Přijato k publikaci v roce 2018 10.14311/mecdc.2020.01.01

# AUTONOMOUS VEHICLES AND EUROPEAN DATA PROTECTION LAW

**EVA FIALOVÁ**
Institute of State and Law of the Czech Academy of Sciences, Národní 18, Praha 1, Tel.: 723 981 144, Email: eva.fialova@ilaw.cas.cz

**ABSTRACT**
Autonomous vehicles process a huge amount of data about the driver, or rather passengers of the vehicle, as well as about other persons (pedestrians and passengers of other vehicles). This is why the autonomous vehicles raise questions about the protection of personal data. In 2018 a new European data protection legislation came into force. The General Data Protection Regulation places new obligations on controllers of personal data and provides new rights to data subjects, which will relate to operations of autonomous vehicles and their infrastructure. The providers thereof will have to implement the principles of data protection legislation into their systems. In this context the personal data is not just data concerning the identity of the driver, a passenger or other persons, but any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or even due to a peculiar behaviour in the vehicle. The paper will focus on the new legal regulation in relation to the operation of autonomous vehicles.
**KEYWORDS:** AUTONOMOUS VEHICLES, DATA PROTECTION, GDPR, PRIVACY

**SHRNUTÍ**
Autonomní vozidla zpracovávají velké množství údajů o řidiči vozidla, resp. cestujících ve vozidle, jakož i o dalších osobách (spolucestujících, chodcích a pasažérech v jiných vozidlech). To je důvod, proč provoz autonomních vozidel vyvolává řadu otázek týkajících se ochrany osobních údajů. V roce 2018 nabyla účinnosti nová evropská právní úprava regulující tuto oblast. Obecné nařízení o ochraně osobních údajů přináší nové povinnosti správcům osobních údajů, jakož i nová práva subjektům údajů, která se budou týkat provozu autonomních vozidel a infrastruktury. Výrobci a poskytovatelé služeb budou muset do svých systémů implementovat legislativu o ochraně osobních údajů. Osobními údaji nejsou pouze údaje týkající se totožnosti řidiče, cestujících nebo jiných osob, ale veškeré informace vztahujících se k identifikované nebo identifikovatelné fyzické osobě, kterou lze přímo nebo nepřímo identifikovat, zejména odkazem na identifikátor, jako je např. název, identifikační číslo, lokalizační údaje, nebo třeba i kvůli osobitému chování ve vozidle. Tento článek se zaměřuje na novou právní úpravu ve vztahu k provozu autonomních vozidel.
**KLÍČOVÁ SLOVA:** AUTONOMNÍ VOZIDLA, GDPR, OCHRANA ÚDAJŮ, SOUKROMÍ

## 1. INTRODUCTION

The operation of autonomous vehicles results in a huge amount of personal data being processed about drivers, or in the case of fully autonomous vehicles, about users (for the sake of simplicity the term driver is used for the driver as well as for the user of a fully autonomous vehicle). The processed data may also relate to third persons, e.g. fellow-passengers, pedestrians and drivers and passengers of other (autonomous) vehicles, in other words, the cameras, sonars and radars collects huge amount of data about their interior and exterior [1]. The legal framework for the protection of personal data was harmonized in the European Union on the basis of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Since the Directive has been transposed in national legal systems and the level of protection of personal data differed across the European Union, the protection of personal data is nowadays governed by the Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "the Regulation" or "GDPR"). The Regulation is directly effective in all Member States of the European Union. This means that in contrast to the Directive 95/46/EC the Regulation does not have to be transposed into the national laws because of its direct effect. This paper will focus on the new data protection regulation and its application with respect to autonomous vehicles.

## 2. PROTECTION OF PERSONAL DATA IN THE OPERATION OF AUTONOMOUS VEHICLES

According to art. 4 par. 1 GDPR, personal data is any information about an identified or identifiable natural person (a data subject). An identifiable person is a person who can be identified directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, network identifier or one or more specific physical, physiological, genetic, psychological, economic, or social identifiers of a natural person. According to the Court of Justice of the European Union, a person is identifiable if the controller has means reasonably likely be used in order to identify the data subject, even with the assistance of other persons [2]. The personal data is, therefore, any information that can be related to the driver of an autonomous vehicle, to passengers, and to drivers or passengers of other vehicles with which the autonomous vehicle comes into contact. Such personal data could, for example, be the posture of the driver, his/her way of handling the vehicle, or his/her location or regular daily route from which a home and work address may be deduced.

