Exploring data protection challenges of automated driving

Vellinga, N. E.; Mulder, Trix

Published in:
Computer Law & Security Review

DOI:
10.1016/j.clsr.2021.105530

Publication date:
2021

COMPUTER LAW & SECURITY REVIEW 40 (2021) 105530

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

Exploring data protection challenges of automated driving

Trix Mulder[a,#], *Nynke E Vellinga*[b,#,*]

[a] *PhD researcher at the Faculty of Law and the Faculty of Medical Sciences of the University of Groningen and part of the Security Technology and e-Privacy Research Group, The Netherlands*

[b] *Postdoc researcher at the Faculty of Law of the University of Groningen and part of the Security Technology and e-Privacy Research Group, The Netherlands*

ARTICLE INFO

Keywords:
Data protection
GDPR
Automated driving

ABSTRACT

With the increase in automation of vehicles and the rise of driver monitoring systems in those vehicles, data protection becomes more relevant for the automotive sector. Monitoring systems could contribute to road safety by, for instance, warning the driver if he is dozing off. However, keeping such a close eye on the user of the vehicle has legal implications. Within the European Union, the data gathered through the monitoring system, and the automated vehicle as a whole, will have to be collected and processed in conformity with the General Data Protection Regulation. By means of a use case, the different types of data collected by the automated vehicle, including health data, and the different requirements applicable to the collecting and processing of those types of data are explored. A three-step approach to ensuring data protection in automated vehicles is discussed. In addition, the possibilities to ensure data protection at a European level via the (type-) approval requirements will be explored.

* Corresponding author.
E-mail addresses: t.mulder@step-rug.nl (T. Mulder), n.e.vellinga@rug.nl (N.E. Vellinga).
N.E. Vellinga, PhD: University of Groningen, Faculty of Law, Department of European Law, PO Box 716, 9700AS Groningen, The Netherlands. Tel: +31503635603.

https://doi.org/10.1016/j.clsr.2021.105530

1. Introduction

How would you feel if your car knows your heart rate, or counts the number of times you blink? With the emergence of automated vehicles, the number of sensors keeping an eye on you, the user of the vehicle, will increase. The car will know if you are able to take back control of the wheel, or when a traffic situation makes you break into a sweat.[1] Sounds disturbing?

The important role sensors and cameras that detect a user's physical state can play for road safety has been signalled by stakeholders, but so have privacy concerns. For instance, the EU Member States already mentioned in the 2016 Declaration of Amsterdam on cooperation in the field of connected and automated driving[2] the right to privacy and data protection, and they agreed to a joint agenda which, amongst others, should ensure privacy and data protection.[3] In this contribution, we will take a closer look at the privacy concerns regarding data on the health of the user of the vehicle, driving on public roads within the EU. If through sensors and cameras the vehicle collects information on the heart rate of the user, its eye movements and other indicators of the physical and mental state of the user, can these data be stored by the operator of a fleet of automated vehicles and perhaps sold to, for instance, the health care insurer of the user? Is it allowed to combine these data with other data, such as the location of the vehicle and the time of day, and sell it to a company wanting to advertise their restaurant to the user? We will explore the possibilities and restrictions of the processing and use of these data under the EU General Data Protection Regulation (GDPR). The GDPR is a general data protection instrument that is technology neutral and applies to data collected by automated vehicles.[4] In addition to setting legal boundaries, the GDPR also offers inspiration for how to deal with data protection issues in this technologically enriched world. This inspiration serves as a starting point for a novel three-step approach applied to automated vehicles on the integration of data protection in automated vehicles. This approach will ensure that in the future, one no longer has to worry about the protection of personal data when using an automated vehicle. First, the different levels of automation and the different possibilities of collecting health related data through the sensors and cameras are discussed. After an introduction to the GDPR, we will explore what the possibilities and limitations are of collecting and using data related to the physical state of the user of the automated vehicle. By doing so through a use case, we will identify the legal consequences under the GDPR of collecting data concerning health, also referred to as health data, via sensors and cameras in automated vehicles.

2. Levels of automation

The Society of Automotive Engineers (SAE) has described six different levels of driving automation.[5] SAE Level 0 and Level 1 vehicles are on the road today. These vehicles have at most a system that can control either the longitudinal or lateral motion of the vehicle.[6] An SAE Level 2 vehicle is more advanced, but there are already some SAE Level 2 vehicles on the road.[7] The number of SAE Level 2 vehicles is expected to increase substantially in the near future. The system of an SAE Level 2 vehicle is able to execute both the lateral and the longitudinal motion control of the vehicle.[8] The driver has to perform the remainder of the dynamic driving task, such as the object recognition, and has to intervene when necessary.[9] The driver will have to supervise the system and has to be ready to take over the longitudinal and lateral motion control of the vehicle at all times.[10] The system of an SAE Level 3 vehicle is able to perform the entire dynamic driving task, but does require a user to take over the performance of the dynamic driving task when a situation occurs that the system is unable to handle, or when the vehicle reaches the end of its operational design domain (e.g. the highway ends).[11] The system should issue a request to intervene and give the user sufficient time to take over the driving task.[12] Germany has been very progressive by adopting legislation that sees to this transferral of the driving task. Some manufacturers have already announced they would like to skip SAE Level 3 vehicles[13] because of the risks involved with the transferal of the performance of the dynamic driving task from the automated driving system of the vehicle to the user, whereas other manufacturers do want to bring SAE Level 3 vehicles to the market.[14] The system of an SAE Level 4 vehicle, however, can perform the entire dynamic driving task within its operational design domain without relying on human interference, for instance on the highway.[15]

[1] Data from the heart rate sensor, the number of times you blink, etc., can indicate whether or not a situation makes you nervous.

