to other users of the car was least often provided, which the study team observed is a

similar trend to those seen for most other manufacturers. Still, it is noteworthy that a considerable number of shoppers found no information about these topics, which the study team considers important in the context of security.

Overall, taking together all the verbal, printed and online information that was available to them, mystery shoppers were divided on the question of whether they felt well informed about the issue of security, with the number who felt well informed and the number who did not feel well informed roughly equal.

Mystery shoppers could typically find some information about security in the connected services privacy policy. This information was indicated with a clear heading, although additional information was found elsewhere in the text and was therefore more difficult to find. Also notable is that the information seemed to be divided over two separate policy documents, and the extent and detail of that information and the protection techniques and security standards included vary between these documents. For instance, the places where data are stored are explained in detail in only one of these documents.

5.7.4. Consumers' control over data processing

Salespeople rarely spontaneously provided information about the possibility of exercising control over data processing during dealership visits. When the subject was brought up by mystery shoppers, topics such as the possibilities of limiting the scope of the data processed, stopping data processing and deleting the data were addressed in some cases, whereas the possibility of deciding on the use of the data were mentioned only rarely (which, however, is a finding common to almost all the manufacturers studied). **Mystery shoppers also had mixed opinions about the clarity of this information.** Information about stopping data collection was generally found to be clear. This was, however, less often the case for information on limiting the scope of the data collection and the possibility of deleting data, and information about the possibility of limiting the use of the data. Possibly as a consequence, **most mystery shoppers felt that they were not well informed about the possibilities of exercising control over data processing after their dealership visits.**

The few mystery shoppers who received written documentation from salespeople found it easy overall to retrieve information about controlling data processing in that documentation, although not all of them managed to do so. The information found was mostly considered to be very clear.

A considerable number of mystery shoppers could not find any online information about controlling the data processing. However, the information that was found was generally considered to be clear. Information on the possibility of stopping data processing and deleting the data was usually mentioned. In contrast, information on whether a user can decide on the scope of the collected data and, in particular, on the use of the data was only rarely found.

Overall, taking into account all the verbal, printed and online information that was available, mystery shoppers were divided on whether they felt well informed about the issue of having control over data processing, with equal numbers feeling well informed and not well informed.

The privacy policy was found to mention that the car can be disconnected, and how this can be done. Shoppers also found that a consumer can withdraw their consent to the collection of certain data, and that the privacy policy explained how to do this. The rights of the consumer to obtain access to the collected data, to gain an overview of the data and to delete/change the data were generally found in the reviewed privacy policies (with a few exceptions). **Shoppers reported that they found that information about controlling data processing was clearly indicated in the policy**, although not in a separate section. The language was considered clear, with a few exceptional phrasings that some found difficult to understand.

5.7.5. Data sharing

Salespeople almost never mentioned the topics of data sharing spontaneously during dealership visits. When the subject of data sharing was brought up, the important topics, such as the recipients of the data and the possibility of objecting to or avoiding data sharing, were very rarely mentioned. In the few cases where information was given about who receives the data and the possibility of avoiding data sharing, the shoppers had mixed views on the clarity of that information. Information on the possibility of objecting to data sharing, if provided, was generally found to not be very clear. As a result, a clear majority of mystery shoppers felt not well informed about the issue of data sharing after their visits to the dealer.

A considerable number of shoppers found no information at all online about the issue of data sharing. Overall, the group of shoppers who found it rather easy to find the information was about equal in size to the group who found no information at all or found information with great difficulty. However, the information that was found was in general considered clear. Information about the recipients of the data and whether the user can avoid data sharing was quite often found. Information on the possibility of objecting to data sharing was found less often.

Overall, taking into account all the verbal, printed and online information that mystery shoppers found, they were divided on the question of whether they felt well informed about the issue of having control over data processing, with more or less equal numbers well informed and not well informed.

The feedback about the privacy policy documents showed that shoppers could generally locate information about data being shared with third parties. The text of the privacy policy was regarded as overall clear as far as data sharing was concerned, with some exceptions. Most of the shoppers could identify an indication that only anonymised or pseudonymised data would be shared with third parties. The assessments also found that the policy stated that data could potentially be shared with third parties without the explicit consent of the consumer.

5.7.6. Specific uses of data

Most shoppers did not find a statement about automated decision-making or profiling.

5.7.7. Changes to the privacy policy or terms and conditions

Only one shopper was able to find information about changes to the privacy policy, reporting that it was stated that Volkswagen can unilaterally change its connected services privacy policy, with a list of the changes that can be made. According to the feedback, the consumer would be notified of changes **after** the changes have taken place, which, if this is true, the study team does not consider a good practice.