Personal data may be processed only if the controller has a legal basis to perform such processing as enumerated in art. 6 GDPR. In the case of autonomous vehicles, the contract between the controller and the data subject will provide legal grounds for processing of the driver's data. According to the European Data Protection Board the aforementioned legal ground "will not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject." [3]. If this is not the case, the controller will have to process the data under some other legal ground. Another legal ground for processing may be the fulfilment of a legal obligation of the controller. For example, a law might prescribe to the controller's obligation to process defined categories of data for specific purposes, e.g. insurance purposes, taxation, etc.

Beside that the controller is allowed to process the personal data when such processing is necessary to protect the vital interests of the data subject or of another natural person. For instance, in the case of an accident, the vehicle might evaluate some personal data essential for the saving of lives and transmit them to the controller for further processing in addition to data that are already programmed to be processed in such cases and are therefore processed under other legal grounds.

Other data may be processed if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. As an example of such data could serve the data, which are indispensable for an examination of an accident and the determination of liability (provided that those data will not be processed for the fulfilment of the legal obligation). These interests can be overridden by the interests or fundamental rights and freedoms of the data subject (e.g. a right to privacy or interest in the protection of property).

Personal data may be also processed when the data subject has given consent to the processing of such data. Consent means a freely given, specific, informed and unambiguous manifestation of the data subject's wishes by which the data subject gives a declaration or other apparent confirmation of his/her consent to processing of personal data relating to him/her (art. 4 par. 11 GDPR).Such consent to processing will be typical for the driver's personal data that cannot be processed in accordance with the aforementioned legal grounds. Consent will also be typical for personal data necessary for providing additional services. The controller has to prove that the consent of the data subject has been given. The consent of the owner the vehicle could be attached to a contract of purchase. The controller may ask the driver for the consent during the operation of the vehicle. In the case of other vehicle's user, the controller will have to find a solution for the granting of consent and demonstration thereof.

There is a subtype of personal data that requires stricter protection, the "special categories" of personal data (art. 9 GDPR), and sensitive data according to the previous legislation. Those data relate in particular to a racial or ethnic origin, religious or philosophical beliefs, sexual orientation and health. Also sensitive according to the Regulation are biometric data for the purpose of uniquely identifying a person, for example, the identification of the driver or passenger. The processing of such data is forbidden unless the controller disposes with a legal ground pursuant art. 9 GDPR.

## 3. OBLIGATIONS OF THE CONTROLLER

A controller is a person who determines the purposes and means of the processing of personal data (art. 4 par. 7 GDPR). In relation to the operation of the autonomous vehicles, the data controller may be a manufacturer, a lessor (the owner of a fleet), or an operator of telecommunication or traffic infrastructure. In interconnected vehicles and infrastructure, it will be difficult to determine who are the controller and the processor of data. Besides the interconnected vehicles the autonomous ones might also be "self-contained". This means all the data will rest in the vehicle itself [4]. The interconnected autonomous vehicles and communication between vehicle and infrastructure is under research in this field now [5].

The controller may also be a driver of the vehicle that processes the personal data of third persons and this processing falls within the scope of the Regulation, such as the processing of personal data wholly or partly automatically. The driver may. for instance, be able to download data collected by cameras and sensors, to store them or to process them in any other way defined by art. 4 par. 2 GDPR. In such case, the driver has all the obligations of a data controller laid down by the Regulation. The controller may engage a processor who processes the personal data for the controller on the basis of a written contract, e.g. a provider of cloud computing services or other storage services for data processed during the operation of the autonomous vehicles. Nevertheless, it shall always be the controller who is responsible for personal data processing.