[2] https://www.regjeringen.no/contentassets/ba7ab6e2a0e14e-39baa77f5b76f59d14/2016-04-08-declaration-of-amsterdam-final1400661.pdf.

[3] At the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong in 2017, a Resolution on Data Protection in Automated and Connected Vehicles was adopted, thereby underlining the importance of data protection.

[4] Nikolaus Forgó, Datenschutzrechtliche Fragestellungen des autonomen Fahrens, in: Autonomes Fahren. Rechtsgefolgen, Rechtsprobleme, technische Grundlagen, eds. Opperman, Stender-Vorwachs, C.H. Beck 2017, München.

[5] SAE International, J3016, June 2018.

[6] SAE International, J3016, June 2018, p. 19ff.

[7] For instance Tesla Model S.

[8] SAE International, J3016, June 2018, p. 21ff.

[9] SAE International, J3016, June 2018, p. 6, 14.

[10] SAE International, J3016, June 2018, p. 21.

[11] SAE International, J3016, June 2018, p. 19ff.

[12] See on this so-called 'fallback-ready user' and the dynamic driving task fallback SAE International, J3016, June 2018, p. 7-10, 17.

[13] See for instance Waymo, www.reuters.com/article/us-alphabet-autos-self-driving/google-ditched-autopilot-driving-feature-after-test-user-napped-behind-wheel-idUSKBN1D00MD?il&0, and Ford: www.wired.com/2015/11/ford-self-driving-car-plan-google/ (accessed 3 October 2018).

[14] For instance Audi with its new Audi A8, www.audi-mediacenter.com/en/on-autopilot-into-the-future-the-audi-vision-of-autonomous-driving-9305/the-new-audi-a8-conditional-automated-at-level-3-9307, and BMW: www.2025ad.com/latest/bmw-driverless-cars-strategy/?WT.tsrc=Newsletter&WT.mc_id=100/2018/ext (accessed 3 October 2018).

[15] SAE International, J3016, June 2018, p. 14, 19ff.

An SAE level 5 vehicle is the ultimate automated vehicle as its system can perform the entire dynamic driving task in any situation, on any road, in every weather condition.[16] A human only needs to despatch the vehicle. In order to drive itself and in order to provide safety features, the vehicle collects large amounts of data.[17]

3. Road safety

Although road fatalities have dropped by over 57% between 2001 and 2017, road safety remains a concern as the European Union has seen over 25,000 road fatalities in 2017.[18] Some Member States, like the Netherlands,[19] have even seen an increase in road fatalities in recent years. The EU is striving for zero fatalities by 2050, the so-called Vision Zero.[20] New technologies that, for instance, warn the driver when he is dosing of or bring the vehicle to a safe stop if the driver is not responding, could contribute to achieving this Vision Zero.[21] However, these monitoring systems pose challenges for EU data protection framework.

4. Data collection and automated driving

As users become less engaged in the performance of the dynamic driving task, the user's attention may decrease and users may start engaging in other tasks (eating, checking emails, sleeping). Driver monitoring systems may prove to be necessary to check if the user still focusses on the driving in an SAE Level 2 and an SAE Level 3 vehicle.[22] However, this data is perhaps not necessary for the functionality of the automated vehicle. In other words, the vehicle could be perfectly capable of driving safely without these data. Therefore, the user should be informed about whether the data is collected out of necessity or for the convenience of the user. Collecting data on the attention of the user of the vehicle could be beneficial to road safety. Systems that monitor the eye or head movements,[23] heart rate,[24] or the respiratory rate of the user could all prove to be helpful to establish whether the user's attention is on the driving of the vehicle.[25] The gathered data do not only say something about the user's alertness, but could also say something about the user's health. SAE Level 4 and Level 5 vehicles might also be equipped with monitoring systems and could potentially collect more health-related data. Do you use your fully automated vehicle to travel small distances that you could have easily walked? Do you let your vehicle drop you off at a fast-food restaurant for dinner every evening? All this information could be of interests to, for example, a health insurance company, your doctor or an advertising company. All in all, an automated vehicle could collect considerable amounts of data concerning the health of its users. If an automated vehicle is on the roads in Europe, these data are protected by both the General Data Protection Regulation (GDPR) and Council of Europe's (modernised) Convention 108.[26] Both regulations provide more or less the same level of data protection. Therefore, this paper will only focus on the GDPR.

5. Data protection and road traffic safety

5.1. *Data protection*

The legal protection of privacy on a European level dates back to 1950, when the Council of Europe drafted their European Convention on Human Rights (ECHR), thereby protecting a person's personal freedom. During the decades that followed, information and communication technologies (ICTs) played an ever-increasing role in society. With the use of ICTs, it is possible to processes large amounts of data in a short period of time. This development also affected the legal debate on the protection of personal data. Therefore, the European Union saw the need to protect the processing of personal data by

[16] SAE International, J3016, June 2018, p. 19ff.

[17] In 2015, a vehicle that is connected already collected 25GB of data per hour, according to The Internet on Wheels and Hitachi, Ltd. By Hitachi Data Systems December 2015, p. 3.

[18] http://www.europarl.europa.eu/news/en/headlines/society/20190410STO36615/road-fatality-statistics-in-the-eu-infographic accessed 16 August 2019.

[19] www.swov.nl/en/facts-figures/factsheet/road-deaths-netherlands accessed 29 July 2019.

[20] WHITE PAPER Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system, Brussels, 28.3.2011 COM(2011) 144 final, p. 10. See also Strategic Action Plan on Road Safety, Brussels, 17.5.2018 COM(2018) 293 final, ANNEX 1.

