Article III

Salami, Emmanuel (2020) Autonomous Transport Vehicles vs The Principles of Data Protection Law: Is Compatibility Really an Impossibility?

Reprinted from International Data Privacy Law Journal, Vol 10, Issue 4, (2020) 330–345 with the permission of Oxford University Press.

Autonomous transport vehicles versus the principles of data protection law: is compatibility really an impossibility?

Emmanuel Salami*

Key points

- Autonomous (transport) vehicles have evolved from science fiction into a feature of reality (in) which we now live.
- From a data protection standpoint, one of the challenges confronting the integration of autonomous vehicles into the society is the question of whether or not this disruptive technology is capable of being compliant with the principles of data protection law.
- The importance of focusing on the principles of data protection law lies in the fact that these principles encompass the entire body of data protection law. Failure to achieve compliance with said principles automatically amounts to a failure to comply with data protection law.
- With a focus on the European Union and the European Economic Area, this article seeks to identify the extent to which the extant data protection laws are capable of protecting the right to data protection of data subjects in the use of autonomous vehicles while also making recommendations on how compliance can be best achieved.

Introduction

This article addresses the compatibility of autonomous vehicles (AV) with the principles of data protection law under the legal framework of the European Union/ European Economic Area (EU/EEA). The importance of this article lies in the fact that most data protection law provisions stem from these principles. It is therefore impossible to speak of data protection law compliance without an initial compliance with these rudimentary principles.

AV embody the most advanced stage of vehicle automation whereby the system is completely and independently responsible for all driving tasks everywhere and at all times without any form of human intervention.[1]

To function properly, AV rely heavily on big data,[2] which includes both the personal and non-personal[3] data of drivers, passengers, road users, pedestrians, and other relevant persons. This effectively means that for AV to function as desired, it must necessarily interact or engage with other AV, Internet of things (IOT),[4] traffic signs, cloud services, and other connected devices. Considering the central role data plays in the mode of operations of AV, it is essential that personal data forms the basis of the discussions in this article. Where necessary, the nature of the data (whether personal or not)

* Emmanuel Salami, Faculty of Law, University of Lapland, Rovaniemi, Finland.
The author is grateful to his PhD supervisors Professor Rosa Maria Ballardini and Professor Rob van den Hoven van Genderen for their review of earlier versions of this article. The author is also grateful to the anonymous reviewers and the editor of this journal for their helpful comments and feedback.

1 Andreas Herrmann, Walter Brenner and Rupert Stadler, *Autonomous Driving: How the Driverless Revolution Will Change the World* (UK: Emerald Group Publishing2018), 3. In respect of autonomous vehicles, five levels of automation have been identified for cars, with Level 0 no automation at all; in Levels 1 and 2, the system takes over some of the driving tasks, but the driver is required to continually monitor the system and must be able to take over the driving as soon as it becomes necessary; Level 3 requires less monitoring of the system by the driver; in Level 4, the system is able to drive the car in normal operation and in defined surroundings but the driver can intervene at will; Level 5 is the final stage, which is the fully automated and autonomous driving stage of a car and this forms the focus of this work. Please see: Herrmann and others, ibid, 8–9, 47–51.

2 The foremost definition of big data is the '3Vs definition' which defines big data as high volume, high velocity and high variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making. Gartner IT glossary Big data. <http://www.gartner.comandit-glossaryandbig-data> accessed 17 November 2018.

3 Art 4(1) GDPR defines personal data, inter alia, as any data which either alone or in combination with other categories of data could lead to the identification of natural persons. Therefore, data categories that do not fall within this definition would qualify as non-personal data.

4 For further readings on IOT, see: Adam Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation' (2015) 21 Rich JL & Tech 6.

will be expressly mentioned and specified.[5] In order to properly address the impact of the principles of data protection law on AV, this article examines some of the ways through which AV collect (personal) data and the principles of data protection law as they pertain to AV. The concluding parts of this article consider the relationship between the principles of data protection law and AV, the inherent data protection law compliance challenges as well as the recommendation of appropriate remediation actions that could help resolve identified challenges.

