UiT The Arctic University of Norway

Faculty of Law

Personal data and the concept of consent under the EU General Data Protection Regulation

With focus on data processing in and from vehicles

Mai-Helen Steiro

Master's thesis in Master of Law, JUR-3902, spring 2021

Table of Contents

1 Introduction

1.1 Topic and relevance

This thesis analyzes some of the challenges in the intersection between law and technology. The topics that are reviewed are personal data and consent, as two important aspects of the European Union (EU) General Data Protection Regulation[1] (hereafter GDPR). The thesis explores the GDPR from the perspective of data processed in and from vehicles, as an illustrative example of how the GDPR applies with the technological progress being made with such vehicles.

Personal data is protected through the right to privacy and a private life in international legislation and under EU law[2], but also as an individual, fundamental right.[3] Thus, several and complex legal framework on international and national levels seek to safeguard individuals from having their privacy breached through the processing of such data. The essence is that personal data is processed lawfully, fairly and in a transparent manner, in which principles which the GDPR provides further content and meaning to these overarching principles.

With an increasing use of technology and intelligent solutions in vehicles for different purposes, the responsible parties of the processing are a wider category than before, stretching from automotive industry to many different operators in the digital industry[4], who must be aware of all the aspects and risks of processing this data, in and from the vehicles. Today, current vehicles driving on the road, as well as models coming in nearest years, use or offer technologies connected through communication networks. This has many advantages, such as road safety, but also enables extreme amounts of data to be processed, which can reveal many things about your location and even health.[5] This applies to both automated vehicles on different levels, but also vehicles we don't consider as automated. The fact is, that must vehicles on the roads today are connected and thus imposes a risk to our privacy. Specific safeguards must therefore be

[1] 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.
[2] Article 8 ECHR, HUDOC *case Satakunnan v. Finland* [GC], para 136-137, see also *Rotaru v. Romania* (2014), para 43-44, and Charter of Fundamental Rights of the European Union (CFREU) Article 7.
[3] CFREU Article 8, TFEU Article 16, Convention 108 Art.1, GDPR Recital 1, COM(2020) 264 final, p.1.
[4] EDPB Guidelines connected vehicles, 01/2020, v2.0, p. 4.
[5] EDPB Guidelines connected vehicles, 01/2020, v2.0, p. 4.

taken to prevent misuse of the data. This necessitates a strict legal framework providing sufficient protection of the privacy.

The Regulation on general data protection through the GDPR had legal effect from 2018, which gives better protection of personal data for the individuals[6] than the previous Directive 95/46/EC (hereafter the Directive).[7] The GDPR introduces transparency as a principle[8] and emphasizes the individuals control over their own data and responsibility of the controller to ensure such control.[9]

This also means that a greater responsibility is required from enterprises processing this data[10], such as knowledge of what data is personal, and on which terms the data can be processed in or from the vehicle. Especially as the individuals often are not aware of all the personal data that is processed, the enterprise must give them sufficient amount of control throughout the data processing. This raises many issues in a legal perspective.

Several scandals of breaches of personal data in the big social networks and platforms have raised the awareness of what personal data people share and whether the requirements of consent or legal ground are met.[11] Compliance with the GDPR is therefore an important factor for both big and small enterprises to gain the trust of the individuals to be able to process the data safely.[12]

However, the consideration must be balanced with the objective and ambit under the European Union legislation of free flow of data between the Member States, which is also implemented in the GDPR.[13] This means that the limitations of processing data should not be stretched

[6] COM (2020) 264 final; SYN 24 June 2020, p. 1.
[7] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[8] COM(2012) 11 final, p. 8.
[9] COM(2012) 11 final, p. 2, and COM(2020) 264 final, p.1 and e.g. GDPR chapter 3 of "Rights of the data subject", such as right to information, access, rectification and erasure, see also Recital 7 (2) and Recital 39 (3).
[10] See COM(2012) 11 final, p. 8.
[11] Cambridge Analytica scandal, Schrems case on use of cloud-based services in a non-Member state country; CJEU case C-311/18 (Schrems II).
[12] EDPB Guidelines connected vehicles, 01/2020, v2.0, p. 5
[13] GDPR Article 1 (1) (3), Recital 3, and Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, and COM(2014) 442 final p. 4.

further than necessary, as it can lead to negative effects on the data economy, development of new services and weaken the internal market.[14]

Above all, the privacy and data protection of individuals depends on the data-processing actors to treat the data responsibly. To understand the term and scope of "personal data" and the conditions for consent as a legal ground is, therefore, crucial to make the protection effective. This thesis gives an in-depth review of that, with the focus on vehicles to apply the law in a practical context on some of the implications the GDPR raises.

1.2 Legal sources and methodological challenges

The purpose of this thesis is to address and discuss some specific question in an in-depth legal dogmatic analysis with a view to looking at how the realities of data processing impact on interpretating rules of data protection under the GDPR.

The relevant legislation is the GDPR, which is an international regulation applying to all Member States of the European Union and the European Economic Area (EEA).[15] The GDPR (or "the Regulation") entered into force in 2016, but it is important to note that it was not given legal effect before May 2018.[16] The Regulation replaced the previous Directive from 1995,[17] which means that the regulation is legally binding for each member state in EU/EEA.[18] The previous Directive was implemented and applied in various ways in the different Member States, leading to different levels of data protection within Europe.[19] The data protection is, in that sense, strengthened and harmonized through the Regulation.[20]

Norway incorporated the regulation as national law through the "Personal Data Act" in 2018.[21] According to Art. 2 the obligations under international or European law shall apply before Norwegian law when there is conflict between the norms. This method is to ensure legal conformity and means that the GDPR practically applies as the original version.[22] Therefore,

---

[14] COM(2020) 264 final, p. 1, 14.
[15] Norway, Iceland and Liechtenstein, following its incorporation in the European Economic Area (EEA Agreement), and GDPR Article 3.
[16] GDPR, https://gdpr-info.eu/
[17] Directive 95/46/EC, and GDPR Recital 3
[18] TFEU Article 288 second paragraph
[19] COM(2012) 11 final, p. 18.
[20] See GDPR Recital 10
[21] The Personal Data Act (2018) Article1, with exceptions following by Attachment XI, protocol 1 and the Regulation as such.
[22] See Skoghøy, (2018) p. 128 and 131.

the focus of the thesis is on the legal sources on an international level, as that is binding also on national level (with some exceptions).[23]

This topic raises some issues on the matter of the method. This thesis is written from a legal perspective. However, as the topic is addressing some issues in the intersection between law and technology, and privacy protection is a part of everyday life in society, the rules must be interpreted with this in mind. The application of the data protection norms requires knowledge in other fields, in particular technology, and that this knowledge is updated to adjust to the development of newer technologies.

The GDPR consists of 99 provisions and 174 recitals in the preamble. The recitals are without legal and operative effect, but they constitute the preamble, which contributes with clarification and shed light to the purpose of the provisions. The method employed by the European Court of Justice (CJEU) when interpreting the operative law demonstrates that recitals are of high importance of bringing light to the further meaning of the provisions. The appliance of recitals is, however, restricted to the cases where it is not in conflict with the provision. The norms the provision sets are legally binding and primary source. Clear and unambiguous provisions can therefore not be overruled or modified by the reading of a recital.[24] Nonetheless, as mentioned, GDPR is characterized by some vague and general provisions to be flexible, where use of recitals can be necessary in an extensive degree, giving additional information and conditions to the legislative norm. The European court of justice, along with the guidelines and opinions of EDPB and A29WP, often refers to the recitals and appear to have an important bearing to a give further or more specific meaning to the provisions.[25]

The European Court of Justice plays an important role setting the threshold on how to understand and apply the law in practice. All Member States can request preliminary ruling from the CJEU,[26] thus, they contribute to a concise and conform law enforcement that all the member states have available when applying the law on national level.

Another challenge in this matter is that, even though data protection has developed over many years, the Regulation that is the foundation of the discussion in this thesis has been applicable

[23] See for instance GDPR article 6 (2) where GDPR allow each Member States to give more specific provisions on national level
[24] Lenaerts and Gutierrez-Fons, (2014), p. 22.
[25] See e.g. C-434/16 Nowak, para 48 and 57, C-673/17 Planet49, para 62.
[26] TFEU Article 267

for merely two years. There has not been much time for the Courts and other important actors to further elaborate and interpret the provisions, as well as lack of literature and theory.

However, the regulation is a continuation and strengthening of the previous Directive, which has been applied up until the new Regulation was applied. [27] Decisions from CJEU and other sources regarding the rules under the Directive can therefore have relevance to the interpretation and scope of the Regulation.[28]

Nonetheless, legal analysis applying older sources must be performed with care and awareness to ensure that the present view is reflected. The sources used for the purpose of addressing the questions in this thesis do not raise fundamental issues in applying the Directive to interpret the new Regulation. Mostly, the difference is addressed and clarified; or newer sources are referred, which substantiate that the older view is the present view and correct interpretation of the law.

On the matter of applying GDPR as an international source, the general principle of conformity applies, meaning that the GDPR must be interpreted in a consistent and homogenous approach throughout the Member States, to ensure equivalent protection of individuals.[29]

One entire chapter in GDPR is devoted to the principles under the GDPR, which applies to all aspects and stages of the processing. These principles are therefore an important basis for the general interpretations and notion of the other rules, which will be addressed in the analysis where relevant.

The European Data Protection Board (EDPB) is an independent body, composed of representatives from the Data Protection Authorities.[30] GDPR Article 70 underlines that The EDPB "shall ensure consistent application of this Regulation." Their tasks is to give advisory guidance, annual reports and issue opinions, where different topics are elaborated and given further and specified interpretation.[31] The EDPB replaced the previous Article 29 Working Party (A29WP) which had similar tasks under the old Directive until 2018.[32]

---

[27] Directive 95/46/EC, and GDPR Recital 3
[28] See for instance EDPB Guidelines 05/2020 on consent, p. 4-5.
[29] COM(2012) 11 final, p. 18-19. In the European union and Agreement on the European Economic Area, "homogeneous" is also used in the preamble and article 1 in the Agreement.
[30] GDPR Article 68
[31] GDPR Article 68, 70, 71, 64.
[32] Directive 95/46/EC Article 29 and COM(2012) 11 final, p. 14,

Opinions and guidelines on statutory legislation usually have limited weight as a legal source and is rarely referred to by the Court. However, the court often refers to and relies on the Advocate Generals Opinion,[33] which refers to the works of the expert groups.[34] The fact that the field is rapidly changing and dynamic explains why the framework is characterized by vague formulations in some provisions and leaning on discretional assessments with many elements and factors that must be considered. As the technological development is uncertain, this gives a great flexibility. On the other hand, the independent bodies are given a great responsibility to further develop the specific content of the vague framework set out in the GDPR.[35] Thus, the EDPB has a high influential impact on the interpretation of the GDPR.[36]A considerable amount of the legal sources which elaborates on the provisions are, therefore, guidelines, letters and best practices among others, which consequently must have more legal weight than of what may be normal the European legal system, but with a critical approach.[37]

Guidelines from before 2018 can be relevant, as much of the Regulation is similar to the Directive,[38] especially certain definitions and terms that was well defined through the appliance and practice of the Directive. Although the newer dated Guidelines must have more weight as a source, the older might elaborate or clarify on certain issues, especially where the EDPB have endorsed the previous or explicitly states what has changes. Despite the challenge to navigate through different documents, they must be read in light of each other. In some guidelines, EDPB state clearly to what extent the previous opinion on the subject is still valid. [39] Accordingly, these will still be relevant, with the restriction in general that all guidelines are independent elaborations on how to understand the law and operative sources or legislator's opinion

1.3 Definitions

"Processing" is a wide term under the GDPR, and covers collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation" just to mention some.[40] The term is used in a wide sense in the thesis, the most relevant are when data is collected inside the vehicle and also from a vehicle and then transmitted to an external cloud-service based

[33] See e.g. Case C-673/17, Planet49, para 51, 61, 69.
[34] See e.g. Case C-673/17, Planet49 (AG Opinion) para 81.
[35] Bygrave, 2014, p. 3.
[36] Bygrave, 2014, p. 174, see also general information on https://edpb. europa.eu
[37] Bygrave, 2014, p. 4
[38] Schartum, 2020, p. 24
[39] See for instance EDPB Guidelines 05/2020 on consent, p. 4-5.
[40] GDPR Article 4 (2)

platform for online storage and analysis. It can be processed in the vehicle through different methods, and electronic sensors in the car collecting personal data are also considered as acts or operations falling under this notion of "processing".[41]

The thesis will focus on processing data in and from motor vehicles. Vehicles is not defined in GDPR, but the term is used in accordance with the definition in the Directive 2007/46/EC, concerning the approval of motor vehicles.[42] Article 3 describes a 'motor vehicle' as "any power-driven vehicle which is moved by its own means, having at least four wheels, being complete, completed or incomplete, with a maximum design speed exceeding 25 km/h". A car is an example which is used throughout the analysis. Vehicle is used because it is a wider term, and the issues raised in this thesis will be equally relevant when processing personal data through, for instance, a motorcycle. The term is used in the sense of vehicle for private use, by a "natural person" as a subject who is in need of protection under the Regulation, which is further defined under the legal analysis of "personal data" in chapter 3.

