# Handing over the wheel, giving up your privacy?

Mulder, Trix; Vellinga, N. E.

*Published in:*
Conference proceedings 13th ITS Europe Congress



*Publication date:*
2019

13th ITS European Congress, Brainport, the Netherlands, 3-6 June 2019

Paper number ITS-1755

# Handing over the wheel, giving up your privacy?

**T. Mulder[1*], N.E. Vellinga[2]**

1. Faculty of Law and University Medical Centre Groningen, University of Groningen, the Netherlands,

t.mulder@step-rug.nl

2. Faculty of Law, University of Groningen, the Netherlands

**Abstract**

With the increase in automation of vehicles and the rise of driver monitoring systems in those vehicles, privacy and data protection concerns become more relevant for the automotive sector. Monitoring systems could contribute to road safety, by for instance warning the driver if he is dozing off. But 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, including health data, and the different requirements applicable to the collecting and processing of those types of data will be explored. Thereby, this contribution will give insights into the consequences of the GDPR for the collecting and processing of data gathered by automated vehicles.

**Keywords:**

**DATA PROTECTION, GDPR, AUTOMATED DRIVING**

## 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. Sounds disturbing?

The important role sensors and camera's 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 [1] the right to privacy and data protection, and they agreed to a joint agenda which, among others, should ensure privacy and data protection. 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 camera's 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 this

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 this data with other data, such as the location of the vehicle and the time of day, and sell it on 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 [2]. First, the different levels of automation and the different possibilities of collecting health related data through the sensors and camera's will be 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.

**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 the user still focusses on the driving in a Level 2 and a Level 3 vehicle [3], [4]. Systems that monitor the eye or head movements (see for instance [5]), heart rate (see for instance [5]), 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 and he is not dowsing off (Euro NCAP identified driver monitor systems as a primary safety feature, see [7], see also [8], [9]). The data that is gathered does not only say something about the user's alertness, but could also say something about the user's health. 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, e.g., a health insurance company, your doctor or an advertising company. All in all, an automated vehicle collects 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 the General Data Protection Regulation.

**Data protection and road traffic safety**

*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, 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 impacted the legal debate on the protection of personal data. Therefore European Union saw the need to protect the processing of personal data by means of Directive 95/46/EC, which was issued in 1995 [10]. This Directive was replaced on 25 May 2018 by the General Data Protection Regulation (GDPR)[11].

*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.

**The General Data Protection Regulation**

*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 – for instance the user of the automated vehicle – is within the EU – the user drives with his automated vehicle from Amsterdam to Rome –, the GDPR applies to the processing of the data subject's personal data (Article 3 paragraph 2 under b GDPR). In that case, it is irrelevant whether or not the processor and/or the controller are established in the EU.

*Personal data and the different actors*

The definition of personal data given by the GDPR is very broad (Article 4 under 1 GDPR). Any information that can identify a person is personal data. This 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 is collected, how this data is collected and for which purpose. Therefore, depending on the circumstances, the manufacturer of the automated vehicle could be qualified as the controller, since the manufacturer determines what software is being used, installs the necessary hardware and software, and determines how the user's behaviour is going to be 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 (Article 4 under 8 GDPR). 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 been seen as a controller rather than a processor. Table 1 shows that in some cases both the manufacturer and the fleet operator can be qualified as a controllers. In that case the GDPR determines that they are so called joint controllers (Article 26 GDPR). If this is the case, it 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.

**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 |

*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. This is why the GDPR offers an additional set of rules to protect these kinds of data. In the GDPR, data concerning health is part of the special categories of data called sensitive data, since it comes within a person's most intimate sphere. 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 attends parties which last the whole night, while in fact they are working a night shift instead.

*Data concerning health*

Data concerning health is 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(Article 4 (15) GDPR). This is a very broad definition. The preamble to the GDPR provides some practical examples of what is covered by the definition. It includes, among others, information on a disease, a disability and even a disease risk. This means that information about a person's obesity, high or low blood pressure, genetic predisposition, but also information on tobacco consumption are part of health data since all these examples are linked to the disease risk of a person (Recital 35 GDPR). 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 (Recital 35 GDPR).

According to the independent European advisory body on data protection, the Article 29 Working Party, 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 if 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 [12]. 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 it is used to draw conclusions on someone's health or health risk.

*Protecting the data*

When processing personal data, whether this is 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 needs to be collected for a specified, explicit and legitimate purpose( purpose limitation);
3. the collected data needs to be adequate, relevant and limited to what is necessary in relation to the purpose of processing (data minimisation);
4. the data needs 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: the processing of personal data has to be lawful, fair and transparent. 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 is 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.