AV in this article is used broadly and encompasses autonomous cars (AC), autonomous ships (AS), autonomous trains, and autonomous planes as they (will) all have similar modes of operation as it relates to data collection. One of the objectives of this article was to identify (potential) data protection law compliance gaps in the use of AV with an emphasis on the principles of data protection law while also recommending appropriate remediation actions. The pursuit of this objective begins in the next paragraph with an examination of how AV collect personal data.

How do autonomous vehicles collect (personal) data?

In order to evaluate the relationship between the principles of data protection law and AV, it is necessary to identify some of the ways through which AV collect (personal) data. For this purpose, AC and AS will be used as case studies. It must be noted that the avenues for (personal) data collection identified below are not exhaustive but are merely intended to point out some of the most common means of (personal) data collection in AC and AS. The data collection procedures are addressed separately because even though they both operate similarly, the data collection procedures between AC and AS differ in some detail. This difference is largely because (i) the definition of autonomy differs considerably between AC and AS (this will be addressed below)[6] and (ii) the various operatives performing defined functions in traditional ships are reflected in the data collection and processing process of AS, a feature that is not used for AC.[7] These factors underscore the distinctions in the data collection processes of AC and AS, thereby making it necessary to address said data collection processes separately.

Autonomous cars

A large volume of the (personal) data that are processed by AC are collected from passengers, including travel habits, destinations, stops, routes, body size (derivable from seat settings), number of riders (through the number of seat belts strapped on every trip), musical taste, environmental data, etc.[8] AC possess 'home and emergency buttons', which when triggered, will drive passengers home or contact an ambulance service, respectively. Data recorders may function like the flight data recorders (black boxes) in airplanes. Two types of data recorders have been identified for AC: crash data recorders and journey data recorders, which contact an ambulance service or drive passengers home, respectively.[9] The nature of these features means that AC will have access to the home address, blood group, etc. of passengers. AC will also have data recorders that will record, among other things, the algorithmic decisions of data recorders.[10] While crash data recorders collect and store (personal) data before and after a crash, journey data recorders collect, and store (personal) data while the vehicle is being driven.[11]

Sensors, through which AC can identify objects, persons, road users, traffic signs, etc, are also a very important component of AV. The most important sensors being used by AC are as follows:

Lidar: With the aid of laser lights, this sensor can scan over a distance of 100 m in all directions around AC with the data collected being used in the development of a three-dimensional map for the AC.[12]

Radar: Radar uses radio waves to determine the speed, distance, and angle of moving objects. Though less accurate than lidar in determining angles, radar can work in all conditions and can even use reflections to see objects in its rear view.[13]

Camera: This is the most popular sensor which generates massive amounts of data (millions of pixels) and can

5 While this article focuses on data protection law, it is important to note that other fields of law such as criminal law, insurance law, traffic laws, laws of the sea, etc, may also be applicable to the regulation of various types of autonomous vehicles.

6 This distinction is addressed under para 2.2 below.

7 Ibid.

8 Kai Rannenberg, 'Opportunities and Risks Associated With Collecting and Making Usable Additional Data' in Maurer and others (eds) *Autonomous Driving. Technical, Legal and Social Aspects* (Berlin, Germany 2016), 499–500. <https://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8.pdf> accessed 09 June 2019; Ulrich Kück Bohms, Vernetztes Fahren – Daten als Treibstoff in eine neue Zeit, April 2019. <https://andandwww.datenschutz-notizen.deandvernetztes-fahren-daten-als-treibstoff-in-eine-neue-zeit-3322423and> accessed 21 April 2019.

9 Herrmann and others (n 2) 94.

10 Ibid 125 and 239.

11 European Commission, Black boxes/In-vehicle data recorders. <https://andandec.europa.euandtransportandroad_safetyandspecialistandknowledgeandesaveandesafety_measures_known_safety_effectsandblack_boxes_in_vehicle_data_recorders_en> accessed 27 December 2018.

