DETECTION OF NON-PERSONAL DATA LEADING TO USER IDENTIFICATION, INCLUDING RELATED RECOMMENDATIONS FOR THE FIELD OF AUTONOMOUS MOBILITY

Zdeněk Lokaj,[*] Martin Šrotýř,[**] Miroslav Vaniš,[***] Ivo Janda,[****] Tomáš Ščerba[*****][1]

Abstract: *This paper introduces the issue of personal and non-personal data in autonomous vehicles. Its main objective is to provide a procedure for determining the processed and retained data, to explain the current legal regulation that must be met, and to propose appropriate recommendations for each data category.*

Current law (and the regulatory framework which it has produced) generally distinguishes between two basic types of data, i.e. non-personal data and personal data. The phenomenon that a combination of several pieces of non-personal data may, under certain circumstances[2], result in processing of personal data, which is subject to significant regulation, is not limited solely to the field of autonomous mobility.

This paper deals with data classification in autonomous vehicles, focusing on the challenging cases of non-personal data that can turn into personal data. The initial stage involves identifying the data to be processed, followed by the classification of the identified data. Based on this classification, relevant legal obligations and recommendations are described.

The primary objective of this article is to provide guidance to data administrators (or, to use the terminology of data protection laws, data controllers) in autonomous mobility, enabling them to identify data and take appropriate measures to ensure compliance with legal regulations. The ultimate aim is to ensure that data controllers adhere to legal requirements, a goal that is critical for all data controllers. Beyond that, this article should be relevant also for other stakeholders in the autonomous mobility ecosystem, such as vehicle manufacturers and their suppliers, software application and service providers, and others.

Keywords: *Autonomous mobility, autonomous vehicles, data protection, personal data, non-personal data, mixed datasets*

I. INTRODUCTION

Autonomous mobility is currently a very dynamic field. Various types of devices hidden in autonomous vehicles are being improved, such as object recognition and decision-making by artificial intelligence. The ethical question is often the main issue here, i.e. how artificial intelligence is to make decisions when all options lead to irreversible damage. This has somewhat sidelined the more immediate issue of protection of data in these ve-

[*] Doc. Ing. Zdeněk Lokaj, Ph.D., LL.M. Associated Professor at the Department of Applied Informatics in Transportation, Faculty of Transportation Sciences, Czech Technical University in Prague, Prague, Czech Republic. ORCID: 0000-0002-0624-0430.

[**] Ing. Martin Šrotýř, Ph.D. Department of Applied Informatics in Transportation, Faculty of Transportation Sciences, Czech Technical University in Prague, Prague, Czech Republic. ORCID: 0000-0003-0049-4381.

[***] Ing. Miroslav Vaniš, Ph.D. Department of Transport Telematics, Faculty of Transportation Sciences, Czech Technical University in Prague, Prague, Czech Republic. ORCID: 0000-0002-7589-6206.

[****] JUDr. Ivo Janda, Ph.D. Partner at White & Case LLP, Prague, Czech Republic.

[*****] JUDr. Tomáš Ščerba, Ph.D. Former Local Partner White & Case LLP, Prague, Czech Republic.

[1] This article is part of the project "Protection of non-personal data and databases in autonomous systems", which is co-financed from the state budget by the Technology Agency of the Czech Republic (www.tacr.cz) under the DOPRAVA 2020+ Programme.

[2] This is mainly the issue of so-called mixed datasets, where it applies that if non-personal data cannot be unambiguously separated from personal data, the entire dataset should be treated as personal data.

hicles, but preserving the confidentiality of vehicle data is in fact one of the essential prerequisites for the successful acceptance of autonomous mobility by society and users.

In 2018, the Regulation 2016/679 of the European Parliament and the Council 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; "GDPR") came into effect, requiring entities managing or processing personal data to comply with a substantial set of new rules. However, with respect to autonomous mobility, it is necessary to go even further, as autonomous vehicles are going to process significant amounts of data in the future.

While the vast majority of this will be non-personal data and entities should treat it accordingly, there is the possibility that, with large volumes of data, some combinations of these non-personal data may allow for the possible identification of the user of the autonomous vehicle – which could be a problem, should the data only be processed according to the rules applying to non-personal data.

In principle, two specific areas can be found in the literature where non-personal data is at risk of being "converted" into personal data. First, the driver behavior model, which remains applicable on lower levels of autonomy, may directly involve the task of identifying the driver. The other area is the adjustment of vehicle parameters to the user.

The main objective of this article is to present the reader with a procedure for determining what kind of data autonomous vehicles process and retain and related relevant information on the legal rule which must be observed, depending on the type and scope of data processed. The article also makes recommendations as to what actions and behavior facilitate compliance with the data processing and retention rules.

The article first gives an overview of the state of scholarly work on the issue. It then gives a brief overview of the data flow in autonomous vehicles and explains the general procedure for categorizing such data into classes. This is followed by the process of assigning data classification and a description of the legal obligations according to the nature of the data. In the last section, recommendations for each data classification are being proposed.

II. LITERATURE REVIEW

Fialová and Matejka[3] focus on real-time data collection and processing of data in the context of the operation of autonomous vehicles, including issues related to this process and the impact on personal privacy. They offer the solution of adopting specific legislation on the processing of personal and non-personal data. Their article points out that the current legal framework of the GDPR is inadequate.

Supriyadi[4] addresses the issue of personal data differentiation in the context of big data and the possible concept of their precise identifiability. The research shows that factors

[3] FIALOVÁ, E., MATEJKA, J. Data Protection and Privacy Issues in the Use of Autonomous Vehicles. *The Lawyer Quarterly*. 2022, Vol. 12, No. 4, [2023-04-25]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/531>.

[4] SUPRIYADI, D. The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*. 2023, Vol. 3, No. 1, [2023-02-05]. Available at: <http://www.jhcls.org/index.php/JHCLS/article/view/71>.

relevant to understanding the terminology in data protection law are relevant to assessing the direct or indirect identification of an individual. These are already included in EU legislation.

Sen and Gopal[5] deal with the issue of non-personal data in India and adjacent areas. Their paper responds to a local government framework dealing with non-personal data, outlining and analyzing its main points. It also suggests approaches to the further development in non-personal data management. In particular, it explores the links between the proposed framework and its potential to accelerate innovation for public use.