**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 on 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.

*Types of data*

*Imagine a user, who frequently uses a 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 also equipped with a heart rate sensor and a camera that tracks her eye movements.*

The data mentioned in the use case are stored under the user's details. So, the data can be used to identify a natural person, the user. Therefore, these data are personal data within the meaning of the GDPR. 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. However, if the same data are used by the health care insurer to assess her general health, these data become data concerning health. The collecting of the data regarding the location of the user does not make the data data concerning health as it is not used by the fleet operator to make an assessment of 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. The data regarding the eye movements and the heart rate of the user are, however, 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.

*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 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 or not the processing was lawful. The

processing was lawful (1) if the data subject consents to the processing, (2) if processing is necessary for the performance of a contract, (3) if processing is needed for compliance with a legal obligation, (4) if processing is necessary to protect the vital interests of the data subject or of another natural person, (5) if processing is necessary for the performance of a task carried out in the public interest, (6) 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 (1) and (2) are the most relevant. The fleet operator will need to know who rented the vehicle, how long the vehicle is being used, the distance travelled, the location where the vehicle is parked at the end of the trip, the details of the renter so as 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 user. 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 contracts 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's transports her weekly shopping with the vehicle, the fleet operator will have to ask the user's (data subject's) consent. These data are not necessary for the performance of the contract (Article 6 (1) GDPR) and is therefore not in conformity with the requirements on data minimisation and purpose limitation.

The data concerning health collected by the fleet operator are the eye movement and the heart rate of the user of the automated vehicle. This is 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 if 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. This is not the case for the fleet operator. Another exemption, which could be of interest in this context, is Article 9 (2)(g) 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 (Article 9 (2)(g) GDPR). 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.

*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 than parks itself in a safe spot. Thanks to the data from the heart rate sensor, the paramedics were 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.*

First, 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, in Article 9 (2)(c). 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 (Consideration 46). In this case, there is another legal basis for processing, namely Article 9 (2)(h) GDPR. 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 Articles 5 GDPR have to be taken into account.

Secondly, 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) could apply as "cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system" are of public interest (Consideration 52).

*Buying the data*

*The user's health care insurance 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 Consideration 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 is used for other purposes, 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" (Article 4 (11) GDPR). Freely given consent means that the user has to be given a real choice, with no negative consequences if she does not consent (Consideration 42). 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 [13]. The Article 29 Working Party stresses that "consent and contract cannot be merged and blurred."[13] The purpose for which the health care insurer wants to purchase her 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 (…)"[13]

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.

**Final remarks**

This contribution showed that there are possibilities to collect, share and sell personal data and data concerning health gathered by the automated vehicle. However, strict requirements apply, especially with regard to data concerning health. These requirements are put 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 (dpia, 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 dpia is even mandatory. A dpia can contribute to fulfilling the required privacy by design and privacy by default (Article 25 GDPR). Privacy by design, in this context, 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)[2].

This is a continuous process: the controller should constantly ask himself whether the processing or collecting of the data is proportionate. Privacy 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 privacy by design and privacy by default subsequently contribute to complying with Article 6 GDPR. So, 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 [14]. It can be required to provide the approval authority with the dpia on the software of the automated vehicle, indicating the considerations on the interests of data protection and, e.g., road safety.

**References**

1. Declaration of Amsterdam on cooperation in the field of connected and automated driving, 2016.
2. Forgó, N. (2017). *Datenschutzrechtliche Fragestellungen des autonomen Fahrens*, in: Autonomes Fahren. Rechtsgefolgen, Rechtsprobleme, technische Grundlagen, Opperman and Stender-Vorwachs (eds.), C.H. Beck.
3. Knight, W. (2015). Automated Vehicles: One Eye on the Road, Another on You, *MIT Technology Review*, 19 June 2015.
4. El Dokor, T. (2016) 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.
5. 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).
6. www.mobihealthnews.com/43191/ford-puts-the-brakes-on-its-heart-rate-sensing-car-seat-project (accessed 3 October 2018).
7. Euro NCAP (2017). Euro NCAP 2025 Roadmap. In pursuit of Vision Zero, September 2017.
8. The US National transportation Safety Board, Safety Recommendation H-17-042.
9. Rahman, H., S. Begum and M. U. Ahmed (2015). Driver Monitoring in the Context of Autonomous Vehicle, for the Thirteen Scandinavian Conference on Artificial Intelligence Nov. 4-6, 2015.
10. Directive 95/46/EC of 24 October 1995.
11. Regulation (EU) 2016/679 of 27 April 2016.
12. Article 29 Working Party (A29WP), Annex by letter – health data in apps and device, 2015 p. 5.
13. A29WP, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10 April 2018.
14. Directive 2007/46/EC of the Council of 5 September 2007.