All shoppers found information stating that the terms and conditions can be changed unilaterally, with the specification of the changes that can be made. It also stated that consumers are to be notified about the changes, but it was unclear when that would happen. One shopper's feedback was that this would happen after the changes have taken place. Shoppers also found it difficult to consistently assess what a consumer would have to do if they did not agree with the changes, providing different interpretations on what would need to be done. The study team believes that this indicates, at least, that the provided information was not easy for all shoppers to understand, and that Volkswagen should consider improving its clarity and accessibility.

5.7.8. Exclusion or limitation of liability

Most shoppers could identify a general clause that limits the liability of Volkswagen in the context of the connected services. No indication was found that this liability would be limited in the event of breaches of the data protection laws, which, according to the study team, is the correct practice.

5.7.9. Termination and lock-in

Only one shopper could find information that mentioned that refusing or terminating the collection of certain data could affect the usability of certain connected services (although not the normal use of the car).

Most shoppers reported that the privacy policy confirmed the right of the consumers to data portability, allowing them to transfer their data to another system. However, the right to obtain the data was found less often. No explicit information was found about any cost impact of terminating data processing (such as less optimal energy use).

5.7.10. Software and security updates

Shoppers could not find information about guaranteed software or security updates.

5.7.11. Code of conduct and external supervisory authorities

Some shoppers found a (nameless) internal code of conduct, and a reference to an external supervising authority.

5.7.12. Basic information on contracting

Most shoppers found information on the fact that consent for data processing would need to be issued as soon as the connected services were activated, after purchasing the car. As the terms and conditions and the privacy policy are readily available before the purchase, the consumer has the opportunity to become acquainted with the binding documents, which logically means that it is acceptable to request consent on activation.

Most shoppers found it stated that a combination of accepting the terms and conditions and the actual use of the services makes up the binding agreement. This description, however, was not always clearly understandable by mystery shoppers. Most shoppers also found it stated that consumers are only allowed to withdraw from the contract within a limited time period after the contract starts.

6. Annex 2 – Assessment scope for each manufacturer

Tables 6.1–6.7 summarise for each manufacturer the scope of the assessment, in terms of the model/trim investigated, the connected services brand considered, the countries in which mystery shopping visits and audits took place, and the sources that were audited (if found).

Table 6.1. BMW assessment scope

BMW	
Model/trim investigated	BMW 3 Series (any trim)
Connected services brand name	BMW Connect
Countries where assessment took place	Germany, Ireland, Poland
Sources audited	
Connected services website	Germany: https://www.bmw.de/de/topics/service-zubehoer/bmw-connecteddrive/bmw-connected-drive-uebersicht.html Ireland: https://www.bmw.se/sv/avdelning/erbjudanden/bmw-digital-services-and-connectivity/bmw-connected-drive-overblick.html Poland: https://www.bmw.pl/pl/topics/fascination-bmw/electromobility/samochody-elektryczne.html

Privacy policy	Germany: https://www.bmw.de/content/dam/bmw/marketDE/bmw_de/new-vehicles/pdf/BMW_ConnectedDrive_Datenschutz.pdf.asset.1644850761823.pdf Ireland: https://btccontentwebappeu.azurewebsites.net/staticcontent/Angular/gdpr/v3/?target=bmw-browser#/legal-docs-content?version=2021.11.01-38&fileName=Bmw_cd_pp_se-sv.json Poland: https://www.bmw.pl/content/dam/bmw/marketPL/bmw_pl/topics/offers-and-services/Connected%20Drive%20Disclaimer/Legal_BMW_BMWi_PL_pl_11-18.pdf.asset.1541492020824.pdf
Terms and conditions	Germany: https://www.bmw.de/content/dam/bmw/marketDE/bmw_de/new-vehicles/pdf/01_BMW_TermsConditions_D1_09122021.pdf.asset.1639057464388.pdf Ireland: https://btccontentwebappeu.azurewebsites.net/staticcontent/Angular/gdpr/v3/?target=bmw-browser#/legal-docs-content?version=2021.11.01-38&fileName=Bmw_cd_tc_se-sv.json Poland: https://www.bmw.pl/content/dam/bmw/marketPL/bmw_pl/topics/offers-and-services/Connected%20Drive%20Disclaimer/Legal_BMW_BMWi_PL_pl_11-18.pdf.asset.1541492020824.pdf
Printed documents (yes/no)	Germany: yes Ireland: no Poland: no

Table 6.2. Renault assessment scope

Renault	
Model/trim investigated	Renault Clio (any trim)
Connected services brand name	My Renault
Countries where assessment took place	Ireland, Spain, France
Sources audited	
Connected services website	Ireland: https://www.renault.ie/renault-connect.html Spain: https://www.renault.es/renault-connect/servicios-multimedia.html France: https://www.renault.fr/renault-connect.html
Privacy policy	Ireland: https://www.renault.ie/privacy.html Spain: https://www.renault.es/informacion-legal.html France: https://www.renault.fr/renault-connect/donnees-services-connectes.html
Terms and conditions	Ireland: https://myr.renault.ie/cgu.html