Sandeepa et al.[6] provide a comprehensive study of the protection of personal and non-personal data in B5G/6G in order to identify the current status and future options to ensure the protection of personal data. Their paper compares these data types in detail and identifies gaps and threats, based on which possible privacy solutions are proposed for future use within the B5G/6G network.

Another paper[7] defines automation in different areas of transport and touches on ethical issues related to the operation of different vehicles. It also discusses the operation of autonomous vehicles from the security and data protection perspective. It attempts to define autonomous vehicles by comparing them with other modes of transport that have a higher degree of automation. It defines how autonomous vehicles can affect our lives and privacy as well.

The article by Costantini et al.[8] describes how GDPR regulation affects data in autonomous vehicles. In addition, it describes the approach to regulation in several countries outside Europe, such as Brazil and New Zealand. It concludes by comparing these approaches and providing suggestions for policy recommendations at local, European, and international levels.

The next paper in our overview[9] focuses on the potential use of Event Data Recorders for Autonomous Driving (EDR/AD) in intelligent transportation systems, describing security, data provenance and privacy, and other regulatory and technical issues with respect to the many stakeholders and interest groups involved.

Another article[10] identifies the legal challenges in the field of insurance with regard to smart technologies. It explains the reasons for providing vehicle data to insurers and identifies the values and principles promoted by the EU with regard to smart technologies and

[5] SEN, S, GOPAL, I. Non-Personal Data: Policy, Economics and Technology. *SSRN*. 2021 [2023-02-05]. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3911698>.

[6] SANDEEPA, Ch., et al. A Survey on Privacy of Personal and Non-Personal Data in B5G/6G Networks. In: *arXiv preprint arXiv:2212.06987* [online]. 14. 12. 2022 [2023-05-02]. Available at: <https://arxiv.org/abs/2212.06987>.

[7] CROITORU, I., LAURENȚIU, A., ZĂGAN, P. A. Self-Driving Vehicles. A Perspective on Ethics. *European Journal of Law and Public Administration*. 2022, Vol. 9, No. 2, [2023-05-02]. Available at: <https://www.lumenpublishing.com/journals/index.php/ejlpa/article/view/5962>.

[8] COSTANTINI, F., et al. Autonomous vehicles in a GDPR era: An international comparison. *Advances in transport policy and planning*. 2020, Vol. 5, [2023-05-02]. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S2543000920300081>.

[9] VEITAS, V. K., DELAERE, S. In-vehicle data recording, storage and access management in autonomous vehicles. In: *arXiv preprint arXiv:1806.03243*. [online]. 2018 [2023-05-02]. Available at: <https://arxiv.org/abs/1806.03243>.

[10] KRAUSOVÁ, MATEJKA, A. J. Autonomous vehicles and in-vehicle data in the context of motor insurance. *The Lawyer Quarterly*. 2020, Vol. 10, No. 2, [2023-05-03]. Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/403>.

summarizes the related legislation. The results provide a basis for further research on how to balance the provision of vehicle data for the purpose of insuring autonomous vehicles.

Collingwood[11] addresses privacy implications and liability issues. The disadvantage of using an autonomous vehicle is the loss of the ability to be relatively anonymous, as the data will contain information about the driver, route, passengers, etc., which is used by companies operating autonomous fleets to analyze their services. Another issue addressed in the paper is liability in the event of an accident. The article points out that, as innovation in autonomous mobility continues apace, one must not forget the need for legislation to keep up with the technological development.

Bloom et al.[12] describe the sophisticated sensors used to capture continuous environmental data in self-driving vehicles. The paper explores people's perception of the sensory and analytical capabilities of self-driving vehicles, how comfortable they are with these different capabilities, and their willingness to take steps to opt out of data collection.

The next paper[13] describes the "Vehicular Ad-hoc Network" (VANET), a technology important for Intelligent Transportation Systems providing safe and convenient driving, route optimization, accident prevention, communication channel security and network security against malicious virus/spyware attacks. It provides resource allocation schemes for different aspects of VANET, and analyzes and discusses security and message privacy issues, autonomous vehicle communication, and network issues.

Lim and Taeihagh[14] analyze autonomous vehicles as a potential transport solution for smart and sustainable development and look at the options for mitigating negative social, economic and environmental impacts. Their paper identifies privacy and cybersecurity aspects of AVs that are important for smart and sustainable development. It also assesses the efforts of governments to address cybersecurity risks through regulations.

Gaeta[15] focuses on the issue of the protection of personal data processed by autonomous vehicles and the related profiling process of users using the technology, who are often unaware of the consequent risks from possible hacking of personal data. This is due to the development of autonomous and connected driving in smart cities.

The paper by Růžička et al.[16] gives an example for processing parameters (mostly non-personal data) from detectors, FCD data or data from information systems, which in the

[11] COLLINGWOOD, L. Privacy implications and liability issues of autonomous vehicles. *Information & Communications Technology Law*. 2017, Vol. 26, No. 1, [2023-05-03]. Available at: <https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1269871>.

[12] BLOOM, C., et al. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. *Symposium on Usable Privacy and Security (SOUPS)*. 2017 [2023-05-03]. Available at: <https://www.usenix.org/system/files/conference/soups2017/soups2017-bloom.pdf >.

[13] NAYAK, B. P., et al. Autonomous Vehicles: Resource Allocation, Security, and Data Privacy. *IEEE Transactions on Green Communications and Networking*. 2021 [2023-05-03]. Available at: <https://ieeexplore.ieee.org/abstract/document/9530556>.

[14] LIM, H. S. M., TAEIHAGH, A. Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*. 2018, Vol. 11, No. 5, [2023-05-03]. Available at: <https://www.mdpi.com/1996-1073/11/5/1062>.

[15] GAETA MARÍA, C. Data protection and self-driving cars: The consent to the processing of personal data in compliance with GDPR. *Communications Law*. 2019 [2023-05-03]. Available at: <https://d1wqtxts1xzle7.cloudfront.net>.