[21] Strategic Action Plan on Road Safety, Brussels, 17.5.2018 COM(2018) 293 final, ANNEX 1, p. 5-6, On the road to automated mobility: An EU strategy for mobility of the future, Brussels, 17.5.2018 COM(2018) 283 final.

[22] Will Knight, Automated Vehicles: One Eye on the Road, Another on You, MIT Technology Review, 19 June 2015, Tarek El Dokor, Autonomous Vehicles Need In-Cabin Cameras to Monitor Drivers. Self-driving cars require driver-monitoring capability to know when it is safe to hand over control, IEEE Spectrum, 4 October 2016.

[23] See for instance Nvidia DRIVE IX, www.nvidia.com/en-us/self-driving-cars/drive-ix/, and Cadillac Super Cruise: www.cadillac.com/world-of-cadillac/innovation/super-cruise (accessed 3 October 2018).

[24] See for instance the heart rate sensing seat that ford was working on: www.mobihealthnews.com/43191/ford-puts-the-brakes-on-its-heart-rate-sensing-car-seat-project.

[25] Euro NCAP identified driver monitor systems as a primary safety feature: Euro NCAP 2025 Roadmap. In pursuit of Vision Zero, September 2017, p. 7. The US National transportation Safety Board recommends driver monitoring systems, see Safety Recommendation H-17-042. See also Hamidur Rahman, Shahina Begum and Mobyen Uddin Ahmed, Driver Monitoring in the Context of Autonomous Vehicle, for the Thirteen Scandinavian Conference on Artificial Intelligence Nov. 4-6, 2015. Halmstad, Sweden, Jacob Kastrenakes, Jaguar wants to monitor its drivers' brainwaves, heart rate, and breathing, The Verge, 19 June 2015, www.theverge.com/2015/6/19/8815419/jaguar-brainwave-heart-rate-breathing-monitors (accessed 3 October 2018) and fortune.com/2017/05/03/ford-self-driving-car-biometric/.

[26] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf(2018)15-final.

means of Directive 95/46/EC, which was issued in 1995.[27] This Directive was replaced on 25 May 2018 by the General Data Protection Regulation.[28]

5.2. *Balancing the right to data protection and road traffic safety*

The right to data protection is not an absolute right, it should be balanced to other rights. With regard to automated driving, one could argue that road traffic safety should prevail over the right to data protection. The prevention of fatalities can be seen as more important than the protection of data on the driver's health. However, in this contribution we will show through a use case that both the public interest in road safety and the personal right to data protection can co-exist. A good legal framework is necessary to warrant data protection without losing sight of other public interests, such as road safety.

6. The general data protection regulation

6.1. *The scope of the GDPR*

The GDPR applies to all processing of personal data, either automated or non-automated. The territorial scope of the GDPR is quite large. If the data subject is within the EU, the GDPR applies to the processing of the data subject's personal data.[29] This is for instance the case if a user of an automated vehicle uses the vehicle to drive from Amsterdam to Rome. In that case, it is irrelevant whether the processor and/or the controller are established in the EU.

6.2. *Personal data and the different actors*

The definition of personal data given by the GDPR is very broad.[30] Any information that can identify a person is personal data. Therefore, the GDPR does not apply if "data rendered anonymous in such a manner that the data subject is not or no longer identifiable." [31] However, if data is merely pseudonymised, the data are still considered to be personal data because pseudonymisation can, other than anonymisation, be reversed. The identifiable person is referred to as the data subject, in this case the user of the automated vehicle. Almost everything that can be done with personal data is covered by the concept of processing in the GDPR. Article 4 (2) GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Furthermore, the GDPR provides for rights for data subjects, but also sets obligations for controllers and processors of personal data. The controller is the party who determines what data are collected, how these data are collected and for which purpose.[32] Therefore, depending on the circumstances, the manufacturer of the automated vehicle could be qualified as the controller, since the manufacturer determines what software is used, installs the necessary hardware and software, and determines how the user's behaviour is monitored.

The GDPR reserves another important role for the processor of personal data. The processor is the one that processes the personal data on behalf of the controller.[33] In the case of automated vehicles, both the software developer and the fleet operator can be seen as processors, since both process personal data on behalf of the controller. However, in some cases the fleet operator can be seen as a controller rather than a processor. This all depends on the specific circumstances of a situation. The following table gives an overview of the different actors in both automated vehicles and the GDPR.

Table 1 shows that in some cases both the manufacturer and the fleet operator can be qualified as controllers. In that case, the GDPR determines that they are so called joint controllers.[34] This can make it harder for data subjects to exercise their rights, since it might be unclear to the data subjects who is responsible for what. Therefore, Article 26 GDPR determines that the joint controllers must, by means of an arrangement, determine their respective responsibilities for compliance with the GDPR in a transparent manner.

6.3. *Sensitive data*

Next to regular personal data, there is a category of personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms. This merits specific protection as the context of their processing could create significant risks to fundamental rights and freedoms. These so-called sensitive data require additional protection as they touch the very core of a human being. Therefore, the GDPR offers an additional set of rules to protect these kinds of data. In the GDPR, data concerning health are part of the special categories of data. Unauthorised disclosure of data concerning health may lead to various forms of discrimination and violation of fundamental rights. If, for example, someone regularly works nightshifts, it is easy to misinterpret the data generated by the automated vehicle driving to the city at 10 p.m. and returning home at 6 a.m.. Without context, one might think that the user of the automated vehicle lives a wild life and regularly

[27] 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 [1995] OJ L 281/31.

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[29] Article 3 paragraph 2 under b GDPR.

[30] Article 4 under 1 GDPR.

[31] See consideration 26 GDPR.

[32] See for more background: Denis Kelleher and Karen Murray, EU Data Protection Law, Bloomsburry Professional 2018, London, p. 98-100.