The controller must adhere to the data protection principles enumerated in art. 5 GDPR in order to be compliant with the Regulation. Personal data must be processed lawfully, fairly and in a transparent manner. The controller has to have legitimate purposes for the processing. The personal data must not be processed in a manner that is incompatible with the given purposes. However, further processing for scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes. The controller must stick to the data minimisation principle. This principle means that the controller can only process data relevant to the given purpose and are limited in scope to what is necessary for that purpose. It is likely that the controller will manage to defend the processing of personal data relating to vehicle operation and its further use in the development of the autonomous vehicles, even in case that the personal data cannot be anonymized. The processed data have to be accurate and must not be stored longer that is necessary for the purpose. After the retention period, the data cannot be further processed.

One of the pivotal obligations of the controller and the processor is to ensure the integrity and confidentiality of the personal data. Pursuant to art. 32 GDPR the controller has to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in relation to the rights and freedoms of natural persons. These risks include not just the threat to the right to privacy and data protection. The potentially infringing information may be the location where the vehicle is parked overnight, what is the usual route of the vehicle, etc. Based on the data, a detailed profile of the driver and his/her financial status, habits and preferences can be made [6].
The controller has to also assess the risk in relation to other rights, for instance the right not to be discriminated against in the case of profiling of a data subject. By selecting appropriate measures the controller will have to take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk level in terms of likelihood and severity for the above-mentioned rights and freedoms. These measures include pseudonymisation and encryption, the ability to ensure confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and the implementation of a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

It can be assumed that companies and authorities engaged in the operation of autonomous vehicles will process a huge amount of personal data on numerous data subjects, their identifiers, daily habits and routines, profiles, connection with other persons etc. The right to privacy, data protection and other rights of those data subjects may be infringed by a breach of the integrity of the system and data leakage and loss. A controller that processes the personal data collected during the operation of autonomous vehicles will thus have to adopt strict measures to ensure the data security. A data breach may cause an intrusion into the private and family life of a user, his or her information self-determination or in some cases it might even affect his/her her personal safety in case that the information about the regular locations and habits has been compromised.

Assuming the probability that a personal data breach will result in a risk to the rights and freedoms of natural persons, the controller must without undue delay and, where feasible, within 72 hours of having become aware of it, notify the the supervisory authority (art. 33 GDPR).

Another obligation of some controllers is to carry out a data protection impact assessment pursuant to art 35 GDPR. Where a type of processing, especially one using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller will, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A data protection impact assessment is in particular required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling or a systematic monitoring of a publicly accessible area on a large scale.

It can be assumed that the controllers processing the personal data in connection with the operation of autonomous vehicles

will be obliged to carry out a personal data impact assessment before commencing processing. The reason for the obligation is the above-mentioned character of personal data processing during the operation of the autonomous vehicles. Moreover, the controllers will certainly systematically and extensively evaluate the personal data for safety or commercial reasons. Autonomous vehicles will also incorporate new technologies, or the current technologies will be used differently, so the risk to the rights and freedoms of data subjects is difficult to estimate at present. This fact represents an additional reason for a data protection impact assessment carried out by the operator prior to processing.

The controller in the case of personal data processing relating to the operation of the autonomous vehicle will have to designate a data protection officer (art. 37 GDPR). The data protection officer has to be designated when the core activities of the controller consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. Since the operation of autonomous vehicles represents the processing of a huge amount of personal data on a large scale as well as regular and systematic monitoring, there is no doubt about the obligation of the controller to appoint a data protection officer.

## 4. DATA PROTECTION BY DESIGN AND BY DEFAULT

According to the data minimisation principle, the controller processing personal data in connection with the operation of autonomous vehicle must take steps not to process more data than is necessary for the purpose for which the data are processed. In addition, art. 25 of the Regulation obliges the controller to take all possible steps to guarantee data protection by design and by default. This means that appropriate technical and organisational measures have to be implemented so that the data protection principles are safeguarded in order to meet the requirements of the Regulation, i.e. to protect the rights of data subjects and to ensure the security of the data processing.
When implementing data protection by design (sometimes also called privacy by design) the controller has to consider the data protection principles already at the stage of product or system development. According to its originator Ann Cavoukian privacy by design means "embedding privacy into information technologies, business practices, and networked infrastructures, as a core functionality, right from the outset – means building in privacy right up front – intentionally, with forethought. PbD may thus be defined as an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls." [7]. Autonomous vehicles have to be technically designed in a way compliant with the principles of personal data protection.