[16] RŮŽIČKA, J., et al. Big Data Application for Urban Transport Solutions. *Smart City Symposium Prague (SCSP) IEEE*. 2022 [2023-05-03]. Available at: <https://ieeexplore.ieee.org/abstract/document/9792538>.

future will also be used by autonomous vehicles in certain selected areas. It is obvious that large amounts of data will be involved.

Another article[17] discusses the existing risks of vehicle cyber security and road safety threats. It identifies the key principles of cyber security in vehicles, describes the existing legal framework and identifies its gaps. Current legislative measures focus on preventing unauthorized access to vehicle systems but do not identify the steps necessary to limit the damage in the event of unauthorized access.

Kemp[18] describes the support for the development and deployment of driverless cars and 'connected autonomous vehicles' (CAVs) that can communicate with each other and with U.K. infrastructure. No realistic analysis has been made of the safety regulation of these vehicles or the ability to control their interaction with other road users. It summarizes the safety regulatory regime for automated transport systems.

Hussein et al.[19] discuss methods and issues of security and privacy for VANETs and vehicular cloud computing. Location privacy methodologies are developed to protect confidential information about the vehicle and its driver. The paper discusses data management models in VANETs and compares them with cryptography models in terms of different types of attacks, and discusses simulation tools and applications in vehicular networks, including architecture and security and privacy issues.

The next article in our overview[20] deals comprehensively with the issue of personal data protection in autonomous driving systems from the perspective of all stakeholders. It touches marginally on cybersecurity and privacy in electronic communications. It provides a general description of autonomous driving systems, their elements, and the key players involved in the generation or processing of personal data. Finally, it proposes solutions to protect data across the entire process using the principles of "privacy by design" and "privacy by default".

Mlada et al.[21] deal with the description, operation, and handling of digital privacy of natural persons and GDPR from the perspective of autonomous vehicles. With the development of autonomous systems, the sensitive and systematic handling of personal data needs to be addressed in order to ensure the smooth development and use of autonomous vehicles in the future, which is why the paper analyzes and describes the different elements from the perspective of privacy protection. It offers measures and steps that need to be taken to successfully secure the personal data of all stakeholders involved in autonomous systems.

---

[17] VELLINGA, N. E. Connected and vulnerable: cybersecurity in vehicles. *International Review of Law, Computers & Technology.* 2022, Vol. 36, No. 2, [2023-05-03]. Available at: <https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2060472>.

[18] KEMP, J. R. Regulating the safety of autonomous vehicles using artificial intelligence. *Communications Law* 2019, Vol. 24, No. 1, [2023-05-03]. Available at: <https://eprints.lancs.ac.uk/id/eprint/131659/>.

[19] HUSSEIN, N. H., et al. A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions. *IEEE Access.* 2022, Vol. 10, [2023-05-03]. Available at: <https://ieeexplore.ieee.org/abstract/document/9856630>.

[20] LOKAJ, Z., et al. Ochrana osobních údajů v systémech autonomního řízení. Co je nezbytné pro bezpečné fungování a jak toho dosáhnout? *Revue pro právo a technologie.* 2021, Vol. 12, No. 24, [2023-05-03]. Available at: <https://www.ceeol.com/search/article-detail?id=1011209>.

[21] MLADA, M., et al. Protection of personal data in autonomous vehicles and its data categorization. *Smart City Symposium Prague (SCSP) IEEE.* 2022 [2023-05-03]. Available at: <https://ieeexplore.ieee.org/abstract/document/9792557>.

Vaniš et al.[22] describe the current state of the legal framework regarding data, mainly non-personal data, in autonomous vehicles, reflecting the further development and increased installation of embedded electronic systems in new vehicles. In line with the concept of smart cities, a huge amount of data is being generated, hence the need to introduce a classification of data according to the degree to which the data qualifies as personal. This paper offers a description of data classification as well as the design of software to help manufacturers and administrators with data protection issues.

The articles described in the above overview are for the most part dedicated to the assessment of the current legislative framework (GDPR), security and protection of personal data in the context of processing and sharing data within autonomous vehicles. A number of them studies the implications of the development and increased use of autonomous vehicles for the lives of all stakeholders. Technologies for intelligent transport systems, designed to secure data against cyber-attacks, are also discussed, including an example of hacking into these vehicles and misusing their controls, with the consequent risk of health hazards.

Even a cursory search of the articles makes it evident that the issue of non-personal data is not given sufficient attention. In contrast to the aforementioned articles, this article focuses specifically on non-personal data, and on the circumstances under which it could become personal data.

III. DATA OVERVIEW

There are many ways how to deal with data in autonomous vehicles. For the purposes of this article, we will focus mainly on non-personal data that may be directly related to the driving or crew of the autonomous vehicle. Unfortunately, it is not possible to analyze all data within an autonomous vehicle. Therefore, we will divide the data into different categories and focus on the parameters within each category, which will then be used to illustrate the classification process and the resulting recommendations in the next section of the paper. The division of these data and a short description including examples of parameters is shown in Tab. 1.

[22] VANIŠ, M., et al. Classification of non-personal data in autonomous vehicles. *Smart City Symposium Prague (SCSP) IEEE*. 2022 [2023-05-03]. Available at: <https://ieeexplore.ieee.org/abstract/document/9792536>.

Tab. 1 – Overview of data types in an autonomous vehicle

Data category	Description	Examples of parameters
Operational	Data based on the SAE J1939 standard which contains all parameters that can flow in a common vehicle.	Driver's Identification, Tachograph, After treatment Reagent Information
OBD + CAN	Parameters that can be read over the CAN bus via the OBD interface.	VIN Gas pedal pressure Oil temperature
Data related to a higher level of autonomy	Parameters related to autonomous driving (camera, microphone, lidar or radar data).	Point data record length Number of point records Video collection Audio record
Infotainment	Parameters and data that can be included in the vehicle's infotainment system, so-called personalized data.	Profile name Contacts GPS data Software version
EDR + DSSAD	Data from the EDR unit, which is used for analysis in the event of an accident, and the DSSAD system, which provides information on the interactions between the driver and the autonomous system.	Side air bag deployment, time to deploy, driver Engine RPM[23] Occupant size classification, driver
Biometric	Data for the purpose of unambiguous identification of persons.	Finger prints Eyes
Vehicle status	Data related to vehicle settings. Some of these settings are directly controlled by the driver.	Time Speed Limit Warning Seat position
C-ITS	Data extracted from messages in cooperative systems	Type of vehicle Lateral acceleration Station ID

Obviously, the data produced in the vehicle could be divided also in other ways. At the same time, it is clearly not feasible to list all parameters flowing in the vehicle within the confines in this article. Based on the analysis of the parameters mentioned, a proposal for their classification was developed.