[33] Article 4 under 8 GDPR. See also: Denis Kelleher and Karen Murray, EU Data Protection Law, Bloomsburry Professional 2018, London, p. 258-261.

[34] Article 26 GDPR.

Table 1 – roles according to the GDPR, depending on different circumstances.

	Processor (Article 4 para. 8 GDPR)	Controller (Article 4 para. 7 GDPR)	Recipient (Article 4 para. 9 GDPR)	Data subject (Article 4 para. 1 GDPR)
Fleet operator	Yes, if the fleet operator processes the data on behalf of the controller.	Yes, if the fleet operator determines the purposes and means of the processing.	Yes, if the personal data is disclosed to the fleet operator and he is not the controller nor the processor.	No
Manufacturer	No	Yes, if the manufacturer determines the purposes and means of the processing.	Yes, if the personal data is disclosed to them and they are not the controller nor the processor.	No
User	No	No	No	Yes, the user is the identified or identifiable natural person.
Buyer of data	No	No, but the buyer can be the controller of the newly created data set.	Yes, if the data is disclosed to the buyer.	No

attends parties which last the whole night, while in fact the user is working a night shift instead. Data concerning health are one of these special categories of data that merit specific protection.

6.4. *Data concerning health*

Data concerning health are personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status.[35] This is a very broad definition. The preamble to the GDPR provides some practical examples of what is covered by the definition. It includes, amongst others, information on a disease, a disability, and even a disease risk. This means that information about a person's body weight, blood pressure, genetic predisposition, but also information on tobacco consumption, are data concerning health since all these examples can be linked to the disease risk of a person.[36] The preamble furthermore adds that it does not matter what the source of the information on a disease, a disability, and a disease risk is.[37] This means it is not necessary that this source is an official medical device.

According to the independent European advisory body on data protection, the Article 29 Working Party,[38] in their 2015 'Annex – health data in apps and devices', personal data are data concerning health when

(1) *the data are clearly medical data*, this is the case when the data are on the physical and mental health of the data subject and are generated in a professional, medical context;
(2) *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*. For example, raw sensor data of someone's heart rate, age and gender are stored together, apart from the question if the data are used to draw conclusions on someone's health; or
(3) *conclusions are drawn about a person's health status or health risk*.[39] In this case it does not matter whether the raw sensor data is considered as data concerning health or not. This means that even data about how often someone uses an automated vehicle for short distances becomes data concerning health as soon as these data are used to draw conclusions on someone's health or health risk.

The GDPR entails safeguards for the processing of personal data and, in addition to that, additional measures need to be taken to protection data concerning health.

6.5. *Protecting the data*

When processing personal data, whether these are data concerning health or not, processors and controllers need to abide six principles of Article 5 GDPR:

1. the processing has to be lawful, fair and transparent;
2. personal data need to be collected for a specified, explicit and legitimate purpose (purpose limitation);
3. the collected data need to be adequate, relevant and limited to what is necessary in relation to the purpose of processing (data minimisation);

[35] Article 4 (15) GDPR.
[36] Recital 35 GDPR.
[37] Recital 35 GDPR.
[38] Under the GDPR the Article 29 Working Party is known as the European Data Protection Board (EDPB). In this contribution we will refer to either the Article 29 Working Party or the EDPB, depending on when the opinion was issued.
[39] Article 29 Working Party (A29WP), Annex by letter – health data in apps and device, 2015 p. 5.

4. the data need to be accurate and kept up to date (accuracy);
5. the personal data cannot be kept longer than is needed for the purposes for which they are collected (storage limitation); and
6. appropriate technical and organisational measures have to be taken to protect the data (integrity and confidentiality).

This first principle entails three elements: lawfulness, fairness and transparency. Although the GDPR is not very clear on when the processing is fair and transparent, it is clear on when the processing is lawful. The GDPR mentions six grounds for processing data that are considered to be lawful in Article 6 (see the use case below). If there is no legal ground for the processing, the processing is considered to be unlawful.

However, when the processed data are data concerning health, Article 6 GDPR does not apply: in principle the processing of sensitive data is prohibited, unless one of the exemptions mentioned in Article 9 (2) GDPR applies. The relevant exemptions and safeguards of Articles 6 and 9 GDPR will be discussed in-depth, when applicable, in the use case below.

7. Use case

The technology around automated driving is continuously developing, so the driver monitoring systems discussed in this paper are just some examples of systems that are currently being studied or anticipated. Whether such a system will eventually be in vehicles driving down public roads remains to be seen. The use case is divided into different sections, each handling a specific issue. Only the applicable provisions of the GDPR will be discussed.

7.1. *Types of data*

Imagine a user, who frequently uses an SAE level 3 vehicle. She uses the vehicle to travel to and from work, to drive her to her favourite restaurant, to her friends and family, to her doctor's appointments, to her daughter's day-care, and to the football matches of her favourite club. The automated vehicle is equipped with a heart rate sensor and a camera that tracks her eye movements. All gathered data are stored under the user's details.

The data from the use case can be used to identify a natural person, the user. Therefore, these data are personal data within the meaning of the GDPR.[40] As touched upon above, whether these personal data qualify as data concerning health depends on the circumstances. In this case, the data regarding the location of the user are not necessarily data concerning health: if these data are shared with a friend of the user to meet in a crowded city, these are not data concerning health. The data regarding the location of the user are not data concerning health when the fleet operator does not use these data to assess the health of the user. This also applies to the data concerning how often the user uses the automated vehicle and which distances she travels: if these data are not used to make an assessment of her health, these data are not data concerning health. However, if the health care insurer uses the same data to assess her general health, these data become data concerning health.[41] In addition, the data regarding the eye movements and the heart rate of the user are always data concerning health. After all, the raw sensor data can be used in itself to draw a conclusion about the health status of the user.[42]

7.2. *Collecting the data*

The data on how often the user uses an automated vehicle, where she drives to, at what time of day, her heart rate and her eye movements are all collected by the fleet operator and saved through a cloud-based service.