Privacy for the purposes of this thesis is a term referring to the right each individual has to their own "private life", as defined in Article 8 (1) of the European Convention for the Protection of Human Rights and fundamental freedoms, (hereafter ECHR). The Article provides the individual a right to respect for their private life, family, home and correspondence. Processing personal data is an action that can interfere with this right, thus protection of this data is considered necessary through legislation on national level to safeguard individuals and ensure that their self-determination is intact.[43] Data protection is a fundamental right set out in the Article 8 of the Charter of Fundamental Rights of the European Union (hereafter CFREU) and Article 16 (1) of the Treaty on the Functioning of the European Union (hereafter TFEU), which provides that everyone has the right to the protection of personal data concerning him or her.[44]

1.4 Delimitation and the way forward

This thesis examines the scope of personal data and consent as a legal ground for processing such data. There is not space to treat other legal grounds, other than what is necessary and relevant for the specific questions raised and to shed light on the issues in focus. The consequences of breach of privacy protection are only mentioned briefly, as the purpose is to

[41] Schartum and Bygrave, 2011, p. 137
[42] Directive 2007/46/EC
[43] ECHR guide on article 8, 31.12.2020, p. 45, para 180.
[44] GDPR Recital 1

examine and clarify when data is personal and what is required for a consent to be valid – in other words, some of many aspects that a controller must consider to avoid breach of GDPR and being subject to sanctions.

Sensitive data as a sub-category of personal data is discussed merely to address some examples of data sets that may be processed, but the thesis should not be read as a comprehensive analysis or in depth review of sensitive data and the grounds for processing such data, as set out in Article 9 GDPR.

The thesis is limited to practical and legal issues on regards of processing data in and from vehicles, to narrow the focus and apply the rules in a context that is relevant now and the nearest future for several actors. However, the thesis is primarily a legal analysis. The technological aspect is not described to a particularly comprehensive extent but limited to a basic and general level of what is necessary to shed light on important legal aspects and issues that should be further looked into. The technical terms of the technologies are therefore only examples put in a context, but a thoroughly assessment of the technology should not be necessary to understand the issues addressed.

The data privacy framework in EU also consist of the ePrivacy Directive[45], which regulates the "processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". [46] It applies to the electronic communication sector and complements the GDPR.[47] The rules of how communication services can process personal data certainly play a role for the protection of the drivers of the vehicles, as subscribers themselves or that the vehicle collects data through such services.[48] However, the general Regulation (GDPR) is the focus in this thesis.

An overview of the most important chief actors that must be addressed to understand the main issues raised is presented in chapter two. Chapter three gives an in-depth legal analysis of the criteria of personal data, addressing the scope of this data and typical practical examples applied

[45] 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), L 201/37.
[46] ePrivacy Directive Article 3 (1), Article 1.
[47] ePrivacy Directive Article 1 (2).
[48] EDPB guidelines 01/2020 on connected vehicles v2.0 p. 14, 27.

to vehicles. Chapter four is the other main chapter, which focuses on consent as one of the legal grounds for processing personal data. The conditions of a freely given consent are analyzed in a legal aspect and put in a practical context addressing how and what a controller must take into account when obtaining consent. Finally, the final remarks are in chapter five.

2 Chief actors under the GDPR

There are several chief actors under the GDPR that are important. The most central to define in purpose of the thesis are the data subject, controller, processor and recipient. The obligations under the GDPR will depend on the roles of the party, thus, it is crucial to clarify this before starting any processing of data to avoid breach of the GDPR.

A data subject is a "natural" person[49] who can be "identified", Art.4 (1). The data subject here is the driver or the passengers of the vehicle, but they will be referred to as the driver for the sake of simplicity.

A "controller" is described in Article 4 (7) as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines (..) the purposes and means of the processing of personal data", where the purposes and means of such processing are determined by Union or Member State law and the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

The "purposes and means" of the processing is a wide category, in which the party must determine both, as they are cumulative. The content of "purposes and means" is referred to as "the why and how" of the processing.[50] However, "means" must be understood as the main means of the processing. The criterion of means does not include "non-essential means".[51]

"Determines" indicates that, as long as the actor has a saying on any part of the processing, regardless to what extent, it can fulfill the requirement as a controller and thus have to comply to the GDPR with the legal obligations that follows. The key element is that the actor decides the purposes and means.

[49] GDPR Article 1.
[50] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3
[51] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3

As controller can be "jointly with others", this enables more than one entity to be involved in the data processing, as long as the party "determines the purposes and means of the processing of personal data."[52] This concept on joint controllership was introduced in the new GDPR in Article 26. Controllership can be shared, without regards if one of the controllers determines a lot more and without a minimum requirement of the amount the controller determines. However, it is required that each entity is necessary for the processing of the data and that "processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked".[53]

The joint controllership can be organized as the controllers having some say in the same part of the process as a common decision, or that they decide each of their part complementing each-other.[54] However, when an entity has some say in both the means and the purposes of the processing, and is necessary for the processing, the party qualifies as a controller.

A private individual can also be a controller, hence the term "natural" person in Art. 4 (7). However, the scope of the Regulation does not cover "purely personal or household activity" according to Article 2 (2) (c) GDPR and Recital 18, such as filming your own family and posting it in the chat with your family. The recital dictates that if such activity has a "connection to a professional or commercial activity", for instance, that you send the video to a tv channel so they can show it on TV, it is within the scope.

The European legislators and the Court have taken a broad view of the notion of controller.[55] The role as controller can be anyone and "there is no limitation as to the type of entity that may assume the role of a controller", according to the EDPB from 2020.[56] Usually it is the company or "organisation as such" who controls the data, and not an individual.[57]

The controller, in the case where the driver of the automated vehicle is the data subject, would typically be the car manufacturer company, for instance, Volvo (but not necessarily in respect of all the data). Another party can be a part of a joint controllership if they are a part of determining why and how to process the personal data about the driver. This can be a developer

---

[52] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3
[53] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3
[54] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3
[55] Case C-131/12 Google Spain, para 34, and C-210/16, Wirtschaftsakademie, AG opinion, para 28, and EDPB Guideline 07/2020 on concept of controller and processor, p. 9 and 35.
[56] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3
[57] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3.

or service provider of other value-added services in vehicles.[58] Their responsibility is further given in chapter 4 of GDPR, in particular Art. 24 (1), which dictates a duty to implement, review and update "technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation".

Another chief actor under the GDPR is the data "processor", which is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller", Art. 4 (8) GDPR.

The first criterion is that the processing is "on behalf" of the processor. This means that the processor is always in a relation to the controller, and under the instructions of the controller.[59] In light of the term "controller", the processor has a different role, and the processor does not determine the "means and purposes" of the processing. If so, they will be regarded as controller and have the obligations pursuant to the GDPR as a controller. A certain degree of determination is accepted within the instructions of the controller though, such as "to choose the most suitable technical and organizational means".[60] Article 28 in the GDPR further determines the obligations of the processor.

A second condition to be a processor is that the processor is another actor, or "entity" than of the controller.[61] A controller can naturally undertake the processing of the data, and is it up to the controller to undertake this task himself or outsource the processing to a separate legal entity. It is only the latter case that the role of processor emerges.

Typical examples of entities acting as processor in relation to the vehicle manufacturer are equipment manufacturers and automotive suppliers.[62] These entities can nevertheless be a controller for other purposes, and in relation to others.[63]

In addition to the controller (and processor) on the processing side, another actor is the "recipient", "to which the personal data are disclosed, whether a third party or not, under Art. 4 (9). The disclosing of the data must have a legal ground in accordance with the GDPR, which, for example, requires explicit consent from the data subject, such as an insurance

[58] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 12
[59] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 3
[60] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 4
[61] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 4
[62] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 12
[63] EDPB Guidelines 07/2020 on the concepts of controller and processor, p. 12

company receiving health data.[64] In regard to vehicles, this can be a "commercial partner of the service provider", who acts as a new data controller, or as a data processor.[65] The recipient must comply with the obligations that the Regulation sets.

An important note is that the controllers have more obligations under the GDPR than processors do, as the controller determines means and purposes and instructs the processor. For the purpose of this thesis, controller will mostly be used as the responsible party in relation the protection of the data subjects' personal data.

On the legislative level and in regard to developing the data protection legislation, the important actors are the Council of Europe (CoE), the Organisation for Economic Cooperation and Development (OECD), the United Nations (UN), and the EU. [66]

3 Are data processed in or from a vehicle subject to the rules of GDPR?

3.1 What is personal data under the GDPR?

The objective of the GDPR is to protect "personal data".[67] Therefore, the first question for an actor processing data in and from vehicles is whether this data vehicles is "personal". In general, EU legislators and CJEU has taken a broad view of the notion of "personal data" [68], but a legal analysis will be performed in the following to draw the lines and scope of the term under the GDPR.

In Art. 4 (1) "personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject')". The wording dictates four cumulative criteria for what is personal data: "any information"; "relating to"; "identified or identifiable"; and "natural person".

The definition of personal data in the GDPR is at this point identical to the formulation in the previous Directive Article 2 (a), making legal sources and interpretations for the latter interpretations applicable also for the scope of personal data in GDPR. The terms are all related

[64] Article 9 (1) and (2) (a) but see also other legal ground for processing sensitive data in Article 9 (2) letter b) to j).
[65] EDPB Guidelines 07/2020, p.12.
[66] Bygrave (2014), p. 18-19.
[67] GDPR Article 1 and Article 2.
[68] See e.g. C434/16 Nowak v Data Protection Commissioner (2017), para 33-34, and chapter 3.2.

to each other, therefore, a division as such can be rather artificial for the comprehension of the scope of personal data. However, several of the terms are not sufficiently clear and it is therefore necessary to interpret one by one to analyze the wording in light of the objective of the regulation and case law, as well as other sources that can shed light on how to understand the legislative norm and scope of personal data.

3.2 The scope of "any information"

3.2.1 Does "any information" refer to both physical and electronic data?

"Any information" by its wording covers all possible information. The literal meaning of "any" information is thus narrowed and limited, naturally in the context of the other requirements giving criteria to the "information": it must be "relating to an identified or identifiable natural person ('data subject')."

The formulation "personal data is any information" in Article (1) suggests that data and information are synonyms.

On the other hand, data may be associated with information connected to technology, meaning information from an electronic or digital medium, such as a computer or phone. That would indicate that the GDPR would only apply to electronic data. "Information" can be argued to be a wider term semantically, as data can be information, but perhaps not all information is "data" in a technological perspective.[69]

However, the use of the term "information" to describe data may indicate that the legislators do not mean to differ between these. In the CJEU decision of Case C434/16 Nowak v Data Protection Commissioner[70], the question was whether examination answers were personal information. The court expressed in general that the term "any information" is not restricted to "(..) information that is sensitive or private, but potentially encompasses all kinds of information (…)." [71]

[69] Bygrave (2015), p. 113.
[70] Case C434/16 Nowak
[71] Case C434/16 Nowak, para 34

A wide scope suggests understanding "any information" literally and without restrictions. The information can be in the "form of opinions and assessment", but whether it can be physical and not only digital is not explicitly addressed by the Court.

A physical document with text written on it is not as natural to categorize as "data" "wholly or partly by automated means" or that these documents "form part of a filing system or are intended to form a part of a filing system" as set out in the material scope of the regulation.[72] However, as long as these requirements are fulfilled, nothing in the law or case law explicitly states that handwritten or physical documents are exempted, thus they must be considered as "data" or "information".

Several cases from the European Court also illustrates such lines. In the case of Nowak[73], the question was not whether these documents were information or data in the terms of the law, but whether it was "personal" or not. Even though it is not clear from the facts if the examination answers were physical documents, the Court clarifies that "In the case of a handwritten script, the answers contain, in addition, information as to his handwriting." [74]

It appears that the Court does not differentiate between information or data, as the latter could potentially narrow the scope to only electronic data. The Advocate General of the European Court of Justice instructs that "It may be available in 'written form' or be contained in, for example, a sound or image."[75]

In the preamble of the GDPR, the legislators set out a technology neutral protection that "should not depend on the techniques used". [76] This also points in the direction of not differentiating between "information" and "data" in the purpose of the wide scope of personal data that the regulation seeks to protect.

This view is also taken by the A29WP,[77] along with the preparatory works for the Norwegian act[78], which substantiates this conclusion. "Any information" is a wide term, where the

[72] GDPR Article2 (1).
[73] Case C434/16 Nowak, para 26 and the following
[74] Case C434/16 Nowak, para 37
[75] Joined Cases C- 141/ 12 and C- 372/ 12, YS (AG Opinion), para. 45
[76] GDPR Recital 15 (1)
[77] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 4
[78] NOU 1997:19, chp. 10.1.1 and chp. 21 and Ot.prp. nr. 92 (1998-1999), chp. 4.2.2 and chp. 16

legislator indicates that "personal data" must be interpreted broadly, purposely to give the best protection possible.