Data protection by default (or privacy by default) means that the manufacturer or designer applies the most stringent privacy settings which can only be subsequently changed only by the data subject. For Cavoukian privacy by default is one element of the privacy by design approach [8]. The data subject can later opt-in for a less stringent data protection setting. However, the opt-in should not be irreversible. German Verband der Automobilindustrie (VDA) supports the active involvement of the consumer in data processing options. "The members of the VDA are striving to enable customers to determine themselves the processing and use of personal data through various options. The members of the VDA will enable these options through contractual provisions, consents or technical features in the framework of optional features and choices that are given, through which the customer can activate or deactivate services, unless the processing is regulated by law." [9]. Data protection by design and the option for the user to change the privacy settings is advocated by the Data Protection and Privacy Commissioners in their Resolution on Data Protection in Automated and Connected Vehicles [10].

In the event of violation of the obligation, the supervisory authority may impose severe fines. The amount of the fine will depend in particular on the nature, severity and duration of the infringement. The supervisory authority will take into account the nature, extent or purpose of the processing, as well as the number of data subjects concerned and the extent of the damage caused to them. The imposed fine may be up to € 20 million or 4 % of total worldwide annual turnover.

## 5. RIGHTS OF THE DATA SUBJECT

The Regulation strengthens the rights of data subjects. Data subjects are the driver of the autonomous vehicle, a passenger or a third person outside the vehicle whose personal data are automatically processed during the operation of the vehicle.

A data subject, whether it is a driver, a passenger or persons whose personal data are processed in connection with the operation of an autonomous vehicle, has the following rights under the Regulation:

1. the right to information (art. 13 and 14 GDPR)
2. the right of access (art. 15 GDPR)
3. the right to rectification (art. 16 GDPR)
4. the right toerasure sometimes called the right to be forgotten (art. 17 GDPR)
5. right to restriction of data processing (art. 18 GDPR)

6. the right to data portability (art. 20 GDPR)
7. the right to object (art. 21 GDPR)
8. the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similar effects concerning the data subject (art. 22 GDPR).

The right to data portability is the right to transfer the data between the controllers. This right can only be exercised when the data are processed on the basis of consent or a contract and the processing is carried out by automated means. This right may be applied in the case of changing the operator of an autonomous vehicle if the data subject is interested in transferring the personal data collected during the operation of the autonomous vehicle to another operator.

The data subject cannot claim the right to erasure when his/her data are processed on the basis of a legal obligation of the data controller. The right to erasure is not absolute. If the processing of the personal data is required by a law which enshrines the obligation of processing of certain data collected in connection with the operation of the autonomous vehicles, the data subject cannot claim the right to erasure of his/her personal data.

Profiling of the personal data is allowed in accordance with the Regulations. Pursuant to art. 4 par. 4 GDPR profiling is any form of automated processing of personal data involving the use of data to evaluate certain personal aspects related to a physical person, such as driving or reactions of the vehicle user or his or her habits for the marketing purposes. The right not to be subject to automated processing may be typically applied in the assessment of insurance risk. Profiling must not result in an automated decision. The right not to be subject to an automated decision will not apply if the automated processing is necessary for a performance of a contract or the automated decision-making is permitted by law or when this type of processing is based on the explicit consent of the data subject.

## 6. AUTONOMOUS VEHICLES AND EPRIVACY

The processing of personal data in the field of electronic communications is regulated in the European law by Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications). This directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services or public communications networks.