12 Herrmann and others (n 2) 95.

13 Ibid 95–96.

recognize colors, which makes it very effective for scene interpretation.

Ultrasound: This sensor measures the distance between AC and nearby objects using sound waves.

The sensors above also depict some of the methods through which AC capture the (personal) data of passengers and pedestrians alike, thereby bringing the personal data collected therein within the purview of data protection law.[14]

This discussion would be incomplete without reference to the mobile vehicular cloud (MVC).[15] The MVC is a variant of the traditional cloud computing systems,[16] which uses mobile devices in providing cloud services.[17] The necessity of the MVC lies in the fact that it helps AC to overcome the dependence on remote servers for the processing and storage of data by using services provided by potential nodes and road-side hardware equipment.[18] MVC assist AC to achieve a 'distributed and facilitated execution of tasks which are related to viably overseeing and managing various transport activities on roads.'[19] In plain terms, MVC store data collected by AC in cloud services located on the AC instead of a remote cloud location. The use of MVC helps in saving costs which would have ordinarily been incurred in uploading data on the web as well as the cost of download, which are regular costs that would ordinarily have been incurred in the use of a remote cloud service.[20] In the use of MVC, AC save the data they collect in their MVC and these data are shared and processed amongst AC on the road by each AC having access to the other's MVC. This eases the process of navigating the mobility of AC on the road.[21] The effect of the use of the MVC is that AC will become mobile data carriers of some sort.

Figure 1 justifies the assertion that AC communicate with other AC, cloud services, and IOT on the roads. 'A' represents the connection between the cloud platforms and AC, 'B' represents the connectivity between traffic signs and AC, 'C' and 'E' represent the vehicular clouds, whereas 'D' and 'F' represent mobile devices, which will all be connected to and share (personal) data with AC.

Autonomous ships

AS have been largely designed to function just like AC.[22] However, the level(s) of autonomy in AS are not as pronounced as in the case of AC. This is due to the fact that when a ship is classified as being autonomous, there may still be people onboard who are capable of taking over control of the ship under defined circumstances such as in the event of emergencies.[23] This is, however, unlike AC which are capable of complete autonomy without any possibility of human intervention.[24] AS have been classified into autonomous ships and unmanned ships.[25] Autonomous ships can perform a set of defined operations with little attention from the bridge crew,[26] though other human operators may be present.[27] On the other hand, unmanned ships are operated without any human presence on the ship's

14 This personal data includes the pictures and physical appearances of pedestrians and other information from the surroundings of an AV (which may amount to personal data). Such information could include racial or ethnic origin, membership of a religious group, etc. For instance, a picture which shows a person wearing a hijab would have effectively revealed that such person is a Muslim, thereby revealing their religious belief which effectively amounts to sensitive personal data. This kind of data will amount to observed data. The Information Commissioner's Office, Big data, artificial intelligence, machine learning and data protection, 20170904, version 2.2, 12. <https://andandico.org.ukandmediaandfor-organisationsanddocumentsand2013559andbig-data-ai-ml-and-data-protection.pdf> accessed 18 November 2018.

15 MVC is also synonymous with the concept of mobile cloud computing.

16 Cloud computing has been defined as 'a location-independent computing which helps in providing resources to client on an on-demand basis through the web service interface where customers do not own the physical infrastructure, they use resources as a service and pay only for resources that they use. This technology allows much more professional computing by centralizing bandwidth, processing, memory and storage'. For further reading, see: Rohana Amarakoon, Mobile Cloud Computing for Big Data Management in Future Smart Phone App Development (14 March 2017), 1. SSRN:<https://ssrn.com/abstract=2932652> accessed 20 May 2020.

17 Ibid.

18 Mohammad Pasha and Khaleel Ur Rahman Khan, 'Scalable and Energy Efficient Task Offloading Schemes for Vehicular Cloud Computing' (2018) 10(6) International Journal of Computer Networks & Communications (IJCNC) 35.