Within this use case, the fleet operator is the controller and the cloud-based service is the processor of the personal data. As described above, the data that are collected by the fleet operator on the location of the user, the use of the vehicle by the user, and the duration of the trips are not data concerning health. They are, however, personal data and therefore the fleet operator has to abide the general principles of Article 5 and 6 GDPR. From the six principles mentioned in Article 5 GDPR, the principles on lawfulness of the processing, purpose limitation and data minimisation are the most relevant when looking at the collection of data in the discussed use case.

On the basis of Article 6 GDPR, it can be determined whether processing is lawful. The processing of personal data is lawful (a) if the data subject consents to the processing, (b) if processing is necessary for the performance of a contract, (c) if processing is needed for compliance with a legal obligation, (d) if processing is necessary to protect the vital interests of the data subject or of another natural person, (e) if processing is necessary for the performance of a task carried out in the public interest, or (f) if processing is necessary for the purposes of the legitimate interests pursued by the controller. Concerning the data on the location of the user, the use of the vehicle by the user, and the duration of the trips, consideration (a) and (b) are the most relevant. The fleet operator will need to know who rented the vehicle, how long the vehicle was used, the distance travelled, the location where the vehicle is parked at the end of the trip, and the details of the renter to charge her for the use of the vehicle. These data are necessary for the fleet operator to charge renters for the costs of the use, and to enable the renting of the vehicles by multiple users. To offer his service to a user, the fleet operator has to collect all these data. The processing of these data is, therefore, necessary for the performance of the contract with the users, including the user from the use case. However, if the fleet operator wants to collect additional data, such as whether or not the user transports her weekly shopping with the vehicle, the fleet operator will have to ask the user's (data subject's) consent (consideration a). These data are not necessary for the performance of

[40] We proceed on the premise that these personal data will at best be pseudonymised, see section 6.2 for the difference between anonymisation and pseudonymisation.

[41] Article 29 Working Party (A29WP), Annex by letter – health data in apps and device, 2015 p. 4.

[42] Article 29 Working Party (A29WP), Annex by letter – health data in apps and device, 2015 p. 5.

the contract (consideration b of Article 6 (1) GDPR) and the collecting of these data are therefore not in conformity with the requirements on data minimisation and purpose limitation.

The data concerning health collected by the fleet operator consist of the eye movements and the heart rate of the user of the automated vehicle. Given art. 6 (3) of the upcoming General Safety Regulation, one can collect these data if this is 'necessary in relation to the purposes for which they were collected', which is the premise in this use case.[43] Therefore, only the GDPR sets boundaries for the collection of these data concerning health. Article 9 (1) of the GDPR states that the collecting of these data concerning health are in principle not allowed, unless the exceptions from Article 9 (2) GDPR apply. Most eye-catching is the exemption of Article 9 (2)(h) GDPR which allows the processing when the data are necessary for medical diagnosis. This exemption has to be read in conjunction with Article 9 (3) GDPR, which determines that those data have to be processed by or under the responsibility of a professional subject to the obligation of professional secrecy.[44] The fleet operator is not subject to professional secrecy. Therefore, this exemption does not apply. Another exemption, which could be of interest in this context, is Article 9 (2)(g) GDPR on the necessity of the processing for reasons of substantial public interest. This has to be on the basis of Union or Member State law which should be proportionate to the aim pursued and respect the essence of the right to data protection. It should also provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. One could argue that road safety is of substantial public interest. In the Member States that have such laws as mentioned in Article 9 (2)(g) GDPR, this exemption could therefore apply. If, however, a Member State does not have a law as mentioned in Article 9 (2)(g) GDPR, the exemption laid down in Article 9 (2)(a) GDPR might be applicable: the data subject (the user of the automated vehicle) has to give her explicit consent. The processing should furthermore be in conformity with general requirements of Articles 5 GDPR.

7.3. *Sharing the data*

During one of her trips, the vehicle requests the user to take over the driving from the automated system because of a complex situation caused by road works. The heart rate sensor in the steering wheel, that is used to monitor the driver's awareness, picks up a deviation in the user's heart rhythm. The deviation is so severe, that it could be the sign of a live-threatening condition. Therefore, the automated system of the vehicle warns the emergency services, which send an ambulance to the user. Meanwhile, the camera that tracks the eye movement of the user signals that the user slowly loses consciousness. The automated vehicle then parks itself in a safe spot. Thanks to the data from the heart rate sensor, the paramedics are able to quickly diagnose and treat the user's heart condition. The health care insurance of the user would like to access these data as well to assess whether the costs incurred for the treatment were proportional.

Regarding the sharing of these data with the paramedics, the GDPR opens up the possibility of processing data concerning health to protect the vital interests of the data subject, in this case the user of the automated vehicle.[45] This is only allowed if the data subject was not capable of giving consent. This was the case in the use case: the user was unable to give her consent, as she was unconscious when the paramedics arrived. However, the considerations of the GDPR state that if there is a different legal basis for the processing, this is preferred.[46] In this case, there is another legal basis for processing, namely Article 9 (2)(h) GDPR on medical diagnosis. The paramedics, other than the fleet operator, are subject to the obligation of professional secrecy and the processing is necessary for the user's medical diagnosis and treatment. Once again, the requirements of Article 5 GDPR have to be taken into account. However, art. 6 (3) of the upcoming General Safety Regulation states with regard to the data discussed that 'those data shall not be accessible or made available to third parties at any time and shall be immediately deleted after processing.' On the other hand, in Recital 14 of the General Safety Regulation, it is mentioned that 'Any processing of personal data, such as information about the driver processed in event data recorders or information about the driver's drowsiness and attention or the driver's distraction, should be carried out in accordance with with Union data protection law, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council (…)'. This seems contradictory to art. 6 (3) General Safety Regulation. Perhaps art. 6 (3) General Safety Regulation should be interpreted as an extra strict measure on top of the GPDR's provisions. However, it should be noted that in this specific case this would lead to an undesirable outcome (e.g. patient cannot be offered appropriate medical help). Given the uncertainty of the interpretation of art. 6 (3) General Safety Regulation and the scope of this article, this article will not further be discussed. Nevertheless, it is important to investigate the relationship of the General Safety Regulations and the GDPR to provide clarity on issues such as the one described here.