As "data" and "information" are used as synonyms in the regulation, the term is technology neutral, and the Court endorses a broad approach, "any" information in any format can be argued as information or "data" per definition. There has not been a question before the Court as to whether a piece of information was "information" in the terms of the regulation[79]. The crucial element appears to rather be the content of the information and how the information can identify a person.

A narrowed definition, such as the one mentioned above on regards of "data", should not be applied. "Any information", therefore, covers both electronic and physical information if it is fulfilling the requirements of the material scope.

3.2.2 Must the information be correct?

In the Nowak case, the court states that "any information"

> "(..) is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information (…), not only objective but also subjective, in the form of opinions and assessments, provided that it relates to the data subject."[80]

The A29WP also mentions that "any information" covers both objective and subjective data.[81] Objective data indicates facts about as a person and are the least problematic to define as "personal data", for instance, a police record or bank document with details on you as a person.

The fact that it can also be subjective information, implies that a subjective opinion or statement about others, which is not necessarily true or based on actual facts, is within the scope of such "information". That indicates that the information does not have to be true or correct.

There might be cases where a person was wrongly identified and the "relation" between the information and the person turned out to be wrong, for example, that the wrong user of the car was identified. Art. 4 (1) does not explicitly require that the information is correct, but based

[79] search in CURIA April 2021 by me
[80] Case C434/16 Nowak v Data Protection Commissioner (2017), para 34.
[81] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 6.

on the aim of the law to protect the privacy of people, it is necessary to ask whether a person's privacy is in need of protection if the information about them is incorrect.

An important part of the GDPR is, considering the principle of accuracy, that the processor must make sure that the information is "accurate and, where necessary, kept up to date".[82] The data subject also has the right to access[83] and to rectify the information.[84] A logical consequence of this is that the information might be incorrect, but nevertheless be data that requires compliance with the regulation.[85]

In the opinion of the A29WP, it does not matter if the information is true or false. [86]

In the light of the aim of the regulation, a person who is mentioned or identified is put in a vulnerable situation and had their privacy breached whether the information is true or not. If your name is related to a crime based on that the car linked to the crime is owned by you, the harm has already happened, even though it was another driver. A lot of data from devices and applications can give indications and assumptions of the habits of a person, which in the wrong eyes can lead to a wrong picture of the reality, and unwanted conclusions and actions. Even though the mistakes can be corrected, the risk of being harmed, in the way the GDPR seeks to avoid to individuals, is high. Therefore, the ones who sits on such data, either controller, processor or other stakeholder or parties receiving the wrong information or sharing the wrong information, should be as much responsible as if it was correct. Nevertheless, the person who had their identity revealed is in necessity of their privacy protected regardless.

This view is also reasonable in a practical aspect, as the controller do not know at the time of processing whether the information is correct or not and should, therefore, treat it as personal data, regardless. One of the ambits of the GDPR is namely to make the actors responsible when processing personal data. Thus, it is not reasonable that the controller is exempted from the responsibility due to a "lucky mistake" if it turns out that the information was in fact identifying the wrong person. The information should therefore not depend on whether it is correct and thereby limit the responsibility.

---

[82] GDPR Article5 (1) (d)
[83] GDPR Article15 (1)
[84] GDPR Article16
[85] A29WP 136. Opinion 4/2007 on the concept of personal data, p.6.
[86] A29WP 136. Opinion 4/2007 on the concept of personal data, p.6.

What is limiting the scope of "information" is therefore not the content or the information itself, but whether it can relate to a person, which leads to the next and closely connected requirement of "relating to".

3.3 When is the information "relating to" the identifiable person?

"*Relating to"* an identified or identifiable natural person in general terms means that the data must be *about* the individual in question. The word indicates that a connection or a link between the personal data and the person must be established, hence the data must not only be personal but personal *about* the individual in matter (the natural person).

For example, a folder with information about your medical history at the doctor's office or the tax office's folder with your name obviously have the content of personal information about you, and the personal data in question is related to you.[87] To establish a connection or "relation" between the data and the person is as in these examples uncomplicated.

In the Nowak, the CJEU refers to three elements on the matter of the evaluation of "relating to": content; purpose; and effect.[88] The case concerned Mr. Nowak, who claimed that he was entitled to receive a script of his submitted examination paper that was now corrected, which his employer refused on the grounds of the script not containing data related to Mr. Nowak. In the analysis on whether the requirement of "relating to" is fulfilled, the question is specifically whether the examination paper has a content, purpose or effect that is "linked" to Mr. Nowak as a "particular person." [89]

The A29WP also refers to these three alternative elements to determine whether the threshold of "relating to" is met, which are elements of either "content", "purpose" or "result".[90] These three elements will be discussed in the following, in the light of the Nowak case and the A29WP.

3.3.1 The element of content

On the matter of the content-element, the Court explains how the examination answer of Mr. Nowak "reflects the extent of the candidate's knowledge and competence in a given field and,

[87] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 6.
[88] C434/16 Nowak, para 35.
[89] C434/16 Nowak, para 35.
[90] A29WP 136, Opinion 4/2007 on the concept of personal data, p. 10.

in some cases, his intellect, thought processes, and judgment".[91] Therefore, the Court concludes that the element of content was present in this case.

The Court also referred to different national legislation already, determining that written answers submitted by a "candidate at a professional examination constitute information that is linked to him or her as a person", but in the respective country of the case, Ireland, this was still unclear.[92]

Whether this element of "content" gives any additional clarity to the evaluation of the requirement "in relation to" is disputable. The phrase "content" is simply pointing if the information in question is "containing" personal data.

In the A29WP the "content" is referred to as "corresponding to the most obvious and common understanding in a society of the word 'relate'". [93] The elaboration on this element is when the information (data) is "about" the person, hence a wording and synonym of "relation to". This confirms the redundance of adding an element of "content".

In the case of Nowak, the script of the examination was the object with the content. When the court states that this indeed contains data about Mr. Nowak's "competence and field" and therefore is "related to" Mr. Nowak, it is difficult to see that "element of content" is contributing on the matter of evaluating if there is a "relation", further than just interpretating the requirement itself.

The more interesting and helpful tools are the two other elements: "purpose"; and "effect" or "result".

3.3.2 The element of purpose

Regarding the examination papers, the court states that "the purpose of collecting those answers is to evaluate the candidate's professional abilities and his suitability to practice the profession concerned."[94] Without elaborating further on this matter, or explicitly conclude, the Court hereby indicates that the element of purpose is present.

---

[91] C434/16 Nowak], paragraph 37.
[92] C434/16 Nowak, paragraph 36.
[93] A29WP 136 Opinion 4/2007 on the concept of personal data, p. 10
[94] Case C434/16 Nowak, para 38.

This type of information about collected through an examination paper can establish a relation between the person and the data.

This means that the exam paper is not necessarily with the content of the candidate's professional abilities. However, if the purpose with the exam is to collect this kind of information, which, it often is, then the actual content does not matter. This has a practical aspect to it, as it is not up to the "collector" to evaluate if the actual content in each specific case does relate to this kind of information. If the purpose of this is to collect that information, there is no need to evaluate the actual content.

According to the A29WP, the element of purpose is present if "the data are used or are likely to be used (..) with the purpose to evaluate, treat in a certain way or influence the status or behavior of an individual."[95] This appears to be an inspiration to the courts' evaluation of this element.

3.3.3 The element of effect or result

In the Nowak case, the Court held that the use of the information from the examination paper "is liable to have an effect on his or her rights and interests*",* as *"*it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought." [96] In other words, the requirement for this element to be present is that there is a possibility that the information is responsible ("liable") to have an effect for the person.

This indicates a low threshold to establish this "relation" or link between the data and the person and is compliant with a broad notion of the "personal data" term. It is not required that the information will have an effect, only that it "may" have an effect.

A29WP uses the element of "result" instead of effect, explained as "their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case".[97] This indicates a wider literal meaning of "relation" than the two previous elements. If the previous elements are not present it is still possible to establish a relation. This last element is therefore the most important, as it sets out the upper threshold for whether information can be considered "personal".

---

[95] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 10
[96] Case C434/16 Nowak, para 39
[97] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 11

To demonstrate this threshold, the example used by the A29WP is illustrative. A taxi company is collecting real time location data of the taxis with the purpose of providing better and faster service to the clients.[98] The first question is whether this data relates to the taxi drivers. This example would fall under the special rules of processing personal data in employment relations, but it illustrates how to assess whether a specific type of dataset is relating to a person.

The location data from the taxi reveals the whereabouts of the driver and is so to speak data relating to the driver and his whereabouts. On the other hand, this "relation" is not as obvious as in the previous examples. And as stated by the A29WP, "Strictly speaking the data needed for that system is data relating to cars, not about the drivers".[99] The purpose of collecting the data has nothing to the with the taxi driver and is not with the focus on the taxi driver. This could indicate that the data does not relate to the taxi driver, and that he is not in need of the protection that the law seeks to give. The element of content or purpose is therefore not present.

However, the opinion concludes with that, in such a situation, the processing of this location data should be subject to the rules of data protection, because the system "have a considerable impact on these individuals" *[100]*, as the system would allow monitoring of the performance of the drivers.

The processing of location data of the taxis was therefore "likely to have an impact" on the drivers "rights and interest", although it did not have the purpose to do so. The A29WP of the guidelines to the old Directive 95/46/EC thereby draw a broad scope through this example.

In the taxi example, the question would be if the data had a "content" of information about the driver, or more specific if the location data was about the driver. It might be possible to conclude with this, but less straightforward compared to the example of Nowak and the script of the examination document. Imagine requesting your boss for the location data about the taxi you are driving, versus asking for a paper you wrote yourself. It is likely that the latter would be more obvious to have the rights of in terms of personal data.

If instead of looking for if the data was with an element of content or purpose, the focus should be on the result element, as it was indeed easier to establish the link of "relation". This

[98] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 11
[99] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 10
[100] A29WP 136. Opinion 4/2007 on the concept of personal data, p. 10-11

demonstrates that in cases where it is difficult to establish the "relation" between the data and the person, the three elements will be a helpful tool to evaluate if there is a sufficient "relation" between the data collected and the person. If the element of result is non-existent, or difficult to argue is present, then it is probably outside of the scope of the "personal data" term.

Instead of using the term "content", it can be asked whether the location data was "in relation" to the taxi driver. Probably the conclusion would be the same, and just as difficult (or easy) to reach. However, the elements are a helpful tool when the content element is non-existent to draw the line of the scope of "relation", starting with the easiest and moving to the most questionable: first content, then purpose, then, if needed, "result". The latter sets the absolute threshold.

As mentioned, the term "relating to" is also narrowing the possibility that "any" possible information can be subject to personal data. After analyzing the meaning and scope of the criteria "relating to", it is clearly a high threshold to conclude that data is not relating to the person.

3.4 When is the person that the information relates to "identified or identifiable"?

To fulfill the requirement of personal data, the information must relate to "an identified or identifiable" natural person.[101]

Article 4 (1) defines "an identifiable natural person" as:

> "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" [102]

The wording of "identified" indicates that the data separates the person from a bigger group of people. It is closely connected to identity, which summons information describing you as a unique person. By the A29WP it is referred to as someone "distinguished" from others.[103]

---

[101] GDPR Article4 (1).
[102] GDPR Article4 (1)
[103] A29WP 136 Opinion 4/2007 on the concept of personal data, p. 12, and A29WP 199 Opinion 08/ 2012 Providing Further Input on the Data Protection Reform Discussions', p. 4

“Identifiable” is given as a second alternative, “or”, implying that “personal data” also covers information that is able to identify someone. In other words, it is not necessary that the data leads to identification already at the time of collecting the data. The data controller has to take into account the possibility that the data can identify someone at a later stage in the processing of the data.

The element of identifiability is the upper limit for the scope of this requirement. It constitutes the threshold, as it is this term that, in the assessment, establishes the link between the data and the person, and is decisive for whether the data is “personal data”.[104]

The scope of “identifiability” imposes several practical challenges that will be addressed in the following.

The paragraph provides further definition of what it takes to fulfill the requirement of “identifiability”, referring to identifiers such as a “name, identification number, location data, an online identifier.”[105]

“Such as” refers to the mentioned identifiers being examples and not a complementary list. The determinant is if "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;” can lead to identification of a person, either “directly or indirectly”.

“One or more” factors suggests that there can be different information that together leads to identification. This is closely connected to the alternative of “indirectly” identification.

The term “indirectly” identification indicates information that by itself is not identifying the person, but leading to identification by using other additional information, such as a second source or secondhand information.

An “identification number” or “location data” as mentioned in the article, is not revealing the identity of a person itself, but is a source of data leading to identification by a simple search or

[104] A29WP 136 Opinion 4/2007 on the concept of personal data, p. 12
[105] GDPR Article4 (1)

additional information. Name is the most common directly identifier, but it is not necessary to know someone`s name to identify them.[106]

This is reflected by the understanding of indirectly identifiers and by CJEU. In the judgment of case C-101/2001, *Bodil Lindqvist,* the Court considered "telephone number or information regarding (..) working conditions and hobbies" as processing of personal data, which in that case was referred to on an open Facebook-group.[107] The conclusion of the Court was that the private person posting such information about her colleagues in the group, Lindqvist, was in breach of the privacy protection rules, which at that time was the Directive 95/46/CE" 11.[108] The same understanding must be applied to the GDPR as the definition of "personal data" is similar. The Court did not state explicitly that these were "indirectly" identifying the persons, but this appears from the assessment by the Court, as the identifiers were not directly identifying the persons.