At present, the legal framework for the protection of personal data in the electronic communications sector is being revised. The European Commission proposed a Regulation on Privacy and Electronic Communications (the "ePrivacy Regulation"), which will, along with the GDPR, be directly effective in all Member States of the European Union as well as the GDPR. Even though it is only at the draft stage and and the final wording is not yet set down [11], the ePrivacy Regulation will probably apply to the transmission of communication between machines. The recital 12 of the ePrivacy Regulation mentions explicitly that the regulation shall apply to machine-to-machine (M2M) communication. It is questionable what kind of M2M communication can be considered as an electronic communication service, the area regulated by the ePrivacy Regulation [12]. To assess whether the ePrivacy Regulation will enshrine the communication between autonomous vehicles and the vehicles and the infrastructure, a definition of the electronic communication service has to be taken into consideration. The definition of this service refers to the European Electronic Communications Code (Directive (EU) 2018/1972 establishing the European Electronic Communications Code). Pursuant to the art. 2 of the European Electronic Communications Code the electronic communications service encompasses, besides other things, services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services. It is not clear whether the M2M communication of the autonomous vehicles and to what extant can be consider as the electronic communication service [13]. The clarification thereof is significant since the data processing in case of the provision of the service will be conditioned by compliance with the rules of the ePrivacy Regulation. Pursuant to the draft of the ePrivacy Regulation, service provider may provide the service primarily with the user's consent unless he will process the data under other legal grounds which are nevertheless limited in number.

## 7. CONCLUSION

The operation of autonomous vehicles will involve the processing of a huge amount of data. The GDPR will apply to the processing of personal data collected, transmitted, disclosed, used or profiled in connection with the operation of the vehicles. The manufacturers, the lessors and other personal data controllers will have to be compliant with the new legislation when they will process the personal data of the driver, passenger or third persons. In comparison with Directive 95/46/EC, the Regulation will set down new obligations of the controller, in particular, to appoint a data protection officer, to notify the supervisory authority of a data breach, to carry out a data protection impact assessment and to implement the privacy by design and by

default into their products and processes. On the other hand, the Regulation provides the data subject with some new rights (the right to data portability, the right not to be subject to an automated decision and an enhanced right to data erasure). The rights of the data subject are aimed at ensuring greater transparency and control for the data subject over his/her personal data. However problematic issues may arise in practice, e.g. the finding of the appropriate legal ground of processing, a manner of obtaining the consent of data subject or appropriate data breach safeguards. A question whether the communication among vehicles and between the vehicles and the infrastructure will fall under the ePrivacy Regulation and if so, to what extent, still remains unclear.

## ACKNOWLEDGEMENTS

The paper was supported by the Technology Agency of the Czech Rebublic under grant No. TL02000085 Civil Liability for Damage Caused by Operation of Autonomous Vehicles.

## REFERENCES

[1] COLLINGWOOD, L. (2017). Privacy implications and liability issues of autonomous vehicles. Information and Communications Technology Law, vol. 26, no. 1, p. 35.
[2] Judgement of the Court of Justice of the European Union no. Case C582/14 (Patrik Breyer v.Bundesrepublik Deutschland).
[3] European Data Protection Board. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (Version for public consultation). p. 7. Available at: Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects
[4] GLANCY, D. J. (2012). Privacy in Autonomous Vehicles. Santa Clara Law Review, vol. 52, no. 4, p. 1176.
[5] FRIEDRICH, B. (2015) Verkehrliche Wirkung autonomer Fahrzeuge, in: MAURER, M. et al. Autonomes Fahren, Berlin, Hedelberg: Springer Verlag. 349.
[6] COLLINGWOOD, L. (2017). p. 36.
[7] CAVOUKIAN, A. (2012). Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices, p. 8. Available at: http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf
[8] ibid.
[9] Verband der Automobilindustr (2014). Data Protection Principles for Connected Vehicles, p. 3. Available at: https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeug
[10] 39th International Conference of Data Protection and Privacy Commissioners (2017). Resolution on Data Protection in Automated and Connected Vehicles. Available at: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=27212
[11] See ePrivacy Tracker. Available at: https://www.eprivacy.law/e-privacy-chronology
[12] STORMS, S. (2018), Quo vadis, ePrivacy? Confidentiality of machine-to-machine communications. Available at: https://www.law.kuleuven.be/citip/blog/quo-vadis-eprivacy-confidentiality-of-machine-to-machine-communications/
[13] European Automotive and Telecom Alliance (2018). Data protection & privacy. Available at: https://www.acea.be/uploads/news_documents/EATA_regulatory_briefing_paper-Data_protection_ePrivacy.pdf