19 Ibid.

20 Gerla Maria, Vehicular Cloud Computing, UCLA (2012) 152–53. <http://nrlweb.cs.ucla.edu/nrlweb/publication/download/779/06257116_1_.pdf> accessed 12 December 2018; Shaw Thomas, *Emerging Technologies Law, Global Practice, Create Space* (CA: Independent Publishing 2016), 154–77.

21 VB Staff, Data storage and AI are driving the evolution of autonomous cars, 4 May 2020. <https://venturebeat.com/2020/05/04/data-storage-and-ai-are-driving-the-evolution-of-autonomous-cars/> accessed 23 May 2020.

22 Mogens Blanke, Michael Henriques and Jakob Bang. *A Pre-analysis on Autonomous Ships* (Denmark: Technical University of Denmark 2016), 1. <https://andandwww.dma.dkandDocumentsandPublikationer andAutonome%20skibe_DTU_rapport_UK.pdf> accessed 22 October 2018.

23 Full autonomy in AS has been defined as when the AS is able to make decisions without human intervention. Also, six autonomy levels (AL) have been adopted for AS. These include AL 0 where there is no autonomy at all. AL 1-5 involves different levels of autonomy with varying levels of human monitoring and intervention, while AL 6 involves full autonomy with no human intervention. Blanke (n 22) 3 and 6.

24 fn 1.

25 The Norwegian Forum for Autonomous Ships (NFAS), Definitions for Autonomous Merchant Ships, Ornulf Jan Rodseth and Håvard Nordahl (ed), 2017, 7. <http://andandnfas.autonomous-ship.organdresourcesandautonom-defs.pdf> accessed 29 October 2018.

26 The bridge of a ship is the platform upon which the ship is controlled. The personnel who operate the bridge of the ship are called the bridge crew.

27 The Norwegian Forum for Autonomous Ships (n 15) 7.

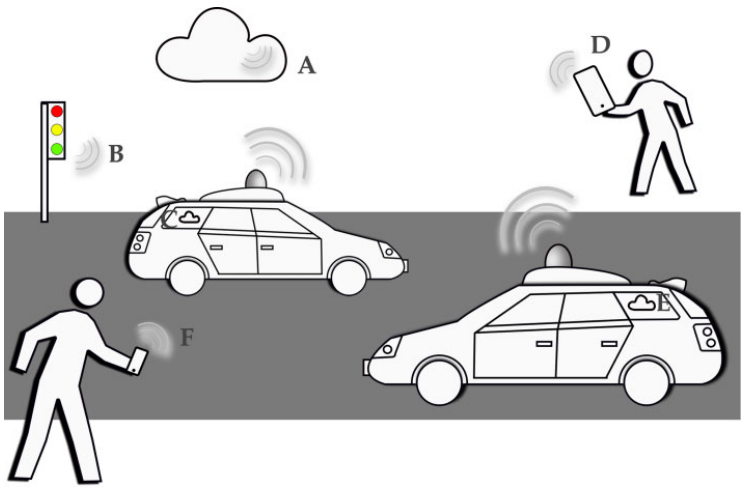

Figure 1. Graphical representation of the interconnectivity between AC and IOT/other devices on the roads[124].

bridge to perform or supervise its operations. Going by these definitions, unmanned ships are the fully autonomous ships.[28] However, the focus of this discourse on AS is to identify the avenues through which AS collect (personal) data. Some of such avenues are addressed as follows:

Due to the unique nature of shipping, it may be impracticable to leave ships unmanned (even when they are fully autonomous) particularly because of emergencies, technical faults, piracy, etc.[29] Therefore, the shore control centre (SCC) was developed to monitor and control ships from an on-shore work station. It has been contended that it may be challenging to design a fully AS without an SCC as the SCC may be needed to take over conventional shipping roles (such as the roles of captains, officers of the deck, etc.).[30] The SCC can be described as the bridge of a ship located on a remote but inter-connected on-shore site. The SCC can communicate with the ship and initiate operations on the ship through automation and autonomous technology.[31] The SCC is an enormous source of (personal) data collection and processing and therefore falls within the scope of data protection law.