With the increasing amount of digital traces we leave behind by using internet and electronic applications, it is becoming more easy to add different types of information and link it to a person, as the Lindqvist case showed already back in 2003 and A29WP.[109] A quick search for a telephone number can lead to the name, residence and a lot of other information, even more than what was possible 18 years ago by the time of the Lindqvist case.

The European Commission stated that

> "A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc)".[110]

By the term identifiability, the possibility of adding more identifiers together and including indirectly identification in the assessment of "personal data", the legislator has taken into account today's rapidly developing information-society and the large scale of processing and

[106] A29WP 136 Opinion 4/2007 on the concept of personal data, p. 14
[107] Case C-101/2001, Lindqvist, para 19.
[108] Case C-101/2001, Lindqvist, para 27
[109] A29WP 136 Opinion 4/2007 on the concept of personal data, p. 5
[110] COM (92) 422 final, p. 9.

sharing data. These terms contribute to the wide scope of "personal data". However, the wider the scope, the more difficult to state the limits specifically.

Some guidelines to this assessment are given by the Recital 26, that are not legally binding for the member states but reflects on how to understand the provisions. The Recital 26 reads:

> "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

The formulation is similar to the previous Directive on most points except from "by another person" which in the previous Directive was "any other person".

"Singling out" indicates that the information is able to identify or point out one person from the rest. In that sense, it elaborates on the criterion of "identifiability", rather than being an additional criterion. This appears to be the correct interpretation, both in the wording of "such as, singling out", and the A29WP and theory, as it was first suggested to add the phrase under the criterion of identifiability, formulated as "when, within a group a person can be distinguished from other members of the group and consequently be treated differently".[111] This was proposed changed to "singled out and treated differently".[112] Even though only part was put in the formulation of the GDPR, it serves as a part of the criterion of "identifiability".[113]

3.4.1 What means are reasonable to take into account to evaluate if a person is identifiable?

The key phrase is "all the means reasonably likely to be used" that must be taken into account to determine if a person is identifiable. Immediately, this narrows the scope to only what is "reasonable". The recital is further pointing out that "all objective factors" should be taken account of, "such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." [114]

[111] A29WP 199 Opinion 08/ 2012, p. 4.
[112] A29WP 199 Opinion 08/ 2012, p. 4.
[113] Bygrave and Tosoni (2020) Commentary on Art. 4 (1), p. 109
[114] Recital 26.

The factors of cost and time suggests that even though it is possible to identify someone, it is not necessarily personal data in the scope of the Regulation if the identification requires "unreasonable" resources. A lot of time and money can make it possible to identify, for instance, hiring a technical expert to retrieve or extract certain data or develop a complex software to make searches to find a specific person. Thus, according to the wording, it might not be reasonable to take into account such means and, therefore, it must be outside of the scope of the Regulation. The objective factors can be other than cost and time and must be applied to each different case, in the light of the ambit of the Regulation, namely the data subject's protection of privacy. The higher cost, the more difficult to access data, meaning a certain extent of the protection for the data subject already.

Exactly where to draw the lines is still not certain with this formulation. With the speed of today's technology development, it is difficult to make a certain consideration on the "technological developments", or to rule out the possibility of identification entirely. This vague and discretional evaluation is perhaps leading the data controller or processor to apply GDPR and treat all data as personal, to not risk fines and consequences. [115] Questions can be raised, such as what the point is to evaluate the scope of personal data is, if there is such a small, uncertain possibility, that the data is actually not personal. These factors require technological knowledge on the field of data processing. Combined with the legal assessment and evaluation of the Regulation, this illustrates the challenges in the intersection between law and technology and the difficulties applying the Regulation in practical. In the European Commission's report on how the law has been in practice, it is the view that certain aspects are quite challenging for the appliers, in which the scope of personal data is one of them.[116]

However, European court of Justice has clarified the scope on some points.

In the judgement of Breyer, the court deals with the scope of "personal data" in regard to "identifiability" and what is reasonable means.[117] Breyer, a German citizen, objected on federal institutions' legal ground for storing information on the dynamic IP address and data connected to his IP address. Static IP addresses are already submitted as personal data by a former case in

[115] GDPR Chapter 8
[116] COM(2020) 264 final, in particular p. 7
[117] C-582/14, Breyer

the CJEU, in the "Scarlet Extended" case, because the address could be connected to a specific computer and lead to identification of a particular individual.[118]

On the contrary, dynamic IP addresses cannot identify someone directly because a new IP address is generated every time the user goes off- and online, therefore it is not "information relating to an identified natural person', revealing the owner or another user of the computer.[119] The issue before the court was whether the dynamic IP address was personal data even though the federal institution storing it could not identify Breyer. Additional data from the internet service provider (ISP), a third party, could, together with the IP address, lead to identification.[120] When raising the question as to whether the federal institutions online service had "means reasonably like to be used" to identify the subject, the court agrees with the Advocate General who stated that means are not reasonable if they are "prohibited by law or practically impossible" on account of the mentioned factors in the recital 26.[121] As the federal online service could access the data from the ISP in a legal manner according to the rules of the state in question, it was considered to be reasonable means and the Court confirmed that dynamic IP address was personal data in this case.

The case illustrates that what is reasonable will vary from case to case, such as the available technology at the time of the processing. This points to the need for a dynamic assessment that is intact with the technological developments.[122] The technology available has increased and will continue to increase massively. From later case law, since the first case on personal data (Lindqvist in 2003)[123] to more recent case law, the issues arising have become more complex.[124] Along with the Breyer case, this illustrates the extensive competence needed to assess the rules in the intersection between law and technology, such as the assessment of identifiability.

The amount of data and for how long time the data is processed, in context of what is used for, are factors indicating the means reasonably likely to be used. In a vehicle, perhaps some data is merely processed in real time and not stored locally.[125] On the contrary, data collected from

[118] C-582/14, Breyer, para 33.
[119] C-582/14, Breyer, para 38
[120] C-582/14, Breyer, para 37 and 45.
[121] C-582/14, Breyer, para 46.
[122] A29WP 136 Opinion 4/2007, p. 15
[123] Purtova (2018), under chapter 4.2
[124] Such as social platforms (Lindqvist-case), IP addresses (Breyer-case).
[125] Such as some raw-data, EDPB guidelines 01/2020 v2.0 p.16

the car and, for instance, stored externally in a connected cloud or other method of processing outside of the vehicle, can indicate that more means are reasonable to take into account, as a cloud-based service implies higher risk. [126] Then, it requires an assessment of what technological developments, that may lead to identifiability in the years that the data, will be processed. The longer time the data will be stored and processed, the higher possibility that a person can be identified during that time span.[127] Therefore, the obligations of the controller to process the data in accordance with the principles, such as data minimisation[128] and storage limitation[129] will also come into play in the assessment of what is reasonable to be taken into account.

Nevertheless, the A29WP notes that a "purely hypothetical possibility" of identification is not "reasonable".[130] This means that it is not required that the controller speculates whether the technology perhaps develops in a way that makes it possible to identify someone. There must be certain clues or reference points to state that current or future technology can lead to the identification of an individual. Factual basis or assumptions must be available to state that a person is identifiable. This is also submitted by CJEU, appearing to be a valid and current view, also to prevent that all data can somehow be personal in a future perspective of what is "possible".[131]

Controllers must therefore most importantly take into account the designated factors of technology and resources, in addition to consider that vehicle-data imposes a high risk to privacy of drivers in general. Applying this, on specific datasets used in the context and purpose of their processing in each case, they can determine whether it leads or may lead to identification.

3.4.2 Who can hold the data that can lead do identification?

The person who is identifiable can be singled out or distinguished by the "controller". Additionally, Recital 26 (3) refers to that it must also be taken into account which "means are reasonably likely to be used by 'another person'". The reference frame of who can hold the data

[126] EDPB guidelines 01/2020 v2.0 p. 21
[127] A29WP 136 Opinion 4/2007, p. 15
[128] GDRP Art. 5 (1) (c)
[129] GDPR Art. 5 (1) (e)
[130] A29WP 136 Opinion 4/2007, p. 15
[131] A29WP 136 Opinion 4/2007, p. 4

that identifies a person is therefore both the controller and "another person". "Another person" is not specific and can indicate anyone else.

However, in the previous Directive the phrase was "by any other person". This suggests a wider group of people than "another person". The new wording seems to be changed consequently with the objective to narrow the scope of who else than the controller can be considered when determining who holds the data can lead to identification. On the other hand, if the legislator wished to narrow the scope, it could have been done clearer with small effort.[132]

Who "another person" is under the GDPR art 4 (1) must be seen in light of what is "reasonable" and "likely" to take into account, meaning that the means that another person is likely to use can be taken into account if the person is of some relevance to the processing. Consequently, the entire world cannot be taken into account, only actors that have some relevance to the processing of that data. Otherwise, the scope will be so wide that all information in theory can lead to identification. As mentioned above, "any information" "relating to" are wide terms, which depend on the other terms also, and the criterion of "identifiability" is of particular importance, as it's the core of the Regulation: if the person can be identified, he should be protected. Therefore, if the reference frame of who can use the "reasonable means" could be anyone in the entire world, that would, in theory, mean that "anyone" is identifiable, which is not very practical nor necessary. This will depend on the data processing, but possible that "another person" than the controller of the processing data from a vehicle, can be processor, other stakeholders, car-equipment manufacturers, car workshops, service providers and other actors related to that industry.[133]

3.4.3 Is anonymized or pseudonymized data personal?

To make personal data non-personal may be a goal to process as much data as possible or to avoid compliance under the GDPR. Through methods such as anonymization or pseudonymization, some specific data can be removed or encrypted, so that it is more difficult for the data to lead to and identify the individual.

According to Recital 26 (5), anonymous information falls outside the scope of the GDPR, namely because it is "information which does not relate to an identified or identifiable natural

[132] Dalla Corte (2019) p. 1.
[133] EDPB guidelines 01/2020 on connected vehicles v2.0 p. 21

person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". If the data fulfills these requirements, the data is in fact not possible to use to identify a person, thus the data subject don't need protection under GDPR.

Pseudonymization however, is a reversible method, where the data can be attributed to a data subject with use of additional information, according to Article 4 (5) GDPR. The controller can use this method to secure the data better. Nonetheless, the requirement is if the person is identifiable, which includes additional information and cross referencing the data. The assessment of what "means are reasonably likely to be used" remains the determinant if pseudonymized data can in fact lead to identifiability of an individual, thus it may be personal data.[134] If the controller of the data from the vehicle wish to process data without compliance to the GDPR, the data must be anonymized.

3.5 Is the driver of the car a "natural person" under GDPR Art. 4 (1)?

In the sense of being a "natural person", the person must be alive to be covered by the protection in the GDPR. A29WP referred to Minutes of the Council of the European Union, where the Council and the Commission confirms that that there can be other rules on national levels deciding differently[135], which is underlined in GDPR Recital 26. In Norway, there are not made modifications on this point. The main rule is that the GDPR does not apply to deceased persons.

Other provisions in the GDPR appears to operate with "legal" and "natural" persons as opposites or different terms, for instance Art. 4. (7) to (10). [136] This interpretation will leave legal persons outside of the scope, for instance organizations and companies. However, this is adjusted through both CJEU and theory. Firstly, the General Court of CJEU has recognized that legal persons can have certain protective rights of data processing, with emphasis on the general provisions of privacy protection in the Human Rights Charter.[137] Information about a legal person may also relate to a natural person, even though those persons are legal persons. For instance, a one-person enterprise is in fact a "legal person". As it is only one person owning the

[134] GDPR article 4 (5), Recital 26.
[135] A29WP 136 Opinion 4/2007, p. 22-23, referring to Minutes of the Council of the European Union, 8.2.1995, document 4730/95: "Re Article 2(a)" in footnote 17.
[136] GDPR Article 4. (7-10) "the natural or legal person".
[137] T-670/16 (Order of the General Court), Digital Rights Ireland, para. 25.

company, certain information can easily identify the owner also as a natural person, hence being "personal data". According to theory, such an enterprise or a small family-run enterprise with a transparent 'corporate veil' should therefore be covered by the Regulation.[138] Again, the determinant is if a "natural persons" privacy is at stake.

This issue may occur in the scenario where a person rents a car in the name of a company. Would the rental agreement data be personal data when the company's name is on the agreement, as opposed to the name of the driver? The company would be outside of the scope as it's a legal person, but it's the data on the driver in the sense of a natural person which is collected and processed. The data of that vehicle in the time span of the rental time is indeed identifying where the driver was, the question is then if it is possible to identify the individuals persons` name. Due to the amount of data processed, the physical appearance of the individual, and that the GDPR opens up for cross referencing data from other parties, identification is highest likely even without the name on the rental contract. In that scenario, it is perhaps an employer as the "company", and specific rules regarding employment relations would perhaps apply. Nonetheless, it illustrates that the demarcation can be difficult to define.