[23] Revolutions per minute.

a. Data classification

In order to correctly determine the characteristics of the data (i.e. whether data processing should be regulated by legislation for personal or non-personal data), a classification has been proposed. The aim is to establish such classification for each parameter in the vehicle according to the following procedure:

- If it is a sensitive (or in terms of GDPR – special category) parameter, the classification of the parameter is rated as Level 4 (personal data). For example, all biometric data are considered Level 4. All these parameters are unambiguous in terms of legislation and the classification is quite clear.
- Where data directly referring to the data subject according to the definition of personal data are involved, again these parameters are rated at Level 4.
- Data that indirectly identifies the user was rated at Level 3 (data which will on balance tend to qualify as personal data). Again, this data is relatively precise in terms of the legal definition (e.g. vehicle VIN code or passenger classification).
- The other parameters are first rated as Level 1 – non-personal data.
- Certain data, however, while non-personal by nature, may in combination with other non-personal data become personal data. This problem is addressed by so-called datasets, which have been created based on scholarly articles[24] dealing with the identification of users based on their behavior or vehicle settings. Parameters falling into this category are rated at Level 2. Tab. 2 contains the basic 4 datasets that are regularly found in vehicles at the moment.[25]

[24] KWAK, B. I., WOO, J. Y., KIM, H. K. *Know your master: Driver profiling-based anti-theft method. 2016 14th Annual Conference on Privacy, Security and Trust (PST)*. Auckland: Institute of Electrical and Electronics Engineers Inc., 2016, pp. 211–218.

MARCHEGIANI, L., FAFOUTIS, X. How Well Can Driverless Vehicles Hear? An Introduction to Auditory Perception for Autonomous and Smart Vehicles. *IEEE Intelligent Transportation Systems Magazine.* 2021, Vol. 14, No. 3, pp. 92–105.

PARK, X. W. M. J., CHENG, Y. Y. D., KITANI, M. O. T. *All-In-One Drive: A Comprehensive Perception Dataset with High-Density Long-Range Point Clouds*. Pittsburgh: Robotics Institute, Carnegie Mellon University.

[25] Additional datasets have been identified as part of the research. The authors of this paper are prepared to provide more information.

Tab. 2 – Datasets examples

Dataset 1	Vehicle speed, Brake pedal position, Gas pedal position, Engine speed, Following distance from vehicle ahead, Brake pedal pressure, Gas pedal pressure
Dataset 2	Steering wheel, Vehicle speed, Engine speed, Brake position, Vehicle direction/speed, Cruise Control/Vehicle Speed, Adaptive Cruise Control, Electronic Brake Controller 1, Oil Pressure
Dataset 3	Trip Fuel Information (Gaseous), Trip Fuel Information (Liquid), Fuel Consumption (Gaseous), Fuel Consumption (Liquid), Engine Temperature 1, Vehicle Dynamic Stability Control 2, Wheel Speed Information, Electronic Transmission Controller #8, Tire Condition
Dataset 4	Mirrors, Seat position, Temperature settings, Fan position, Other driver's adjustments

IV. IDENTIFICATION AND CLASSIFICATION OF PROCESSED DATA

Our classification contains 4 different options. However, in terms of legislation, there are only two possible types of data: personal and non-personal. On this basis, for each identified parameter, it is necessary to first determine its classification and only then to carry out the procedure described in the following section, which should provide information on how to treat this parameter from the perspective of the applicable laws.

a. Data determination and classification

In a first step, it is necessary to ensure that the processed data are correctly classified. It is not possible within the scope of this paper to encompass all parameters[26] that flow in an autonomous vehicle. Following the instructions in Section 3.1 is recommended.

In addition, for each parameter, it is necessary to specify the type of processing of this data. In the case of online data that is not further processed, i.e. only the value of the parameter is checked and then discarded, it is not necessary to deal with the parameter further, unless it has been classified as Level 4. However, care should be taken in cases where a parameter is stored at a time when its value is not in the standard range, as it is possible that not only the value of this parameter but also others will be recorded at the time.

It may also happen that the device processes several different parameters from different sources. For the source itself, the parameter is treated as non-personal because it has no direct connection to any other parameter, but if it is, for example, the vehicle central unit which processes data from different sources, some of which might contain identifiers

[26] Within the project Law protection of traffic-data databases in autonomous driving systems – TL05000681, a classification for a large group of parameters was developed. For more information, please contact the authors.

linked to a specific natural persons, there is an increasing chance that the parameter may have to be treated as personal.

The procedure is therefore the following:

- Determination of all data that is processed within a single device. If there are multiple devices, it is necessary to determine this data for all devices separately.
- Classification of the identified data within each device (see Section 3.1).

There are several possible combinations of the classification of these parameters:

1. Level 1 parameters are processed – thus only non-personal data is processed and therefore only the recommendations and legal obligations from Sections 5.2 and 6.2 apply,
2. The processed parameters are not all at Level 1, but some parameters are classified at Level 2 – i.e., processing of non-personal data is taking place, as well as data that could result in personal data in certain circumstances. It is advisable to think about the parameters at Level 2 in the following way:
   a. for data with Level 2 classification, the retention period of the data should be set to be minimal,
   b. one needs to check whether the data being processed is part of a dataset that could lead to the identification of the driver.