The lookout function is another very important activity on the ship as it helps to protect the security of the ship, maintain its ability to prevent, and manage occurrences, such as collision, man overboard, antipiracy, and also oversee operational communications with cargo owners, ship owners, etc.[32] Conventionally, a lookout is a person detailed to observe everything within an assigned area of the sea and make reports to a designated officer.[33] Three types of lookouts have been identified as surface lookouts (who search from the ship to the horizon), low-sky lookouts (who search from the horizon to 5° above it), and high-sky lookouts (who search from the horizon to the zenith directly overhead)

28 This observation is further supported by the fact that NFAS defines a fully autonomous ship as an unmanned ship with fully autonomous control functions. See: The Norwegian Forum for Autonomous Ships (2017) 4. For the purpose of this article, what matters is not really the level of autonomy in the AV (as this varies among different types of AVs) but rather, the interaction between such AVs and data protection.

29 See: Leslie Josephs, Rolls-Royce has a low-tech solution to pirate attacks on high-tech boats, August 2017. <https://andandqz.comand1050012andno-ladders-and-curved-edges-how-ships-of-the-future-will-fend-off-piratesand> accessed 31 October 2018.

30 The Norwegian Forum for Autonomous Ships (n 15) 8.

31 Rolls-Royce has released some videos showing how a SCC is operated and used in controlling AS. These videos reveal that such SCC will have access to and control all data pertaining to the ship. See: Rolls-Royce, Ship Intelligence for Cargo Vessels, December 2014. <https://andandwww.youtube.comandwatch?v=_nApv-C7qSg&list=PLk-17K0buHIvy68TGjnSUppTq-Gi91lT-> accessed 31 October 2018.

32 The Norwegian Forum for Autonomous Ships (n 15) 16–18. The writer opines that the cargo contained in AS could give away the personal data of the owners of such cargo as its owner, supplier and purchaser (as the case may be), destination, content etc, which could lead to the identification of natural persons are contained in the system of the AS. The writer contends that any breach of such information relating to the cargo may lead to a data breach of vast proportions.

33 Rule 5 of the Navigation Rules, Commandant Instruction M16672.2 mandates Ships to always 'maintain a proper look-out by sight, hearing and other appropriate means possible in order to make a full appraisal of the situation. . .' See: Naval Education and Training Professional Development and Technology Center, Lookout Training Handbook, NAVEDTRA 12968-A, Jerry Lutes (ed), February 2000, 1. <https://andandmaritime.organddocandpdfandlookout.pdf> accessed 02 November 2018.

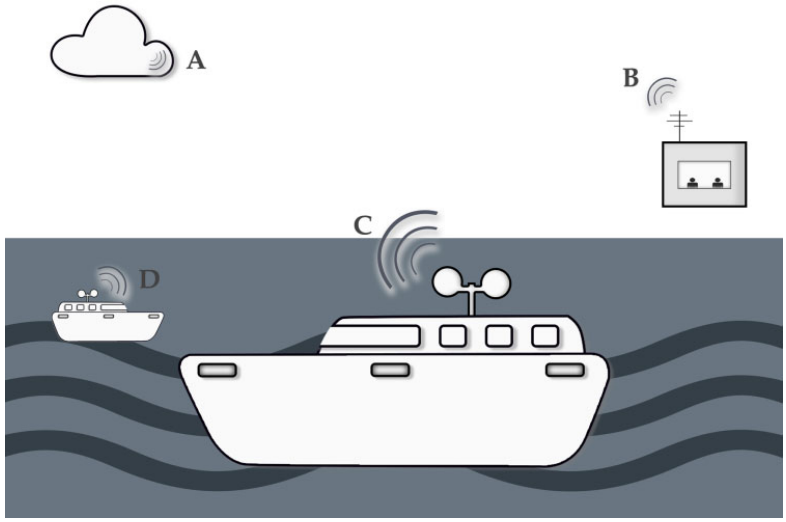

Figure 2. Graphical representation of the interconnectivity between AS, the SCC, and the cloud services.

with technologically advanced tools being used to perform these function as of today.[34] This is another avenue for data collection on an AS.