Next is the sharing of the data concerning the eye movement and heart rate with the user's health care insurer. The exemption of Article 9 (2)(h) GDPR does not apply here, as the health care insurer is not subject to the obligation of professional secrecy. There is no vital interest within the meaning of Article 9 (2)(c) GPDR, as the data has been requested after the incident at a time where the user is capable of giving her consent. Article 9 (2)(g) GDPR could apply as "cost-effectiveness

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

[44] Recital 53 GDPR.

[45] Article 9 (2)(c) GDPR.

[46] Recital 46 GDPR.

of the procedures used for settling claims for benefits and services in the health insurance system" are of public interest.[47]

7.4. Buying the data

The user's health care insurance company later requests data concerning the heart rate and the eye movement of the user during this incident from the fleet operator which rented the SAE level 3 vehicle to the user at the time of the incident. All data regarding all the trips the user has made using one of the vehicles of this fleet operator are stored in one account under the user's details. These data are stored by a cloud-based service. The health care insurance company wants to buy all the collected data as it would like to get a better picture of the general health of the user so they can adjust the premium to the height of her health risk.

The health care insurance company is interested in buying all the available data on the user of the automated vehicle from the fleet operator. Because the insurer wants to use the data to make assessment of the user's health, these data are considered data concerning health (Article 4 (15) GDPR) as they are used to draw conclusions on the user's health status and health risks. Therefore, it is not allowed to processes these data (Article 9 (1) GDPR) unless the exemptions of Article 9 (2) GDPR are met. As mentioned above, the exception of Article 9 (2)(h) GDPR does not apply here. Article 9 (2)(g) GDPR, to the authors' opinion, is not applicable in this case. Although Recital 52 of the GDPR mentions "cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system" are of public interest, the data requested by the health care insurer will be used for another purpose, namely the assessment of the user's general health. This use of the data is not for settling claims, but merely to adjust the premium to the user's health risk. There is, however, one other exemption that could apply: Article 9 (2)(a) GDPR. This entails that the user has to give her *explicit* consent to the fleet operator to sell her data for this purpose. Consent, within the meaning of the GDPR, is "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".[48] Freely given consent means that the user has to be given a real choice, with no negative consequences if she does not consent.[49] The consent for selling the data cannot be bundled together with the contract providing the service of the automated vehicle, as the selling of the data is not necessary for the performance of the contract for the service.[50] The Article 29 Working Party stresses that "consent and contract cannot be merged and blurred."[51] The purpose for which the health care insurer wants to purchase the user's data should be clear to the user, so her consent refers specifically to that purpose. In this context, the user will need to be informed about at least:

I "the controller's identity,
II the purpose of each of the processing operations for which consent is sought,
III what (type of) data will be collected and used,
IV the existence of the right to withdraw consent (…)"[52]

The consent the user has to give, has to be given explicitly as it concerns sensitive data. "Explicit" (Article 9 (2)(a) GDPR) does not necessarily mean that the consent has to be expressed through a written and signed statement. An electronic signature, for instance, could also be regarded as explicit consent. Besides, the user must be aware of the possibility and must be able to withdraw her consent at any time (Article 7 (3) GDPR). Other elements of consent are not discussed here, as they are less relevant in the context of the use case.

8. Three-step approach

As the use case has shown, there are several challenges regarding the collecting, sharing and selling of personal data that are processed via automated vehicles. Especially when it comes to sensitive data, such as data concerning health, the GDPR sets strict requirements. Fortunately, the GDPR also offers guidance on how an organisation can comply with these strict requirements. In the use case, the controller[53] could use a three-step approach: first a data protection impact assessment (DPIA), secondly data protection by design, and finally data protection by default. Data protection by design and by default are legal obligations set in Article 25 GDPR. A DPIA can contribute to, amongst others, complying with these two obligations.

8.1. Step 1: data protection impact assessment

The controller has to determine if a DPIA is mandatory. In the use case, the controller is either the fleet operator or the manufacturer, depending on who decides on means and purpose of the processing (see Table 1). Article 35 GDPR lists several aspects that are important in determining whether a DPIA is mandatory.[54] Such a DPIA is mandatory if the processing of personal data is "likely to result in a high risk to the rights and freedoms of natural persons (…)".[55] In addition, the Article 29 Working Party determines nine criteria that should also be considered. These nine criteria are:

1. *evaluation or scoring*; especially from 'aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements' (recitals 71 and 91 GDPR);
2. *automated-decision making with legal or similar effect*; as mentioned in Article 35 (3)(a) GDPR: 'legal effects concerning

[47] Recital 52 GDPR.
[48] Article 4 (11) GDPR.
[49] Recital 42 GDPR.
[50] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10 April 2018.
[51] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10 April 2018.
[52] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10 April 2018.
[53] See table 1.
[54] Denis Kelleher and Karen Murray, EU Data Protection Law, Bloomsburry Professional 2018, London, p. 268-269.
[55] Article 35 (1) GDPR.