   When data is retained for more than a very short period of time (where the parameter is set to a maximum of 1 second) and it is assumed that the parameter could lead to the identification of the vehicle driver, it is essential that the respective stakeholders strongly consider the recommendations and legal obligations also for personal data, see Section 5.1 and 6.1.
3. Parameters are also processed at Level 3 – this data already contains information directly related to the vehicle, which is why it is best treated as personal data.
4. The processed parameters include Level 4 parameters – these are personal data and the user must comply with the legal obligations and recommendations listed in Section 5.1 and 6.1.

b. Datasets

Therefore, when a parameter is classified as Level 2, the following procedure must be performed. For each defined parameter that is being processed, check its presence in the dataset and whether there are other processed parameters in the dataset. Here follow some possible conclusions:

- The selected parameter is not part of the same dataset as other processed parameters, in which case the data pertaining to this parameter can be processed as non-personal data (with a note that it does not have to be non-personal data under all circumstances)
- The selected parameter is part of the same dataset as some other processed parameters, but these parameters do not form the whole dataset. It is not specified exactly

how to proceed in view of the legislation. However, it is highly recommended to implement the measures set out specifically for this situation, see Section 6.3. If these measures cannot be implemented, it is recommended that one proceeds to treat the data as personal data.

- The selected parameter is a part of the same dataset as other processed parameters and moreover these parameters form the entirety of the dataset. It is recommended to process the data as personal data.

V. LEGAL OBLIGATIONS

As we shall see, from a legal point of view, the only relevant distinction is that between personal and non-personal data.

a. Personal data

The issue with the potential impact of personal data regulation on the mixed datasets described in the sub-section above is caused by the broad definition of "personal data" used by the GDPR regulation. Pursuant to Art. 4 (1) GDPR, personal data is understood to mean "any information related to an identified or identifiable natural person" (each such person hereinafter a "data subject"), whereas "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier."[27] In an electronic environment in particular, however, natural persons may be assigned identifiers used by devices, apps, tools, and protocols that leave trails. These data trails, even though they do not directly identify the person in question, may in and by themselves qualify as personal data within the meaning of the above-cited definition,[28] especially in conjunction with unique identifiers or with other information processed or obtained by such tools from third parties.[29]

This means that even data which by a first approximation qualifies as non-personal data poses the risk of identification of a natural person when combined with another identifier. This also holds if someone other than the controller has the legal and technological means to link a non-personal data item to the identified individual if they expend reasonable effort on such exercise.[30] This too, then, is a case (alongside mixed datasets) where originally non-personal data comes within the full purview of GDPR – i. e., will be considered personal data – because of its linkage to potential identifiers.

---

[27] Identifiers include e.g. name, identification number, location data, an online identifier (IP address, cookies), or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

[28] Cf. Recital (30) GDPR.

[29] In order to treat information as "personal data" within the meaning of Art. 2 (a) of Directive 95/46 or, today, GDPR, it is not necessary that all the information enabling the identification of the data subject be in the hand of one person (paras. (41) – (43) of CJEU judgment C-582/14 – Patrik Breyer of 19 October 2016).

[30] The assessment whether a given expenditure still qualifies as "reasonable" comprises objective factors (time, technical complexity, nature of the data in question) as well as contextual factors (data volume, likelihood of identification given e.g. population density etc.).

As for data flows in autonomous vehicles, given the interconnectedness of all systems (including personal devices that can be connected to the vehicle)[31] and vehicles as such (both with traffic infrastructure and among themselves), any piece of data which in one way or another depends on the activities of the individual operating the vehicle may potentially become personal data. According to the EDPB, special attention is warranted with respect to location data, biometric data (and any special category of data as defined in Art. 9 GDPR) and data that could reveal criminal offenses or traffic violations.[32] In accordance with what has been said above with respect to the principle of integrity, the processing of such types of personal data which includes a large number of data subjects will almost always[33] require an assessment of the impact which the contemplated data processing operations will have on personal data protection.

Within the territory of the European Union, all data that is considered personal data, whether because of its own nature (i.e., because it can be used to identify, directly on in combination with other identifiers, a natural person) or because of its connection with other personal data, comes within the purview of GDPR. This applies even to a data controller established outside the EU, if they offer goods or services to data subjects in the EU or monitor the behavior of data subjects in the EU.

The processing of personal data will thus always be governed by the general principles for the protection of personal data.[34] The data must be processed for one or several specific legitimate purposes, and only for as long and in such scope as is absolutely necessary to attain the declared purposes. The controller must process current personal data and observe the principle of integrity and confidentiality,[35] which also entails protecting the data using appropriate technical or organizational measures against unlawful processing or accidental loss. The controller is liable for the data processing being at all times transparent, fair, and lawful toward data subjects.

The lawfulness of processing is in turn always based on the legal grounds for processing which are generally defined in Art. 6 GDPR.[36] As a rule, in the case of autonomous vehicles, any of these grounds may apply. Operators of autonomous driving systems, car manufacturers, and providers of additional applications not directly related to the operation of the vehicle may process personal data of the driver (or other persons) on grounds of this being

[31] "Also, the development of standalone mobile applications, i. e., applications that are independent of the vehicle (for example, relying on the sole use of a smart phone), to assist drivers is included in the scope of this document, since such applications contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data within the vehicle *per se*." (Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications of 9 March 2021, p. 8).

[32] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications of 9th March 2021, p. 15.

[33] With the exception of processing that takes place based on a legal regulation of the EU or a Member State.

[34] Cf. Art. 5 GDPR.

[35] Where a type of processing in particular 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 shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The GDPR enumerates types of processing which always requires such a data processing impact assessment (DPIA). Processing the personal data of a large number of users related to, *inter alia*, real-time tracking of their location, habits, behavior etc. will almost certainly always require a DPIA.

[36] Or, in the case of special-category data, grounds for processing as defined in Art. 9 (2).

necessary for compliance with a legal obligation, or for performance of a contract or in certain cases based upon consent of the data subject or in order to protect the legitimate interests of such entities. If the data controller is the owner of a fleet of autonomous vehicles, then they will process the personal data for the performance of a contract with the data subject. Insurance companies, government agencies, public-service organizations etc. will process some personal data on grounds of their legal obligations or for performance of a task in the public interest or in the exercise of official authority. Finally, processing may be necessary for the protection of vital interests of the data subject.