If the criteria of "relating to" is met (element of content, purpose or result), the data must be considered "personal".[139] This illustrates that even though the unit or entity that uses the technology where the data is collected is more than one natural person, the law does not entirely exclude in the sense of being other than, or more than, one physical person, for instance, a "legal" person.

However, this adjusted interpretation of "natural person" which in certain cases also covers "legal" person or other formations of small groups, such as a private person, must not be stretched too far, and should not categorize certain groups to fall within or outside the protection as a result of how they are formally organized.

In a vehicle, the person driving is a private individual, driving their own car, and the controller is a commercial part who sold the car to the owner of the car. The data subject in the car is the driver of the car, who is alive, and in the sense of being a driver of their own car they are a natural person and not a legal person. The driver is in that sense a natural person.

---

[138] Bygrave and Tosoni (2020) Commentary on Art. 4 (1), p. 111
[139] A29WP 136 Opinion 4/2007, p. 23.

However, the data that is processed is directly linked to the car in the sense of being an object, which can have more than one driver linked to the data. The term indicates that the person must be one, physical individual. On contrary to a mobile phone where there is one user, a car can have several users. This implies that the data processed from the car is not in fact identifying one "natural person", as it may be data about all the persons driving the car, thus not "identifying one natural person".

There is not much case law on this regard from the CJEU, but the Breyer case which revolved processing data from IP addresses using a computer can shed some light on this. The Court held that:

> "(..) IP address does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer."[140]

A computer can have several users and not necessarily one personal user that clearly leads back to one identifiable natural person. Likewise, a car can have several drivers, and information on one specific car can be argued to not reveal the identity of the natural person who owns the car. However, the Breyer case illustrates that regardless of potentially several users, it was possible to identify Mr. Breyer because of the possibility to access other information which together led to identification.[141] The case of Breyer can in that sense be used as an analogy for the issue addressed on regards to vehicles, to illustrate that the data are of personal nature despite that several persons are connected to the data processed by the vehicle.

This view is substantiated by the European Data Protection Board, who also draw comparison to computer as a "terminal that can be used by different users", and that "this potential plurality of users does not affect the personal nature of the data."[142] Even though EDPB have limited weight, their statement shows that they agree with that the understanding in the Breyer case can apply to vehicles.

---

[140] C-582/14, Breyer, para 38.
[141] C-582/14, Breyer
[142] EDPB guidelines 01/2020 v2.0, p. 5.

The conclusion must be that drivers of vehicles are "natural person" under Art. 4 (1) and are "data subjects" in need of protection under the GDPR.

To summarize, data is personal if it can identify a person, either alone or together with other information. The data controller must, on a case to case basis, evaluate to which extent it is personal or non-personal, to know on what terms to process the data. Due to the wide notion of personal data and the factors mentioned, most data are in fact personal. Actors processing data in and from vehicles must therefore process this data pursuant to GDPR. In general, the assessment appears to be highly linked to whether someone is identifiable, as that will establish a need for protection of privacy (regardless if it is the correct person[143]).

3.6 Is location data personal data?

"Location data" is mentioned explicitly as an "identifier" in the definition of personal data Art. 4 (1). As pointed out with the examples of A29WP in this thesis, it is also discussed how and why location data in certain situations case "relate to" a person and thereby identify a person.

Location data is collected from most vehicles today. Either through the built-in navigational system in the car, which is not necessarily linked to "one person" but all the drivers of the car, or through a device which is not a part of the vehicle but personally linked to the person, such as a mobile phone. Sensors built in the car can also collect and process location data that is not used to get the driver from A to B but necessary for other features of the vehicle, such as giving the weather forecast, or more complex technology providing safer driving or enhanced driver experience.

Data on location of the vehicle can tell where the car is, thus the location of the driver (regardless if it is the correct driver, see chapter 3.2.2 in this thesis). Location data is not only saying something about the whereabouts of the car at a certain time, but routes, duration of the time the car is parked somewhere and thus where the driver is for longer time periods and at what time of the day and habits.

Even though the route of the vehicles journey do not directly refers to what is "work" or "home", geolocation data of the vehicle will for instance show addresses of where the car is parked every night, where it goes every morning, and these addresses could reveal a pattern

[143] See chapter 3.2.2 and 3.5 in this thesis

disclosing where the person leaves and works rather quickly. It is nevertheless not necessary that the data forms a pattern to disclose information that can identify a person. Data on the location of the car can together with other data easily reveal information of, for example, work and home address in the very least.

One may think that it is not much danger imposed to you if someone gets access to this data. Name, phone number and address are already open to the public and can be found by a quick search on google. Location data can independently or together with other datasets, reveal information about the data subject's family members, such as where the kids are, by seeing the location of the morning route and thus the kindergarden. This is just one example of a normal everyday-life routine that illustrates the risks that the revelation of location data of a car can disclose.

The core issue with the data processed from the vehicle, however, is that it makes identification of people possible in such extensive scope and must therefore not be underestimated. Most data subjects cannot even imagine the massive quantity and value information a vehicle can reveal of a person and the data that controllers hold. The European Protection Board emphasizes location data as "particularly revealing of the life habits of data subjects" [144], and that special attention therefore should be given of the controllers and other relevant actors which the GDPR establishes obligations for.

Location data is therefore in general considered personal[145], and often, but not always, it is also falling in the category of sensitive data, depending on the use.[146] In today's informational society, location data is processed in such an amount that it can reveal a lot about the whereabouts of a person, through many devices, such as phone, computer as well as vehicles. Some are therefore of the opinion that all location data should be treated as sensitive data. [147] Imagine if you go to the hospital, jail or church, these can reveal or lead to other information on your health, but also criminal data of you or someone close to you[148], or your religious belief,

[144] EDPB guidelines 01/2020 v2.0 p. 15
[145] EDPB guidelines 01/2020 on connected vehicles v2.0 p. 4
[146] Also stated by the Norwegian preposition, NOU 1975:10 p. 87, that information that at first sight is innocent alone, can become sensitive when held together with other information (my translation)
[147] Schartum et al (2014) p. 127, EDPB appears to follow such lines by emphasizing the ability it has to identify a person due to the huge amount of data generated, Guidelines 01/2020 v2.0 p. 4, 11, 15.
[148] Which is disclosed information under GDPR Article 10 and is prohibited regardless of consent.

which in principle is prohibited. This will further be discussed under sensitive data under section 4.7.

Location data is, therefore, personal data when applying the interpretation set out above on personal data, which means that when data controllers process location data in and from vehicles they must comply with GDPR. One of the important requirements to comply is to have a lawful ground for processing[149], which is one of the main principles of the Regulation and will be addressed in chapter 5. Another important principle, for the controller processing data from a vehicle, is that location data can only be processed if it is necessary, regardless of the consent from the driver. The EDPB addresses in particular that awareness must be raised "to the fact that the use of location technologies requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data".[150]

3.7 What is sensitive data under the GDPR?

In addition to personal data, there is a "special category" of personal data that in principle is prohibited from being processed.[151] This category is often referred to as sensitive data that the legislators saw necessary to protect, as they can impose high risk to fundamental rights.[152]

There are some exceptions to the main rule,[153] enabling the processing of certain sensitive data, but with strict requirements. This must be given particularly attention for controllers and processors of data from vehicles, as some data from vehicles falls or have the potential to fall into this category, even more with the newer technologies. [154]

Information that can reveal racial or ethnic origin, religious beliefs and "biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" are examples that are prohibited to process.[155]

[149] GDPR Article 5 (1), Article 6.
[150] EDPB Guidelines 01/2020, v2.0, p. 12
[151] GDPR Article 9 (1)
[152] GDPR Recital 51, (1) and (2).
[153] GDPR Article 9 (2)
[154] EDPB Guideline 01/2020, v2.0, p. 15.
[155] GDPR Article 9 (1).

3.7.1 When is data concerning health?

A29WP describes scenarios when the data is concerning health in the Opinion of 2015, which advised on namely health data in apps and devices, which is relevant also for the new GDPR and processing of data from vehicles.

The first scenario is when the health data is "clearly medical data", which contains data of physical and mental health and generated in a "professional, medical context".[156] The second example of health data is if "the data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person". If sensor data of someone's heart rate, age and gender are stored together, but it is not in fact being used to draw a conclusion of the health, it is not "concerning health". Nevertheless, raw sensor data can be personal data, and even lead to revealing one of the other sensitive information that is prohibited.

If "conclusions are drawn about a person's health status or health risk", the data is also considered health data, regardless if the raw sensor data is considered as data concerning health. What determines if the data qualifies to be health data, is if the data are used to draw conclusions on the drivers' health or health risk. Data that, to begin with, merely reveals when a person uses the vehicle and where the person drives, can become such health data when, for instance, uses that data to draw a conclusion of the persons health. For instance, if a health insurer company retrieves data on the eye. The health insurer will then be a controller in the terms of the law, who must comply with the GDPR.

Data of eye movement can only be processed if the requirements of exception are fulfilled.[157] The processor must have explicit consent from the data subject that they can process the data of the driver's eye movement with the purpose of drawing health conclusions.[158]

There are other exceptions opening up for processing sensitive data pursuant to Art. 9 (2), where the most relevant to mention is where the national law in the state conciders processing of such data necessary "for reasons of substantial public interest" without otherwise come in conflict with data protection law.[159]

---

[156] A29WP 2015, Annex by letter – health data in apps and device, p. 2.
[157] Art. 9 (2) (a)
[158] See chapter 4 on terms of consent, and explicit consent under this thesis
[159] GDPR Article 9 (2) (g)

Many technologies in vehicles processing raw data that is or potentially can be health data increases road safety, for instance. Road safety is in the public interest, and even an issue emphasized by the European working groups who aims for less fatalities in the traffic on roads in Europe (Vision Zero). [160]

In many situations, especially if there is not a legitimate interest to process the data, the data controller will have to depend on the free choice of the data subject themselves: explicit consent[161], which is assessed further in chapter 4.

There are such massive amounts of data being generated in vehicles that in certain circumstances lead to sensitive data, or that the technology itself requires processing of sensitive data (for instance software recognizing eye movement or open the door with fingerprint). [162] Even more so in the nearest future, with more intelligent solutions and increasing automation of vehicles, generating more data in even bigger amount. Controllers must also be aware that some personal data, which at first sight is not sensitive, nevertheless has the potential to become sensitive data.[163]

The address of a hospital will isolated not identify a person, as it is simply a name of a street. However, when processed from a vehicle to an external cloud-based service, the address can reveal the location of the driver, which means that it will be personal data pursuant to Art. 4 (1).[164] Furthermore, those data can potentially reveal information about the health of the driver, for instance, if added with other data, such as eye movement data of the driver. That will mean that due to the circumstances, it must be considered as health data and be processed data pursuant to the rules of sensitive data in Art. 9 (1).

To answer the main question under this chapter, data processed in or from a vehicle is therefore subject to the GDPR if it is personal, meaning if it can reveal the identity of the driver. As most vehicles today are connected and process a huge amount of data, controllers of this data are most likely to process data that is identifying the driver, either alone or together with other data, also held by third parties. The controller of a vehicle must therefore assess whether the data

---

[160] COM (2011) 144 final, p. 10. See also COM (2018) 293 final, ANNEX 1
[161] Article 9 (2) (a).
[162] EDPB Guidelines 01/2020, v2.0, p.
[163] A29WP (2011) Advice paper on special categories of data, p. 6.; "data which by its nature contains sensitive information (…)", but also "data from which sensitive information with regard to an individual can be concluded".
[164] ART29WP 203 Opinion 03/2013, p. 46, and Schartum et al (2014) p. 127

they process can identify the driver, independent of whether the car has several drivers, because the information relating to the cars also relates to the person using the car. If the data can identify the user of the car, the data is personal, and the processing must be in accordance with the other rules of the GDPR. Furthermore, the controller must assess if the data is or can lead to sensitive information, to determine which ground should be applied to lawfully process the data.

4 The concept of consent

4.1 What is required of a consent as a legal ground to process personal data in vehicles?

Chapter two in the GDPR sets out the principles of processing personal data. According to Art. 6, the processor must have a valid lawful ground for processing the personal data.

There are six different alternatives to process personal data on a lawful ground in Art. 6 first paragraph. Only the first one, consent (a), is based upon a voluntarily action from the data subject. The other grounds are based on the necessity of different reasons: to comply with a contract (which is voluntary to begin with) (b); compliance with a legal obligation that the controller is subject to (c); protect vital interests (d); a task carried out in the public interest or in the exercise of official authority vested in the controller (e); and legitimate interest (f). The list is exhaustive, meaning that one of these listed grounds must apply.

Several solutions and services in vehicles process data from the car, for instance, lane assist, automatic break-system among others, provide improved road safety to different extents. In a sense, processing of such data is therefore "necessary" in order to protect the person. However, it is not necessary in the sense of "vital" interests as the Regulation means to cover. Another alternative that might apply, is if the data controller has "legitimate interests" to process the personal data. If they can`t show to a legitimate interest, the processing must be based on the consent of the data subject; the driver, and that is the topic for the following discussion.