the natural person' or which 'similarly significantly affects the natural person';[56]

3. *systematic monitoring*; the WP29 interprets 'systematic' as meaning one or more of the following: (a) occurring according to a system, (b) pre-arranged, organised or methodical, (c) taking place as part of a general plan for data collection and (d) carried out as part of a strategy ;[57]
4. *sensitive data or data of highly personal nature*; including (but not limited to) date that is part of Article 9 GDPR (the special categories of data, also called sensitive data) and data relating to criminal convictions or offences;
5. *data processed on a large scale*; here the number of data subjects concerned are relevant, as well as the volume of the data, the range of different data items, the duration of the data processing activity as well as the geographical extent of the processing activity ;[58]
6. *matching or combining datasets*; for a different purpose or if this exceeds the reasonable expectations of the data subject;
7. *data concerning vulnerable data subjects*; for example: children, employees and other people that might need special protection, such as mentally ill, asylum seekers, patients, etc.;
8. *innovative use of applying new technological or organisation solutions;* for example when combining finger print and face recognition for access control;
9. *when the processing itself prevents a data subject from exercising a right or using a service or a contract*; when, for example, operations are aimed at allowing, modifying or refusing data subjects' access.[59]

The data collected from the data subject of the use case concerns two types of personal data: regular personal data and data that falls within the special categories of personal data of Article 9 GDPR (the so-called sensitive data). In case of data that is considered to be data concerning health, and as such part of the special categories of data, a DPIA is mandatory according to the fourth criterion of the Article 29 Working Party's criteria. Furthermore, we would argue that even regarding the personal data that is not data concerning health a DPIA is mandatory as all the personal data in the automated vehicle is being processed on a large scale.[60] In the case of selling the data subject's personal data to the insurance company, there is the matching of or the combining of datasets (criterion 6). Even if a DPIA is not mandatory it is still recommended to perform a DPIA. A DPIA has to take place prior to the processing, according to Article 35 (1) GDPR. Because of this timing, a DPIA can help controllers to comply with the obligations of data protection by default and by design. Logically, a DPIA can also help controllers to comply with other data protection principles of the GDPR such as the data protection principles of Article 5 GDPR. In the words of the European Data Protection Supervisor: "The management of data protection risks, is at the core of the privacy by design and by default approach."[61]

8.2. *Step 2: data protection by design*

Article 25 paragraph 1 GDPR sets the obligation for data protection by design. Data protection by design entails taking data protection into account from the start of the very early phases of designing, in this case, the system for the automated vehicle.[62] The technical and organisational measures to safeguard data protection by design depend on the several elements, such as: "(…) the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing."[63] Therefore, when sensitive data ex Article 9 GDPR are processed, more advanced technical and organisational measures will have to be taken.

The development process starts with designing a system. It is important, in the earliest stage possible, for developers to consider data protection regulation when they design a system that will process personal data.[64] However, data protection by design does not stop after the first phases of a development process. On the contrary, data protection by design is important "throughout the technological life cycle" of any system processing personal data.[65] Sometimes, technical changes are made or become possible throughout the life cycle of a system, for instance through a software update of the system of the automated vehicle. This can affect the way in which a system processes personal data. In that case, it is once more important to take the principle of data protection by design into consideration. Article 25 (1) GDPR adds to this that data protection by design should take place "both at the time of the determination of the means for processing and at the time of the processing itself."[66] Data protection by design can contribute to the next step in the three-step approach: data protection by default.

[56] In this context, the audit of algorithms would be desirable. This is in line with recommendation 12 of the European Commission Independent Expert Group in: Ethics of Connected and Automated Vehicles Recommendations on road safety, privacy, fairness, explainability and responsibility, 2020 (available via https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf).

[57] Article 29 Working Party, Guidelines on Data Protection Officer 16/EN, WP 243, 13 December 2016, p. 8.

[58] Article 29 Working Party, Guidelines on Data Protection Officer 16/EN, WP 243, 13 December 2016, p. 7.

[59] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 17/EN, WP 248 rev.01, 4 October 2017, p 9-10.

[60] See also footnote 16.

[61] European Data Protection Supervisor, Opinion 5/2018, 31 May 2018, p. 8.

[62] A. Tamo-Larrieux, 'Introduction' in: *Designing for Privacy and its Legal Framework* (2018 Springer), p. xxiii.

[63] Article 25(1) GDPR.

[64] Tamo-Larrieux argues that therefore "privacy principles and engineering tools should be taught at engineering and computer science schools", see: 'Introduction' in: *Designing for Privacy and its Legal Framework* (2018 Springer), para 10.3.

[65] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10 April 2018, p. 22.

[66] Article 25 (1) GDPR.

8.3. *Step 3: data protection by default*

Data protection by default refers to the implementation of safeguards that protect the right to data protection as a default setting.[67] Article 25 (2) GDRP states that the obligation of data protection by default applies to: "…the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility". According to the European Data Protection Supervisor, this means that the most privacy friendly configuration should be set by default.[68] This configuration, according to Article 25 (2) GDPR, concerns at least the general principles of data minimisation, purpose limitations, storage limitation and confidentiality. These principles are all mentioned in the general article regarding data protection principles of Article 5 GDPR.[69] The European Data Protection Supervisor uses an example to explain data protection by default that is applicable to the use case:

> *"For example, if I use an app for car sharing I expect that my location is used for me to know where the closest car is parked and that my contact details be used to get in touch with me in the context of the service. This does not mean that, by default, my location and contact details should be sent over to local bike sellers to send me advertising and offers."*[70]

In 2014, the Article 29 Working Party already stressed the importance of both data protection by design and by default, especially regarding the Internet of Things (IoT), recommending "Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default."[71] Since then, on 25 May 2018, the GDPR came into force. Now, data protection by design and by default are no longer only recommended, they are a "legal and fully enforceable obligation that all those who process personal data under EU law must comply with."[72] Given the importance of data protection and the importance of (personal) data for automated driving, one could argue that only vehicles with systems that sufficiently protect (personal) data should be allowed on public roads.