In addition, the principle of transparency and fairness mandates that the data controller informs the data subjects of the processing of their data and ensures that their rights are being respected (i.e., in particular, the data controller must respond to any requests whereby data subjects exercise their rights, at the very least informing them that their request cannot be accommodated, and for what reason). Depending on the scope provided by the respective purpose of and legal grounds for the processing, the data subject will have the right of access to their personal data, the right to rectification or erasure of personal data, the right to demand that the processing of their personal data be limited, or the right to object. In addition, if personal data is being processed for the purpose of performance of a contract, then the data subject has a right to the portability of such data.

In addition, data controllers must take appropriate technical and organizational measures in order to ensure that the level of protection[37] corresponds to the risk associated with the specific type of processing, and ensure data protection by design and by default, both before and during processing, and regularly review the effectiveness of the chosen measures and guarantees. The measures and guarantees for processing personal data in the field of autonomous vehicle operation and the minimization of personal data must be taken into account already at the time at which the relevant systems are being designed, and are subject to regular reviews and updates.

Given that the operation of autonomous vehicles will characteristically involve a plurality of participating entities who will process personal data, an assessment will be necessary to determine who, within a given system, is the data controller or the data processor, and which entity will strictly need traffic data so that data anonymization becomes necessary. The operation of autonomous vehicles will often entail what is known as joint data controlling, i.e., two or more data controllers determine the purposes and means of data processing. These controllers ought to enter into (written) contract between them[38] which defines each controller's share of responsibility for the fulfillment of obligations (especially with respect to the exercise of data subjects' rights).

[37] In the event of a breach of personal data security, the data controller must promptly notify the Data Protection Office hereof, i.e., no later than within 72 hours from the moment in which they learned of the breach, unless it is unlikely that the breach will have consequences in the form of a risk for the rights and freedoms of natural persons.

[38] The obligation to enter into a 'controller agreement' is not a statutory duty under the GDPR, but follows from the legitimate need to stipulate the individual rights and obligations between two parties. Where the purposes and means of processing are determined by one controller and the other entities submit to that controller's instructions, then this qualifies as a controller-processor relationship, and in such a case, the participants must conclude a processor agreement. The obligation to enter into a data processing agreement among controller and processors is a statutory duty that follows from GDPR (cf. Art. 28 (3)).

For the foreseeable future, GDPR will certainly remain the key piece of legislation in the realm of personal data protection. Even so, it is advisable to take note of various new legislation (especially on the level of the EU) which is being drafted in response to the development of new technologies. A more recent example in this respect is the ePrivacy Regulation, which is currently in the state of a draft proposal; the wording as it stands would also apply to the eCall system and more generally to electronic communication between machines (M2M) – i. e., among other things, to autonomous vehicles. Within the context of GDPR, this Regulation is expected to serve as the legal basis for processing certain types of electronic communication data (e.g. for the purpose of provision of services, ensuring communication security, or preventing and detecting attacks on end devices), including metadata. It is also certainly advisable to carefully watch the decision-making practice of the EDPB and national supervisory authorities evolve. It stands to reason that this practice will take an interesting development within the next few years when it comes to autonomous vehicles, e.g. with respect to data anonymization (esp. localization data anonymization).

b. Non-personal data

The free movement of non-personal data is guaranteed across the EU under Regulation (EU) 2018/1807 of the European Parliament and the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union ("**Regulation 2018/1807**"); this Regulation stipulates the rules governing Member States' data localization requests (which are being limited to requests justified on grounds of public security),[39] data availability for competent authorities,[40] and the porting of data for professional users based on codes of conduct for the support of transparency and interoperability (whereas the Regulation anticipates the development of such codes).[41] Regulation 2018/1807 addresses various levels of data processing, from storage (Infrastructure-as-a-Service, IaaS) to platform-based processing (Platform-as-a-Service, PaaS) to applications (Software-as-a-Service, SaaS).

Non-personal data processed within the context of autonomous vehicles will as a rule constitute entire databases. In the field of road traffic and at the interface between road-based ITS and ITS used in other modes of transport, the creation, administration, and sharing of databases is subject, in particular, to Directive 2010/40/EU of the European Parliament and the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (the "ITS Directive")[42] and various related EC regulations adopted on its basis,[43] with the goal to maximize accessibility and regular updates of entire (both static

[39] Cf. Art. 4 of Regulation 2018/1807.

[40] Cf. Art. 5 of Regulation 2018/1807.

[41] Cf. Art. 6 of Regulation 2018/1807. In the field of autonomous mobility in particular, the creation of such codes is more than desirable, given the need for clear and unambiguous rules for the processing of non-personal data and the preservation of transparency and trustworthiness toward users (this being a key parameter for acceptance of these new technologies).

[42] In the Czech Republic, the ITS Directive was transposed by way of an amendment to Act No. 13/1997 Coll., on public roads and ways.

and dynamic) databases. Among other things, this facilitates the provision of the interoperable eCall service and other real-time traffic information services across the EU.

The majority of data flowing within autonomous vehicles will by its nature be non-personal data, and as such may be handled without restrictions (irrespective of, among other things, location), in accordance with the above-mentioned Regulation 2018/1807; the stakeholders participating in the operation of autonomous vehicles or transport infrastructure (including public authorities) may freely share such data.

Issues arise when non-personal data (whether as part of a database or of a mixed dataset) cannot be reliably separated from data which might in certain constellations qualify as personal data.

Mixed datasets comprise both non-personal and personal data. According to the scholarly literature[44] and the guidelines of the EDPB (formerly the WP29 working party), if the non-personal data in such a dataset are inextricably linked to personal data, as is often the case within IoT, AI, and more generally smart systems and similar new technologies, then the entire mixed dataset is fully subject to the relevant personal data protection rules, even if the said linkage within a given dataset concerns only a small portion of the total data volume.

According to the European Commission, the term "inextricably linked" refers to a situation in which the separation of non-personal data from personal data within one dataset by the controller "would either be impossible or considered by the controller to be economically inefficient or not technically feasible."[45]

VI. RECOMMENDATIONS

According to the types of data processed, we have divided our recommendations into three areas:

- recommendations for working with personal data (section 6.1),
- recommendations for working with non-personal data (section 6.2),
- recommendations for working with data with Level 2 classification (section 6.3).

a. Personal data (Level 3, 4 classification)

The proper application of the GDPR to the processing of personal data by autonomous vehicles is a matter of utmost importance. As previously discussed in Section 7.2.1, the

[43] To mention just the most important ones: Commission Regulation (EU) 885/2013 on the provision of information services for safe and secure parking places for trucks and commercial vehicles; Commission Regulation (EU) 886/2013 on minimum traffic information; Commission Regulation (EU) 1315/2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No. 661/2010/EU; Commission Regulation (EU) 2015/962 with regard to the provision of EU-wide real-time traffic information services; and Commission Regulation (EU) 2017/1926 with regard to the provision of EU-wide multimodal travel information services.