The implication under the GDPR on this regard is among many: when a consent is possible or mandatory as a legal ground for the processing; what necessitates consent; and what conditions must be fulfilled to obtain the consent lawfully.[165] The most relevant lawful ground for

[165] A29WP 187 Opinion 15/2011, p. 3.

processing in the purpose of this thesis is, therefore, consent[166] and often in addition to a contract between the driver and, for instance, the seller of the car, which will be addressed shortly.

As technology develops and vehicles process data in an increasing speed and amount through built-in sensors, applications and other offline and online methods and software, this comes with a greater need to inform and build trust with the driver. This necessitates a firm and strict regulation to protect the drivers as data subjects, as well as to raise awareness of the extent of the processing and to give control and to decide over their own data.

In the following, the conditions of consent in general will be analyzed, with some practical aspects of complying with the examples of use of consent as a legal ground to process personal data in vehicles; and when it is not necessary or possible to use consent as legal ground.

The term "consent" is defined in Art. 4 (11) as

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The definition and terms of a valid obtained consent must be read in conjunction with the principles applied to the processing of personal data in general. Of particular importance in regards to consent is Art. 5, such as the principle of processing data lawfully, fairly and transparent (a); to only collect the data that are for specified, explicit and legitimate purposes (purpose limitation, letter b); and to only collect data on what is necessary (data minimization, letter c). These principles apply regardless of the lawful ground, which means that consent does not preclude the controller's duties laid down in the principles. EDPB highlights that consent "would not legitimise a collection of data, which is not necessary in relation to a specified purpose of processing and be fundamentally unfair".[167] The consent is therefore to be regarded as an additional condition for processing.

In addition, Art. 7 is of importance as it dictates "conditions for consent" and will be addressed where relevant for the understanding of "consent".

---

[166] But other can be relevant too, see A29WP 187, Opinion 15/2011, p. 8.
[167] EDPB Guidelines 05/2020 on consent, p. 5.

The starting point for the following analysis is the formulation in Art. 4 (11). The other relevant provisions, recitals and expert opinions will be addressed where its relevant and necessary to clarify the criteria of consent.

The provision in Art. 4 (11) states four cumulative criteria for the consent to be valid. It must be freely given, specific, informed, and unambiguous indication of the data subject's wishes.

4.1.1 Freely given consent

A freely given consent indicates that the data subject is in the power of deciding on his own whether he wants to give the controller permission to process his personal data.

The core of a "freely given consent" is that it is given voluntarily and of free will, necessitating that the data subject is in a position where they have autonomy to make a "real choice".[168]

As indicated in the Recital 43 (1), if there is a "clear imbalance between the data subject and the controller" it is "unlikely that consent was freely given", for instance, if the controller is a public authority.[169]

An employment relationship is mentioned as another example of an imbalanced relation by the A29WP, [170] where, in most cases, the employees will be under some kind of pressure under the employer when giving a consent. Here, the data subject does not have an actual real choice, as a consequence of being the weaker part. Therefore, it cannot be considered to be given "freely". An important note is that the provision and recital cover not only the situations mentioned, but all relations where there is a "clear imbalance".

However, the imbalance does not have to be of such clear character as an employment relation typically is. Even though the data subject might feel that they are choosing, the "choice" to not consent to the processing could lead to a consequence or other risks due to an undermining or imbalanced relation. If the relation leads to that, the data subject will "endure negative consequences if they do not consent", therefore, it will not be a valid consent.[171]

---

[168] A29WP 187, Opinion 15/2011, p. 9.
[169] GDPR Recital 43 (1)
[170] A29WP 187, Opinion 15/2011, p. 12, EDPB Guidelines 05/2020, p. 9, see also GDPR Article 88
[171] EDPB Guidelines, 05/2020 p. 7 and p. 9

Negative consequences can also be endured if there are conditions tied to the consent. In this regard, the criteria of consent must be read in conjunction with Art. 7 (4), which applies in general when personal data processing is based on consent as the legal ground. The provision states that in the assessment, "utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

The situation referred to is when the contract is tied to a consent that is not necessary for the contract to be fulfilled. If so, it is most likely not a "freely given" consent, namely due to the consent being a condition for the other terms of the contract. That may lead to a situation where the data subject can endure negative consequences of not consenting or not in fact have a real choice. Thus, it is not a freely given consent.

The additional consent cannot be a "requirement" to fulfill other parts of the contract, as it would mean that the controller do not separate the consents but rather "lure" the data subject to give consent. The guidelines clarify this difficult formulation, stating that "if consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given".[172]

For instance, if there is a contract between the controller and data subject of the purchase of a car. An additional service such as a road safety application in the car requires different operations of processing personal data, thus, an additional consent is required (see "specific" requirement below). If the controller says that the terms of the contract only applies if the buyer (data subject) consents to processing personal data in regards of the added service (value-added service), the consent is not valid as it is "tied" to another part of an agreement and therefore it is not valid.[173]

The A29WP held that "Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent".[174] This is from 2011, but this is highlighted by

[172] EDPB Guidelines, 05/2020, p. 7, paragraph 13
[173] As stated in GDPR Recital 43
[174] A29WP 187, Opinion 15/2011, p. 12

several Opinions, EDPB according to EDPB guideline[175]: This Opinion therefore still have relevance, whereas the guidelines expand and gives further clarification.

A criterion for the Art. 7 (4) to apply is that "the processing of personal data that is not necessary for the performance of that contract". If the processing is necessary to fulfill the contract, then consent is not the appropriate lawful ground to process the data.[176] The controller of the data must therefore assess whether the data is in fact needed, consequently in light of the contract as that lays the basis of what is necessary data for the "performance of that contract".[177] This assessment must take place before the processing starts.[178]

It is important to note that a contract should be used as a legal basis, rather than consent, if the controller carry out a core service, such as selling a car.[179] This depends on the context of the relation between the parties; the contract; and what is the purpose of the processing of the data. In that case, all the terms are laid down in a signed document establishing an agreement between the parties.

The criterion of "necessary for the performance of that contract" must be interpreted strictly.[180] There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.[181] For instance, the consent of processing personal data using the added service of additional service when buying a car is not necessary for the performance of the contract, namely buying the car. The consent of processing personal data pursuant to an additional service that is a choice of the buyer to begin with, is therefore not necessary for the performance of the contract, and consequently not valid.

Pursuant to art. 7 (4), the formulation "utmost account shall be taken" does not imply an absolute restriction. The interpretation by EDPB is that it is "considered highly undesirable"[182], which indicates that the provision operates as a warning to the controller to be aware of the risk they are taking by obtaining consent tied to other parts of the contract.

---

[175] EDPB Guidelines 05/2020, p. 9
[176] EDPB Guidelines 05/2020, p. 10, para 31
[177] EDPB Guidelines 05/2020, p. 10, para 29
[178] A29WP 187 Opinion, 15/ 2011, pp. 30-31, EDPB Guidelines 05/2020, p. 20.
[179] EDPB Guidelines 01/2020, v2.0, p. 13
[180] A29WP 217 Opinion 06/2014 on the notion of legitimate interest of the data controller, p. 16-17
[181] EDPB Guidelines 05/2020 on consent, p. 10
[182] EDPB Guidelines 05/2020 on consent, p. 10

However, in Recital 43 (second paragraph), the same situation is addressed, but with the formulation "Consent is presumed not to be freely given(...)."

If consent is given in this situation, it is "presumed" to be not freely given. The word "presumed" is a stronger indication of that the consent cannot be considered as freely given, than that the controller must take "utmost account". However, a recital is not legally binding, and the provision should consequently have more legal weight. In that sense, the formulation in Art. 7 (4) appears to be more of a strict encouragement to controllers to avoid this, as it most likely will be an invalid consent.

In the newest guidelines, the EDPB holds that "Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary", and that "the two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred."[183]

Article 7 (4) did not exist in the old Directive. However, it is a codification of the understanding of the rules on consent set out by A29WP.[184] According to the AG in the Opinion of Case of Planet49, the provision codifies a "prohibition on bundling"[185] already established from the understanding of the Directive, but that it is "not absolute in nature".[186] Both AG and the Court of Justice leaves it up to the national court to solve.

The history of the provision therefore implies that the interpretation of "outmost account should be taken" in Art. 7 (4) is not absolute, but as the Courts most often interprets in light of recitals and, to a big extent, guidelines and opinions, as they are the experts in the field, the article provides better protection as a result of being stated explicitly in the Regulation.

While it is not certain why the legislators did not implement the absolute prohibition, it might be to show caution as there can be situations where this might not be problematic, but with the present formulation it will protect those who did not have a real choice, as their consent was bundled and depending on other terms. Nonetheless, it is safe to assume that in light of the duty of documentation and burden of proof on the controller set out in Art 7 (1), it is difficult for the controller to prove that consent was given freely by the data subject if it is tied to a

[183] EDPB Guidelines 05/2020, p. 10 (para 26)
[184] EDPB Guidelines 05/2020, p. 11.
[185] C-673/17, Planet49 (AG Opinion), para 97
[186] C-673/17, Planet49 (AG Opinion), para 98

contract as mentioned in Art 7 (1) and recital 43. This is also related to that the consent must be separate, which is relevant especially under the criteria of "specific" consent.

4.1.2 Specific consent

Pursuant to Art. 4 (11), consent must be "specific". This indicates that the consent must describe what the consent relates to and be detailed regarding what the data subject is consenting to. The latter implies that the consent must be specifically and sufficiently "informed" which is the next criterion. These two criteria are therefore naturally linked to each other.

Recital 32, (4) and (5) explains that "Consent should cover all processing activities carried out for the same purpose or purposes". When the processing has multiple purposes, consent should be given for all of them.

According to the proposal of the previous Directive, the meaning of the criterion "specific" was that "it must relate to a particular data processing operation concerning the data subject carried out by a particular controller and for particular purposes".[187] The formulation in GDPR is similar to the provision in the previous Directive, which makes this relevant today. The term "specific" requires that the data subject must be asked consent to individual types of data processing: one consent for collecting location data; and another consent for sharing the data with third parties.[188]

To comply with GDPR, the controller of the data processed from a vehicle must design the consent form on a detailed level on what the personal data will be used for. A general consent stating that the data subjects accept processing of personal data is not sufficient. [189] This criterion must be read in conjunction with GDPR Art. 6 1 a), which requires that the consent is given for "one or more specific purposes".

If a data controller of the personal data processed from the vehicle obtained consent of processing location data for the purpose of providing a navigational service to the driver, the controller cannot use that location data for any other purpose than that navigational service that was set out in the consent. Due to this, the controller might see the possibility of a more general consent with a more general purpose, to save time and argue that the consent covers a variety

[187] COM(92) 422 final, p. 12.
[188] GDPR Article 28 and EDPB guidelines 01/2020 on connected vehicles v2.0 p. 20, para 93.
[189] A29WP 203 Opinion 3/2013, p. 16.

of operations, i.e., "for improving users-experience."[190] However, this is not accepted by the GDPR, as it is not sufficiently specific and would lead to lack of control for the data subject.[191] Improving user experience sounds great for the driver at first sight, as it implies more user - friendly service and driving. But would that consent allow the controller to share that location with third parties? That would be difficult for the data subject to know, risking that the controller can misuse the data and argue that the data subject consented to this, as sharing with another party can improve the user experience. Therefore, a new consent must be obtained from the driver, even though it is the same data, as the processing will be for a different purpose.

4.1.3 Informed consent

Informed consent implies that the controller has an obligation to give adequate information about what the data subject consents to. As mentioned above, the processing of the data must be specific on the purpose of the processing.

Further, the GDPR dictates minimum requirements for the consent to be considered as sufficiently informed. Firstly, the data subject must be aware at least of the identity of the controller and the purposes of the processing for which the data are intended.[192] The type of data that will be collected and used must also be informed.[193]

The requirement of informed consent must be read in conjunction with the data subjects right to withdraw consent under Art.7 (3). This right follows from the core of giving consent to start with, as it is the free will of the data subject. Point three of the provision states that "Prior to giving consent, the data subject shall be informed thereof."[194] This implies that, in addition to holding a right to withdraw the consent, the data subject also holds a right to be informed of that right before he gives the consent. Otherwise, the data subject might not be or become aware of his right and the right is illusionary[195]. It must therefore be considered as one of the minimum requirements for the information.

The next element of information that must be provided in the consent follows from Art. 22 (2) (c). The first paragraph of the provision gives a right for the data subject "not to be subject to a

---

[190] EDPB Guidelines 05/2020 on consent, p. 14, footnote 30; and A29WP 203 Opinion 3/2013 on purpose limitation, p. 16
[191] EDPB Guidelines 05/2020 p. 14
[192] GDPR Recital 42 and EDPB Guidelines 05/2020, p. 15
[193] A29WP 187, Opinion 15/2011 on the definition of consent, pp.19-20
[194] GDPR Article 7 (3) third point
[195] EDPB Guidelines 05/2020, p. 15

decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[196] However, one of the exemptions from this is if the decision is based on the data subject's explicit consent.[197]

The criterion of "explicit" consent is stricter than the conditions of consent set out in Art. 4 (11), because it is an exception to the data subjects right. If such processing is relevant, the information must be so clear and well informed that there is no doubt that the data subject is aware of what he is consenting to.[198] For the purpose of this thesis, it is sufficient to address that the controller must obtain an explicit consent to be allowed to make decisions based solely on automated processing, including profiling.[199]

The last requirement for a consent to be considered sufficiently informed is only relevant if the controller or processor wants to "transfer personal data to a third country or an international organisation"[200], "in the absence of an adequacy decision pursuant to Article 45 (3) or of appropriate safeguards pursuant to Article 46". If that is the case, one of the alternatives for such transfer is that the data subject consents "explicitly", "after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards".