9. Privacy as a technical requirement

Within Europe, vehicles need to be approved before they can drive down EU public roads. Approval is only granted when a multitude of technical requirements from different regulatory acts are met. The directive concerning this approval, Directive 2007/46/EC, states that "those regulatory acts should primarily seek to ensure a high level of road safety, health protection, environmental protection, energy efficiency and protection against unauthorised use."[73] Data protection or privacy are not listed as aims of this Directive. This is not surprising as the data gathered by conventional vehicles is very limited compared to the amount of data automated vehicles and driver assistance systems discussed in this contribution are expected to gather. The amount of data gathered by an automated vehicle could amount to as much as a terabyte a day.[74] This makes data protection a more prominent concern. Besides, with the development of automated vehicles, the technical requirements for vehicles will need to be revised.[75] Given this necessary revision, data protection could also become an integral part of the technical requirements automated vehicles will have to meet. The European Parliament acknowledges the importance of data protection in the context of the approval of vehicles.[76] A review of the data protection impact assessment and the demonstration of the processing of data in compliance with the GDPR could become requirements that need to be met in order to obtain approval of the (type of) vehicle. This way, data protection becomes an integral part of the (type-)approval process, thereby reinforcing the importance of the GDPR.[77]

10. Final remarks

This contribution has explored the possibilities and restrictions of processing and using of personal data gathered by the automated vehicle under the GDPR. The GDPR are offers possibilities to collect, share and sell personal data and data concerning health, that in turn could contribute to road safety. However, strict requirements apply, especially with regard to

[67] L. Jasmontaite et al, 'Data Proteciton by Desing and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' in: EDPL (2018) 2, 182.

[68] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on a proposal for Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions' (2013) 4.

[69] Article 5 (c), (b), (e) and (f), respectively.

[70] European Data Protection Supervisor, Opinion 5/2018, 31 May 2018.

[71] Article 29 Working Party, Opinion 8/2014 on the Recent Developments of the Internet of Things, 16 September 2014, 14/EN WP 223.

[72] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on a proposal for Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions' (2013) 4.

[73] Recital 3 Directive 2007/46/EC.

[74] https://www.ft.com/content/2a8941a4-1625-11e8-9e9c-25c814761640, https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/,Motion for a European Parliament Resolution on autonomous driving in European transport (2018/2089(INI)), recital 17.

[75] https://www.unece.org/trans/main/wp29/meeting_docs_grva.html

[76] 2019 Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/… and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009, Motion for a European Parliament Resolution on autonomous driving in European transport (2018/2089(INI)), recital 17-18.

[77] See also the in the USA required privacy plan developed by the manufacturer: section 12 of H.R.3388 - SELF DRIVE Act.

data concerning health. These requirements are in place to protect the fundamental rights and freedoms of the data subject, in this case the user of the automated vehicle. This contribution has explored some of the possibilities and requirements, but there are many more options when it comes to collecting (personal) data via automated vehicles, the processing of these data and subsequently the requirements that apply to the processing of these data. The GDPR does not only set requirements, but also offers guidance on how to meet these requirements. Through a data protection impact assessment ex Article 35 GDPR the controller can, prior to the processing, gain insight in the impact of the processing on the protection of personal data. When processing sensitive data, such as data concerning health, a data protection impact assessment is even mandatory. A data protection impact assessment can contribute to fulfilling the required data protection by design and data protection by default.[78] Data protection by design, in the context of automated vehicles, means that when choosing the software for the automated vehicle and during the processing of personal data, the interests of the user regarding her personal data should be considered (Article 25 (1) GDPR).[79] This is a continuous process: the controller should constantly ask himself whether the processing or collecting of the data is proportionate. Data protection by default entails that the settings for the data collection by the automated vehicle have to be as "privacy-friendly" as possible (Article 25 (2) GDPR). Collection and processing of more data than necessary is possible, but only with the (explicit) consent of the user. Both data protection by design and data protection by default subsequently contribute to complying with Article 6 GDPR. It is of great importance to take data protection into account before and during the deployment of automated vehicles. Governments, through the EU, might even consider making data protection part of the (type-)approval requirements for automated vehicles.[80] Therefore, it is necessary for all parties (policymakers, researchers, fleet operators, owners, future users, etc.) to join forces in developing a more robust framework.[81] It can be required to provide the approval authority with the data protection impact assessment on the software of the (automated) vehicle, indicating the considerations regarding the interests of data protection and, for example, road safety.

Declaration of Competing Interest

Manuscript: Exploring data protection challenges of automated driving.

The authors whose names are listed immediately below certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

[78] Article 25 GDPR.

[79] Nikolaus Forgó, Datenschutzrechtliche Fragestellungen des autonomen Fahrens, in: Autonomes Fahren. Rechtsgefolgen, Rechtsprobleme, technische Grundlagen, eds. Opperman, Stender-Vorwachs, C.H. Beck 2017, München.

[80] Directive 2007/46/EC.

[81] European Commission Independent Expert Group, Ethics of Connected and Automated Vehicles Recommendations on road safety, privacy, fairness, explainability and responsibility, 2020 (available via https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf), recommendation 8. Other than the Independent Expert Group, the authors are of the opinion that future users should also be consulted as they have their own unique frame of reference.

[82] § 1a-1c Straßenverkehrsgesetz (StVG).