[44] BYGRAVE, L. A., TOSONI, L. Article 4 (1). Personal data. In: Christopher Kuner – Lee A. Bygrave – Christopher Docksey (eds.). *The EU General Data Protection Regulation (GDPR) - A Commentary*. Oxford: Oxford University Press, 2020, p. 113.

[45] Communication from the Commission on the Regulation on a framework for the free flow of non-personal data in the European Union of 29th May 2019, p. 10.

GDPR will apply to the operation of autonomous vehicles whenever such vehicles or related services are offered to data subjects within the EU. It is imperative to closely monitor data flows and communicate effectively with data subjects, especially in relation to third-country controllers or processors. In the latter case, it is essential that transparent descriptions of the data processed by the specific third-country controller or processor are being provided, along with a description of the purpose for which the data is being processed, the legal basis for processing, and the measures taken to protect such data. Generally, a level of protection equivalent to that provided to data subjects by the GDPR must be ensured, which is usually achieved through international treaties or standardized contractual arrangements (e.g., with respect to the US).

Given that the operation of autonomous vehicles involves multiple participants, it is necessary to assess who serves as the controller, who serves as the processor in a particular system, and which participant requires only anonymized data from the operation. It is essential not only to inform data subjects of all entities that have access to their data but also to conclude relevant contracts in the context of controller/processor or joint controller relationships. While the relevant contract is a direct obligation based on the GDPR in the case of a processor, the same does not apply to joint controllers. Nonetheless, it is highly advisable to avoid potential disputes between controllers and to promote transparency to data subjects.

Personal data must be processed for specific and legitimate purposes, based on one of the legal bases for processing, which are exhaustively listed in Articles 6 and 9 of the GDPR. When determining the purpose, it may be advisable to take inspiration from the IWGDPT guidelines, which define several purposes. Given that this is an international organization, future harmonization efforts can be expected both internationally and in Europe.

While processing based on a legal obligation (whether related to AML, tax regulations, or industry regulation) or for the purpose of contract performance is relatively straightforward, the legal basis of legitimate interest of the controller requires an additional balancing test to demonstrate that this legitimate interest may indeed outweigh the privacy and personal protection rights of data subjects. The legal basis of consent should only be used in cases where processing cannot be safely subordinated to another legal basis at the time, primarily because consent can be revoked.

Furthermore, data should only be processed to such extent and for such period as is strictly necessary. Therefore, retention periods and subsequent anonymization or pseudonymization mechanisms should be set consistently and restrictively where necessary. Where possible, data should only be retained for the period required by law in the case of a limitation period. Retention may be problematic in the case of location data. As the EDPB guidance makes clear, location data may be indicative of behavioral patterns of the driver or other persons and thus might, in combination with certain other data, classify as biometric data, which, if used to identify or authenticate those persons, will constitute a special category of personal data under the GDPR regime. Therefore, we recommend that wherever possible, such data be deleted or anonymized immediately after processing.

The controller is obligated to provide the data subject with information on their rights concerning the processing of their personal data, including but not limited to the right of access, the right to rectification, the right to erasure, the right to restrict processing, and the right to object. The controller must respond to the data subject's request to exercise

these rights and, at a minimum, inform the data subject of the reasons why their request cannot be accommodated, particularly in cases where data processing is necessary for the controller to comply with a legal obligation. In cases where personal data will be processed to perform a contract, the data subject has the right to portability.

In order to ensure the consistent protection of personal data and to assess the effectiveness of the safeguards implemented, it is recommended that the obligation to ensure the deliberate and standard protection of personal data be taken into account, and that such measures be reviewed and updated on a regular basis, particularly in the design stage of the relevant systems.

If a personal data breach occurs, the controller must report the breach to the Data Protection Authority without undue delay and at the latest within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Given the potential for a single incident to affect countless vehicles, the introduction of an automated mechanism to record and send error messages may be advisable.

Where a particular type of processing, in particular one that relies on the use of new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing, the controller must, unless such processing is carried out pursuant to a legal obligation, conduct an assessment of the impact of the intended processing operations on the protection of personal data prior to the processing. Processing personal data of a large number of data subjects, inter alia on their real-time location, habits and behavior, etc., will almost certainly require an impact assessment.

In addition to the obligations imposed on controllers and processors by the GDPR, compliance with other rules and regulations affecting the processing of personal data must also be ensured. This will include both the guidance documents of the EDPB and similar organizations, which may serve as interpretative rules of the GDPR, as well as the regulation of eCall and electronic communications. As regards the storage or use of data in terminal devices, the ePrivacy Directive must be followed. In the future, the security of electronic communications itself should be covered by the ePrivacy Regulation, which will limit the processing of electronic communications data and metadata to certain specific exceptions, similar to the GDPR. We therefore recommend monitoring the development of this legislation and starting implementation as soon as possible. In the Czech legal environment, this will include in particular the Data Protection Act (Act on the Processing of Personal Data), which sets forth specific requirements for public entities.

b. Non-personal data (Level 1 classification)

From a legal perspective, the data generated by an autonomous vehicle or required for its operation may be considered non-personal data unless it can be linked to a specific natural person. The processing of such data is governed by the Regulation on the framework for the free flow of non-personal data within the European Union. This regulation aims to ensure the free flow of data, regardless of its location, and imposes an obligation on controllers or processors to allow access to such data by competent authorities and other entities, regardless of their domicile, if allowed by law.

Codes of conduct promoting transparency and interoperability are foreseen under the Regulation, and their development should be monitored to maintain transparency and trustworthiness towards users. In the field of autonomous mobility, the development of such codes is essential to establish clear rules for the processing of non-personal data. This will also enhance the acceptance of these new technologies.