The provisions of transfer to third countries will not be assessed further, but it can be noted that this is merely an element of information that is required if that is relevant for the consent which the controller wish to obtain from the data subject. What is important to note however is that the criterion of "explicit" is stricter than the criterion of consent, similar to the previous element of information.[201]

These are only minimum requirements for the requirement of informed consent under the definition in Art. 4 (11)[202]. As mentioned, the principles still apply as conditions for all the different stages in the process of data-processing. For a controller of data collected by vehicles, that will mean that a consent is not worth anything if what is requested of processing is not in

---

[196] GDPR. Art. 22 (2)
[197] GDPR Art. 22 (2) (c)
[198] See also chapter 7 where the criterion of "explicit consent" is analyzed more extensively
[199] GDPR Art. 4 (4)
[200] Pursuant to chapter GDPR Chapter 5
[201] The requirement "explicit consent" is addressed in regards of consent when processing sensitive data in GDPR Chapter 7.
[202] EDPB Guidelines 05/2020 on consent, p.15, p.16.

compliance with the principles. If the driver consents to process data on geolocation, it is not valid if the controller collects location data that is not relevant for the purpose for which they are processed, as that will be a breach of the principle of data minimization. [203]

The EDPB addresses a particular challenge related to the controllers obligation to give sufficient information, where the "data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users." to avoid "information asymmetry."[204] Vehicles may have different users and drivers under one owner or when the car is sold to a new owner. This may impose an issue for the controller to give adequate information. The vehicle owner is likely to receive the information, as they are the easiest for the controller to inform and reach out to, but how can the controller ensure that all the drivers or the new drivers are provided with the information? The EDPB points to that this issue imposes "a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights."[205] Controllers of data processed in and from vehicles therefore meet some complex problems that must be solved in order to comply with the GDPR while offering practical services. This is one of many practical examples illustrating that the controller must balance conflicting considerations, naturally where the protection of the individual must take precedence over the stakeholders and other controller, as this will cause a slower technological development in various degrees, and, for instance, hinder the increase of road safety and other technologies that both Member States and their citizens can benefit from.

4.1.4 Unambiguous indication of the data subject's wishes

The consent is only valid if it is an "unambiguous indication of the data subject's wishes, by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her". From the reading of the provision it appears more practical to treat "unambiguous indication" and "by a statement or by a clear affirmative action" together, instead of independent requirements.[206]

[203] GDPR Art. 5 (1) (c)
[204] EDPB Guidelines 01/2020, p. 13.
[205] EDPB Guidelines 01/2020, p. 13.
[206] This is also assumed to be in line with EDPB Guidelines 05/2020, p. 18.

The ambiguous indication of the wishes must be made *by* a statement or clear affirmative action. Recital 32 reads:

> "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."

This is similar to the provision but elaborates on the general understanding of consent. Also, instead of the data subjects wish to consent, the term "agreement" is used.

Neither unambiguous nor statement or clear affirmative action was mentioned in the definition of consent in the previous Directive,[207] but "unambiguous" was mentioned as a criterion for making data processing legitimate, which required that the data subject "unambiguously" gave his or her consent.[208]

In the present GDPR, "unambiguous" is moved to the general definition of consent. According to the Advocate General in the recent case of Orange Romania, this is merely a move to make it a part of the more general definition in GDPR Art. 4.[209] As a result, the additional criterion dictate a stricter requirement of consent in the GDPR. This conclusion was also drawn from the Advocate General Szpunar in the Opinion of Case C-673/17.[210]

The wording of "unambiguous indication" implies that the data subjects perform an action that is undoubtfully "indicating" that they agree to the controller processing the data on the terms and information based in the consent.

It is clear from the recital that it does not require a written statement, which expands the notion of what is an unambiguous indication and clear affirmative action. It is sufficiently clear if it is oral, or by electronic means in written form. The latter raises implications to what is necessary to be a clear and affirmative action in the sense of electronic means.

---

[207] Directive 95/46, Article 2(h)
[208] Directive 95/46, Art. 7 (a), and Art. 26 (1) as a criterion to permit transfers to third countries.
[209] C-61/19, Orange Romania, AG Opinion, para 68
[210] C-673/17, Planet49 (AG Opinion), para 70, also underlined in C-673/17, Planet 49, para 61.

In a recent case from the European Court of Justice, the Court took the same view on the criterion of "unambiguous" as the Advocate General in the Opinion, demonstrating that it must be understood in light of the data controllers' burden of proof in Art. 7 (1).[211] That provision provides that the controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data. A written statement is certainly a more unambiguous indication and a clear act of that the data subject agrees to the processing, than an oral. However, this is not a requirement and it is up to the data controller to provide a consent in which they have sufficient "proof".

The recital is clear on this, as they suggest that the electronic means can be the tick of a box, for instance, when visiting a website, provided that it is informed and gives the data subject a clear choice.[212] On the contrary, pre-ticked boxes are expressively excluded. This is clarified through recital 32 (2) and jurisprudence[213] through European case law. Since the boxes are already ticked off, it is not the data subject who actively performs an indication of a wish to consent, therefore it is not "unambiguous".[214]

Such pre-ticked box is an example of a presumed consent, which before the GDPR was applicable and likely still in use by many controllers. Among many examples is the use of cookies to adapt the ads in the website.[215] In vehicles however, it is possible to obtain consent through, for instance, the infotainment system in the car, where the navigational system and radio is, along with various applications and additional choices of services. Some of the data needed for the use and function of the vehicle might not be personal data or can be processed in terms of being essential for the function of the car, and thereby laid down in the contract as a valid legal ground.[216] But for some value-added services that are non-essential for the driving of the car, or for operations or updates of software which change the purpose or require updates after the purchase of the vehicle, consent must be obtained before the processing of personal data.[217]

---

[211] C-61/ 19, Orange Romania, para 42, AG Opinion para 56.
[212] Recital 32 (2), conditioned the other requirements are also fulfilled
[213] C-673/17, Planet49
[214] C-673/17, Planet49, para 52, and AG Opinion para 60, and Recital 32.
[215] EDPB Guidelines 05/2020, p. 12.
[216] EDPB Guideline 01/202, v2.0., p. 9
[217] A29WP 187 Opinion 15/2011, pp. 30-31, EDPB Guidelines 05/2020, p. 20.

One issue that might occur under the GDPR and appliance to vehicles is if the consent must be obtained for each time an operation of processing is ran in the car. Since the GDPR requires freely given, specific, informed and unambiguous consents, and the controller is required to, among other duties, keep the data accurate and up to date,[218] it would be reasonable to argue that a consent must be given each time the vehicle is in use.

The A29WP addressed this under the Directive, stating that "It should be sufficient in principle for data controllers to obtain consent only once for different operations if they fall within the reasonable expectations of the data subject.[219] This means that, if it is the same driver, it is not needed to obtain consent each time if it is the same operation with the same purposes. For instance, if the driver consents the processing of location data once, the next time they drive, the controller can process this data based on the consent given previously. An important note here is however that the driver as a data subject can at any time withdraw his consent pursuant to article 7 (3), and that the other requirements of processing data must be fulfilled, as mentioned under the assessment of the other criteria of consent.

Another implication is if the consent must be obtained for each time the car is used, for instance, in the vehicles where the driver cannot "communicate" to the car who is driving. The driver can be changed from time to time. If consent is not obtained each time, the controller can risk that a previous given consent of driver A to process his location data, later is used as the legal ground for processing data which is in fact relating to another driver B. Driver B never gave consent to the processing of that data, and, as a consequence, none of the requirements for consent are fulfilled.

An important note here is Article 25 GDPR, which gives the controllers a duty to "implement appropriate technical and organisational measures" by the design (1) and by the default (2) of the technology applied to integrate the necessary protection of the data. The issue mentioned must, therefore, be solved already on the design stage and be a part of the technology provided in the vehicle.

Many car manufacturers and providers have an "independent" mobile application linked to the different users, which might enable them to obtain consent through the user profile on the

[218] GDPR Art. 5 (d) e.g.
[219] A29WP 187, Opinion 15/2011, p. 17

phone.[220] Many cars also have the technology to recognize who sits in the seat and can thereby apply the standard adjustments for that person, and different users on the infotainment system to adapt to who is driving the car. The issue addressed could therefore perhaps be solved by, for instance, connecting the driver to a profile linked only to one natural individual. It is important for the controllers to be aware of this issue, especially because some of the applications linking to a person only gives the possibility to steer the car on a limited administrative level, or that the application is not linked to the car on the level of communicating to the car who is driving and then decide what software or value-added services to run based on that.[221]

A strict interpretation of the criteria for consent under the GDPR provides better protection for the data subject and is fundamental to safeguard the privacy of the data subject. It enables the driver to have better control over the data and leads to more transparency between the controller and data subject. On the other hand it creates some challenges for the controller to ensure that the consent is valid at all times, especially for newer technologies that rapidly changes, or more parties having interest in the processing, such as insurance companies, other service providers among others. Some technologies might change during the time of the contract of the car, or new software updates might be necessary, which changes the terms or purposes of the processing. This, among many other factors, makes it necessary to constantly obtain new consents from the data subject which can require a lot of resources from the controller. In this regard, it is the opinion of the EDPB that "The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects." [222]

On the hand of the data subject, this can lead to consent fatigue and worst case that data subjects accept processing of their personal data in a wider range than intended, due to the high frequency of consent requests. This is unfortunately the reality for many data subjects, and instantly decreases the level of protection because it requires too much time and sometimes also knowledge, to familiarize themselves with the risks and consequences of the processing. Strict conditions of consent can therefore come to the subject's disadvantage. The protective effect of

[220] For instance Mercedes-Me- application connected to the individual user, https://www.mercedes-benz.no

[221] For more elaborations on this, EDPB Guidelines 01/2020, v2.0, p. 4

[222] EDPB Guidelines 05/2020, p. 5

rules of consent appear to be negligible in this sense. This has been discussed by the EDPB[223] as well as the Commission for the future work of implementing the GDPR and ensuring sufficient protection for the individuals. All responsibility should and can therefore not lie on the controller alone.

4.2 On what legal ground can the controller process sensitive data?

The GDPR regulates the conditions for processing personal data and some of the data processing in vehicles can be special categories of data or "sensitive data" (as mentioned under chapter 3.7). Already, there are massive amounts of data being generated in vehicles that in certain circumstances lead to sensitive data, or that the technology itself requires processing of sensitive data.[224] With more intelligent solutions and increasing automation of vehicles in the nearest future, the amount of data will increase extensively. The conditions for consent as discussed above (chapter 6) is general and applies to all data. Special categories of data are also personal data, but on such a level that it requires stricter protection. Consequently, more rigorous rules for how and on what terms a data controller can process such data are established under the GDPR. An important matter is that consent as a lawful ground for processing special categories of data are an exemption of the main rule set out in the GDPR that such processing is prohibited.[225]

Processing of sensitive data requires an additional criterion, namely that the data subject gives an "explicit" consent pursuant to Article 9 (2).

What precisely a requirement of "explicit" consent entails, is one of the controversies under the GDPR. [226] Lines can be drawn to the criterion of "unambiguous" in Art. 4 (11), which already lays the basis of a high threshold for the consent. Considering that the processing of these data necessitates higher protection, explicit consent must be interpreted more rigorously than of "unambiguous" consent. A clear and affirmative act is still a precise description of the stricter requirement. However, "indication" is not sufficient, as indication can lead to more varieties of what can be accepted as a clear and affirmative "unambiguous consent". An explicit consent must therefore not only give a clear indication. To tick of a box can therefore be argued to not

[223] EDPB Guidelines 05/2020, p. 19.

[224] EDPB Guidelines 01/2020, v2.0 p. 4; "software recognizing eye movement"
[225] GDPR Art. 9 (1), and Chapter 3 in this thesis
[226] EDPB Guidelines 05/2020, p 4-6

be sufficient, as it is not explicitly ensuring that the data subject actually agreed to the risks that the processing of sensitive data comes with.

Again, written and signed consent could ensure an explicit consent to a greater extent and provide certainty for the controller. Even though an oral statement can make difficulties for the controller on such matter, a written consent is not a requirement for explicit consent either.[227] Due to the extent of electronic data processed in the informational society and the fact that a lot of the consents must be given without physical appearance, written and signed consent would be practically challenging.