	Spain: not found France: not found
Printed documents (yes/no)	Ireland: no Spain: no France: no

Table 6.3. Peugeot assessment scope

Peugeot	
Model/trim investigated	Peugeot 5008 (Roadtrip, GT and GT Pack trims)
Connected services brand name	Peugeot Connect
Countries where assessment took place	Ireland, France, Italy
Sources audited	
Connected services website	Ireland https://www.peugeot.ie/brand-and-technology/online-services/save-time-and-money.html France: https://www.peugeot.fr/acheter/mobilite-et-connectivite/services-connectes.html Italy: https://www.peugeot.it/acquista/mobilita-e-connettivita/peugeot-navigation.html
Privacy policy	Ireland: not found France: not found online but a privacy policy was provided in print Italy: not found
Terms and conditions	Ireland: not found France: not found Italy: not found

Printed documents (yes/no)	Ireland: no France: yes Italy: no

Table 6.4. Toyota assessment scope

Toyota	
Model/trim investigated	Toyota Corolla (any trim)
Connected services brand name	MyT
Countries where assessment took place	Ireland, France, Sweden
Sources audited	
Connected services website	Ireland: not found France: https://www.toyota.fr/service-and-accessories/my-toyota/myt Sweden: https://www.toyota.se/uppkopplade-tjanster
Privacy policy	Ireland: not found France: not found Sweden: not found
Terms and conditions	Ireland: not found France: not found Sweden: not found

Printed documents (yes/no)		Ireland: no France: no Sweden: no

Table 6.5. Hyundai assessment scope

Hyundai	
Model/trim investigated	Hyundai Kona (Prime trim and higher)
Connected services brand name	Bluelink
Countries where assessment took place	Ireland, Spain, Poland
Sources audited	
Connected services website	Ireland: https://www.hyundai.com/eu/driving-hyundai/owning-a-hyundai/bluelink-connectivity.html Spain: https://www.hyundai.com/es/compra/servicios-compra/conectividad-bluelink.html Poland: https://www.hyundai.com/pl/serwis/serwis/bluelink.html
Privacy policy	Ireland: not found Spain: not found Poland: not found
Terms and conditions	Ireland: not found Spain: not found Poland: not found

Printed documents (yes/no)	Ireland: no Spain: no Poland: yes

Table 6.6. Tesla assessment scope

Tesla	
Model/trim investigated	Tesla Model 3 (any trim)
Connected services brand name	Connectivity (Standard/Premium)
Countries where assessment took place	Germany, Ireland, Spain, Italy
Sources audited	
Connected services website	Germany: https://www.tesla.com/de_DE/support/connectivity Ireland: https://www.tesla.com/en_IE/support/connectivity Spain: https://www.tesla.com/es_ES/support/connectivity Italy: https://www.tesla.com/it_IT/support/connectivity
Privacy policy	Germany: https://www.tesla.com/de_de/legal/privacy Ireland: https://www.tesla.com/en_ie/legal/privacy Spain: https://www.tesla.com/es_es/legal/privacy

	Italy: https://www.tesla.com/it_it/legal/privacy
Terms and conditions	Germany: https://www.tesla.com/de_de/legal/terms Ireland: https://www.tesla.com/en_ie/legal/terms Spain: https://www.tesla.com/es_es/legal/terms Italy: https://www.tesla.com/it_it/legal/terms
Printed documents (yes/no)	Germany: no Ireland: no Spain: no Italy: no

Table 6.7. Volkswagen assessment scope

Volkswagen	
Model/trim investigated	Volkswagen Golf (any trim)
Connected services brand name	We Connect Go
Countries where assessment took place	Germany, Ireland, Italy
Sources audited	
Connected services website	Germany: https://www.volkswagen.de/de/konnektivitaet-und-mobilitaetsdienste.html Ireland: https://www.volkswagen.ie/en/connectivity.html Italy: https://www.volkswagen.it/it/servizi-connettivita.html
Privacy policy	Germany: https://consent.vwgroup.io/consent/v1/texts/WeConnect/de/de/dataprivacy/latest/pdf Ireland: https://consent.vwgroup.io/consent/v1/texts/WeConnect/ie/en/dataprivacy/latest/pdf Italy: https://consent.vwgroup.io/consent/v1/texts/WeConnect/it/it/dataprivacy/latest/pdf
Terms and conditions	Germany: https://consent.vwgroup.io/consent/v1/texts/WeConnect/de/de/termsOfUse/latest/pdf

	Ireland: https://consent.vwgroup.io/consent/v1/texts/WeConnect/ie/en/termsOfUse/latest/pdf Italy: https://consent.vwgroup.io/consent/v1/texts/WeConnect/it/it/termsOfUse/latest/pdf
Printed documents (yes/no)	Germany: no Ireland: no Italy: yes

d

DS-05-23-007-EN-N

Publications Office
of the European Union

ISBN 978-92-76-99073-4