Autonomous vehicles also process entire databases, especially for real-time monitoring and sharing of traffic information across the Union and the operation of the eCall system. The ITS Directive, the PSI Directive, and the INSPIRE Directive are important documents for the creation, management, and provision of database data. The Act on Roads and the Copyright Act regulate this area in the Czech Republic.

The purpose of these regulations is to ensure maximum accessibility and regular updating of entire databases, both static and dynamic. It is the responsibility of vehicle or software manufacturers to ensure the smooth flow of data from the databases and to securely separate this data from data that could potentially constitute personal data. Failure to do so risks creating a mixed dataset and transforming non-personal data into personal data.

The experts involved in this project have put forth the following recommendations:

1. In producing manuals for autonomous vehicle services or devices, it is advisable to include a section that provides information about the data and data processing. It is important to note that data which is currently considered non-personal may become personal data in the future, with significant privacy implications for users.
2. Keeping up-to-date with relevant legislation and technical developments is crucial, particularly in the areas where the autonomous vehicle market is expected to develop most.
3. Security incidents related to the processing of non-personal data should be captured, created, and shared.
4. Regular and ad-hoc training on changes in legal and technical areas, related not only to the operation but also to the development of autonomous vehicles, should be conducted.
5. Competencies and responsibilities for the implementation of measures in the area of non-personal data processing should be established.
6. The drafting and passage of new laws related to autonomous vehicles, including decisions of relevant law-making bodies in controversial cases, should be closely monitored.

c. Data with Level 2 classification

In the context of autonomous vehicles, data that is initially considered non-personal can become personal if it can be combined with other data to identify individuals. The determination of whether such identification is possible depends on various objective and contextual factors. As such, any non-personal data that is part of a mixed dataset with personal data should be treated as personal data if there is a likelihood of identification through reasonable means.

The user has two options when dealing with such data: either process it directly as personal data or attempt to render it non-personal. If there are multiple parameters with a Level 2 classification or higher within the same dataset, the user should take precautions to reduce the risk of identification. These include processing the parameters separately, not assigning any time stamps, and anonymizing the data as much as possible.

It is important to note that the evolving position of the EDPB and supervisory authorities on this issue should be monitored, and more detailed guidance on anonymization and pseudonymization in connected vehicles is to be expected.

Regarding the processing of data in autonomous vehicles, there exist two fundamental options: either process the data as personal data or pursue a state of complete non-personality. If the user processes only one parameter with a classification of Level 2 or higher, or if the parameters are not contained in the same dataset, the user may proceed without performing any further operations and should abide by the obligations and recommendations related to non-personal data.

However, if there are multiple parameters with Level 2 classification and they are in the same dataset, there exists a risk that the user could be identified. In such cases, it is recommended to:

- Process these parameters separately, such that they will not be recorded at the same time or in the same databases.
- Abstain from assigning time stamps to these parameters.
- Endeavor to anonymize the data as much as possible, such as by removing unique identifiers that could allow one to establish a link with other parameters.

It should be noted that, apart from the general guidance presented in the first paragraph, all matters applicable to data classified as purely personal apply to the data in this category. The user must monitor the evolving stance of the EDPB and supervisory authorities on this subject closely. Detailed guidance on anonymization and pseudonymization in connected vehicles is expected to be published in the near future.

VII. DISCUSSION

The topic of personal and non-personal data in autonomous vehicles is a complex and evolving issue that requires further research and exploration. While this paper outlines a valuable process for identifying and categorizing data in autonomous vehicles, further work remains to be done in several areas.

Firstly, as autonomous vehicle technology continues to evolve, new types of data may emerge that were not previously considered. It will be important for researchers and policymakers to stay up-to-date on these developments and adapt regulations accordingly.

Secondly, while this paper provides a useful framework for categorizing data as personal or non-personal, there may be cases where the distinction is not clear-cut. As such, there is a need for further research into how to best regulate data that falls into a grey area between personal and non-personal.

Thirdly, this paper focuses primarily on the legal and regulatory aspects of data in autonomous vehicles. However, there are also ethical considerations that must be taken into

account. For example, even if certain data is legally classified as non-personal, individuals may still have concerns about their privacy and how their data is being used. Future research should explore how to balance legal and ethical considerations when it comes to autonomous vehicle data.

Finally, as autonomous vehicles become more common, it will be important to ensure that there are clear and consistent regulations across different jurisdictions. This will require international cooperation and coordination, as well as ongoing research and dialogue between policymakers, industry stakeholders, and members of the public.

Overall, while this paper provides a valuable starting point for understanding personal and non-personal data in autonomous vehicles, there is still much work to be done to ensure that the regulatory and ethical frameworks surrounding this issue keep pace with technological developments and meet the needs and concerns of all stakeholders involved.

VIII. CONCLUSION

The issue of personal and non-personal data in autonomous vehicles is complex, and several papers have already been published on this topic. In this paper, we have presented a procedure for determining the categories into which processed and retained data falls, explained the current legal regulation that must be observed, and proposed appropriate recommendations for each data category. The classification of data proposed herein takes into account various parameters, including sensitive (special category) parameters, data directly referring to the data subject, and data that indirectly allows for identification of the data subject. Additionally, datasets have been created to address the issue of non-personal data that, when combined with other information, can become personal data.

The proposed procedure and data categorization can serve as a guide for data controllers in autonomous mobility to ensure that data processing will comply with legal regulations. It may also be useful for other players in the autonomous mobility ecosystem, such as vehicle manufacturers and their suppliers, software application and service providers, and others.

Our paper builds upon the work of other researchers who have explored the issue of personal and non-personal data in autonomous vehicles. Their work includes studies that have investigated the use of biometric data in autonomous vehicles, as well as those that have focused on the privacy implications of vehicle data collection. Our study contributes to this body of work by presenting a comprehensive procedure for data categorization and providing recommendations for each data category.

In conclusion, the issue of personal and non-personal data in autonomous vehicles is complex, and data controllers in autonomous mobility need to ensure that data processing complies with legal regulations. The procedure and data categorization proposed in this paper can serve as a useful guide for achieving this goal.