The guidelines suggest that a telephone conversation could provide a sufficient explicit consent, if for instance recording the part where the data subject gives the consent, or confirm by pressing a button, or orally after the controller repeats to confirm that it is correct.[228]

Another method of obtaining explicit consent that is more relevant in vehicles where the controller and data subject seldom interact with each other, is through the vehicle or the application linked to the person using the vehicle, by a two-stage verification. The first stage could, for instance, be that the data subject receives a message about the required information of the purpose and dataset that data controller asks to process, and the data subjects agrees. This message could be given on the app connected to the car and that user. The second stage is that the data subject clicks a link or a code, preferably to another platform to safeguard that it is the correct natural person, that he or she confirm the given consent. This step could be that the driver receives an e-mail or SMS from the controller. These steps leave no doubt as the data subject is consenting by going through not only one but two verifications steps, requiring that the data subjects is actively expressing his agreement to processing sensitive data about him or her, which makes it sufficiently explicit.[229]

The requirements of "explicit consent" are in that sense stricter than the processing of personal data, since it is an exception from a prohibition. The controller must consequently be thoroughly when obtaining the consent.

---

[227] EDPB Guidelines 05/2020 on consent, p. 21.
[228] EDPB Guidelines 05/2020 on consent, p. 21
[229] EDPB Guidelines 05/2020 on consent, p. 21

However, it must be within the frames of what is practically possible to obtain for the controller. After all, if the data subjects wish to agree, they must have the free choice to consent. However, it is also here up to the controller to find the technical mechanisms that is in compliance with the law.

Nevertheless, a consent is not a lawful ground for processing, if the "Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject".[230] If national legislation prohibits the processing of the data in question, it is not up to the data subject to choose and consent will not enable the processing.

Finally, the obtaining of a valid consent does not release the controller from processing the data in accordance with the overarching principles on all stages; lawfully, fairly and in a transparent manner, and it must still be limited to only what is for specified purposes; be limited to what is necessary; be accurate; be stored for no longer than necessary; and be kept securely and confidentially.[231]

5 Final remarks

In this thesis, I have analyzed the criteria of "personal data" and "consent" under the GDPR, mainly with focus on the processing of data in and from vehicles.

The analysis shows that the scope of "personal data" is wide but limited to what is "reasonable" that the controller takes into account. In today's increasingly digital society, the technology makes the person identifiable in most cases. The notion of "another" person who must be considered is very wide, though limited to who is of relevance to that processing. The group of relevant actors in the processing of personal data related to vehicles is increasing, as more industries are involved. Even though the criteria are of vague character and with many factors to be considered, the assessment illustrates that the criteria are dynamic and a functioning tool to give protection, adjusted to the present developing. It is however few examples in jurisprudence that data is not personal. The CJEU and EDPB emphasizes a broad notion and the jurisprudence seems to go in the direction of an even wider scope as a consequence of

[230] GDPR Article 9
[231] GDPR Article 5, EDPB Guidelines 05/2020 p. 5.

information society requiring more data from individuals and information being available and easily accessed.

A valid consent requires that it is freely given and a high level of information. The rules are strict, and it is the controller's responsibility to properly document that the requirements for consent are fulfilled, naturally to provide better protection for the data subject. Some of the data may also be sensitive, either by its nature or only in certain circumstances, in which the GDPR establishes even stricter requirements to process the data in accordance with the law, namely explicit consent. This requires that controllers who process data from vehicles, such as equipment manufacturers, service providers, developers, among others, must have good knowledge of whether the data processed is sensitive data or not, hereunder what factors are determining if the data is or can be sensitive data and what to keep in mind to ensure lawful processing.

As pointed out and illustrated through this thesis, the GDPR can be difficult to navigate through, in addition to being vague and fragmentary. For many entities, this requires legal expertise or a lot of time. In addition to risk huge fines, the companies not ensuring compliance with GDPR can lose the trust of the users and customers. The strict requirements are great in the legal aspect but can directly hinder technological development.

Compliance with GDPR can therefore be challenging, especially for the small enterprises without a legal department or resources of both technology and law. [232] This is likely not the case for most vehicle manufacturers but can be the case for smaller developers or other actors in the processing, who might lose competition power due to the required amount of time and resources needed to comply with the GDPR. Nevertheless, the GDPR also provides practical tools such as DPIA and thoroughly guidelines, as well as practical tools provided for by Data Protection Authorities on national level.[233] It appears that the appliance of the GDPR on most areas is practically possible to a great extent,[234] considering the Commissions statements in newer reports.[235]

[232] COM (2020) 264 final, p. 9.
[233] COM (2020) 264 final, p. 9
[234] COM (2020) 264 final, p. 4
[235] COM (2020) 264 final, p. 2

However, this thesis has addressed several norms under the GDPR which may be difficult for the controllers of data processed in vehicles to fulfill. The criteria of giving a sufficiently informed consent to the drivers as well as strict requirements for consent in general meet some practical implications. Due to the high frequency of requests controllers must obtain to comply to the GDPR the protection can be argued to be illusionary protection as data subjects will suffer from consent fatigue. It is therefore a valid argument to state that the concept of consent is a work still in motion.

The European legislators are clear in that it is up to those who process and controls the data to align the technology to the GDPR, such as implementing suitable mechanisms for obtaining consent to process data in and from vehicles, to ensure self-determination and control of the data subjects. Some practical tools and help are provided for already, and controllers must act and undertake action to comply.

The work of the Data protection agencies in the Member States and the expert groups is therefore important in the following years, to give guidance and ensure that compliance of GDPR is realistic, as it is still a "new" regulation. Without focus on the practical implementation of the Regulation, the consequence are, more importantly, that the protection of the individuals is not efficient, especially on the field where data is processed in high amounts and technology changing rapidly, such as connected vehicles.

It must therefore be a goal for the European legislators and the bodies on international and national levels to make the GDPR as practical as possible, so that development is not hindered, and the protection of individuals personal data is not illusionary. According to the EDPB, it is a focus in the following years to continue the work on this to meet the full potential of GDPR. [236] This is necessary to ensure a practical and realistic compliance and implementation the following years to safeguard and realize the fundamental individuals right of data protection as committed to and enshrined in European legislation.

[236] COM (2020) 264 final, p. 13-14

Works cited

European Union Regulations and Directives

Regulation 2016/679, GDPR	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. OJ L119/ 1. , 4.05.2016, p. 1-88.
Regulation (EU) 2018/1807	Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union - OJ L 303/59, 28.11.2018, p. 59–68.
Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281/31 P, 23.11.1995, p. 31-50.
Directive 2007/46/EC	Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive). OJ L 263/1, 9.10.2007, p. 1-160.
Directive 2002/58/EC	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), L 201/37, 31.07.2002, p. 37-47.

International agreements and treaties

ECHR (1950)	European Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950
EEA Agreement (1994)	The Agreement on the European Economic Area, 1 January 1994, OJ No L 1, 3.1.1994.
TFEU (1957)	The Treaty on the Functioning of the European Union (TFEU), Rome, 25.3.1957. Consolidated version, Official Journal C 326/13, 26/10/2012 P. 0001 – 0390
CFREU (2012)	European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
Convention 108 (1981)	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Strasbourg, 28/01/1981.

Communication from the Commission to the European Parliament and the Council

COM(92) 422 final	(COM(92) 422 final—SYN 287) Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data (European Commission)
COM (2011) 144 final	COM (2011) 144 final, WHITE PAPER Roadmap to a Single European Transport Area –

	Towards a competitive and resource efficient transport system, Brussels, 28.3.2011.
COM(2012) 11 final	COM(2012) 11 final 2012/0011 (COD) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 , 2012/0011 (COD).
COM(2014) 442 final	COM(2014) 442 final, Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, Towards a thriving data-driven economy, Brussels, 2.7.2014
COM(2018) 293 final	COM(2018) 293 final, Strategic Action Plan on Road Safety, Brussels, 17.5.2018, ANNEX 1
COM(2020) 264 final	(COM(2020) 264 final; 24 June 2020 Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020.

The Article 29 Data Protection Working Party

A29WP 136 4/2007	01248/07/EN Opinion 4/2007 on the concept of personal data, 20 June 2007; WP136
A29WP 187 15/2011	01197/11/EN Opinion 15/2011 on the definition of consent, 13. July 2011; WP 187

A29WP 199 08/2012	01574/12/EN Opinion 08/ 2012 Providing Further Input on the Data Protection Reform Discussions, 5 October 2012; WP 199
A29WP 203 3/2013	00569/13/EN Opinion 3/2013 on purpose limitation, 2 April 2013; WP 203.
A29WP 217 06/2014	844/14/EN Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, WP 217
A29WP 2011	444105-20/04/2011 Advice paper on special categories of data ("sensitive data") 20.04.2011
A29WP 2015	Annex by letter – health data in apps and devices, 05.02.2015

European Data Protection Board

EDPB Guideline 05/2020	European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020
EDPB Guidelines 07/2020	European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0., 2 September 2020
EDPB Guidelines 01/2020 v2.0	European Data Protection Board, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, 9 March 2021

European Court of Justice

C-101/01 Lindqvist	C-101/01 *Bodil Lindqvist* (2003) ECLI:EU:C:2003:596

C-582/14 Breyer	C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* (2016) ECLI:EU:C:2016:779
C-210/16, Wirtschaftsakademie,	C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (2018) ECLI:EU:C:2018:388
C-210/16 AG Opinion	C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (2018) Opinion of the Advocate General, ECLI:EU:C:2017:796
C-434/16 Nowak	C-434/16 *Peter Nowak v Data Protection Commissioner* (2017) ECLI:EU:C:2017:994
C-434/16 Nowak, AG Opinion	C-434/16 *Peter Nowak v Data Protection Commissioner* (2017), Opinion of Advocate General, ECLI:EU:C:2017:582
C-673/17 Planet49	C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH* (2019) ECLI:EU:C:2019:801
C-673/17 Planet49, A.G Opinion	C-673/17 *Planet 49*, Opinion of the Advocate General (2019) ECLI:EU:C:2019:246
C- 61/ 19, Orange Romania	C- 61/ 19, *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP),* (2020) ECLI:EU:C:2020:901
C-61/19 Orange Romania AG Opinion	C- 61/ 19, *Orange România* (2020) Opinion of Advocate General, ECLI:EU:C:2020:158

C-311/18 Schrems II	C-311/18 Data Protection Commissioner V Facebook Ireland Ltd, Maximillian Schrems (2020) ECLI:EU:C:2020:559
Case C-131/12 Google Spain	C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014) ECLI:EU:C:2014:317
T-670/16, Digital Rights Ireland	T-670/16 Digital Rights Ireland v Commission, Order of the General Court (2017) ECLI:EU:T:2017:838

European Court of Human Rights HUDOC

Rotaru v. Romania (2014)	*Rotaru v. Romania* [GC] no. 28341/95
Satakunnan and others v. Finland (2017)	*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13

Guides

ECHR guide on Article 8, 31.12.2020	European Court of Human Rights (2020), Guide on Article 8 of the European Convention on Human Rights- Right to respect for private and family life, home and correspondence, 31.12.2020. URL: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

Norwegian law

The Personal Data Act (2018)	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger

Norwegian preparatory work

NOU 1975:10 — NOU 1975:10 (1975) Offentlig persondatasystem og personvern. Justis og politidepartementet.

NOU 1997:19 — NOU 1997:19 (1997) Et bedre personvern - forslag til lov om behandling av personopplysninger. Justis- og politidepartementet

Ot.prp. nr. 92 (1998-1999) — Ot.prp. nr. 92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven) – English: Preposition to the Odelsting

Literature

Bygrave, 2014 — Bygrave, L. A.; (2014) *Data Privacy Law: An International Perspective*, Oxford University Press.

Bygrave and Tosoni, 2020 — Bygrave, L.A & Tosoni, L. (2020). Article 4(1): Personal data, In Kuner, C, Bygrave, L.A. & Docksey, C (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press. ISBN 9780198826491. Commentary on Article 4(1), p. 103 – 115.

Lenaerts and Gutierrez-Fons, 2014 — Lenaerts, K.; Gutierrez-Fons, J. A. (2014). To say what the law of the eu is: Methods of interpretation and the european court of justice. Columbia Journal of European Law, 20(2), 3-[vi]

Schartum and Bygrave, 2011 — Schartum, D.W., Bygrave, L.A., (2011) Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger, (2. utgave) Fagbokforlaget, Bergen.

Schartum et al., 2014 — Schartum D. W., Hannemyr G., Tranvik T. (2014) Use of personal locationdata by the police, CompLex 1/2014, Senter for rettsinformatikk, Akademika, Oslo

Schartum, 2020 — Schartum D. W., (2020) Personvernforordningen, en lærebok, Fagbokforlaget, Bergen.

Skoghøy, 2018 — Skoghøy, J. E. A., (2018) Rett og rettsanvendelse, 1. utgave, Universitetsforlaget

Articles

Bygrave, 2015 — Bygrave, L., (2015) *Information Concepts in Law*, Oxford Journal of Legal Studies, Vol. 35, No. 1 (2015), pp. 91–120. DOI:10.1093/ojls/gqu011

Dalla Corte, 2019 — Dalla Corte, L. (2019) *"Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law*", European Journal of Law and Technology (2019), vol 10(1), n. 1, may. 2019. ISSN 2042-115X.

Purtova, 2018 — Purtova, N. (2018) *The law of everything. Broad concept of personal data and future of EU data protection law*, in Law, Innovation and Technology, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176