Figure 2 justifies the assertion that AS communicate with the SCC, cloud services, other AS as well as other devices and IOT subject to the closeness to the shore in some cases. 'A' represents the connection between the cloud platforms and AS, 'B' represents the connectivity between the SCCs and AS, and 'C' and 'D' represents the connectivity between various AS on the waterway.

Having considered how AC and AS collect (personal) data, it is important to mention that progress is also being made with autonomous planes[35] and autonomous trains,[36] though at a slower pace when compared with AC and AS. Similar systems for (personal) data collection will be adopted for autonomous planes and autonomous trains through the use of sensors, cameras, etc., as indicated above.

Having established some of the ways through which AV collect (personal) data, the next section of this article will identify and describe relevant principles of data protection law and also focus on the compliance of the personal data collection of AV with these principles.

An overview of applicable data protection law principles and potential challenges for autonomous vehicles

The principles of data protection are important components of data protection law as it is impossible to achieve data protection compliance without firstly complying with these principles.[37] For the purpose of this article, only those principles which are relevant to the issues under discourse will be highlighted. As (personal) data will be essential to the functioning of AV, a violation of the principles of data protection law could arise

34 Naval Education and Training Professional Development and Technology Center (ibid), 3. Traditionally, binoculars were the most used working tool of a lookout. However, with the advent of technology, more advanced tools and devices such as sensors, lidar and radar, ARPA, Automatic Identification System, VHF bridge-to-bridge radiotelephone, Automated radar plotting aids (sometimes called collision avoidance radar), Differential GPS (DGPS) satellite navigation equipment, Automatic Identification Systems (AIS) radio transponders, Vessel traffic services, Navigation and piloting instruments will be used in AS though some of these technology are already being used in some ships as of today. See: Llana and Wisneskey, Handbook of the Nautical Rules of the Road. <http://andandnavruleshandbook.comandContents.html> accessed 8 November 2018.

35 Geoff Poulton, Autonomous Skies <https://andandwww.airbus.comandinnovationandAutonomous-skies.html> accessed 9 November 2018.

36 Abhijeet Katte (22 August 2018), Cars, Planes, But No Autonomous Trains. What is the Matter with this Sector?, <https://andandwww.analyticsindiamag.comandcars-planes-but-no-autonomous-trains-what-is-the-matter-with-this-sectorand> accessed 9 November 2018.

37 Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (Oxford: OUP2018), 33.

owing to the large volume of big data that will be processed therein, making compliance with some of these principles difficult. The principles of data protection law which may be affected by the big data processing activities of AV will be examined in seriatim below. The focus will be on determining the level of compliance of AV in relation to the relevant principles of data protection law by highlighting inherent compliant gaps in AV.

Lawfulness, fairness, and transparency

This trilogy of principles each has its own legal implication and require that personal data should be processed lawfully, fairly, and transparently.[38]

The lawfulness principle requires that to be justifiable, the processing of personal data ought to be founded in law.[39] Article 6(1)(a)–(f) of the GDPR lists six lawful bases for processing personal data, which are consent[40]; performance of a contract[41]; performance of a task carried out in exercise of public authority[42]; compliance with a legal obligation[43]; legitimate interests[44] of the Controller,[45] or third parties and the protection of vital interests of the data subject.[46] These legal bases have been described as the 'threshold or minimum standard for processing data'[47] and a failure to comply with them renders personal data processing activities unlawful from inception.[48] The principle of processing personal data fairly and transparently are inextricably linked and revolve around the provision of data subjects with adequate information about how their personal data will be processed.[49] Therefore, the fairness and transparency[50] principles would have been breached where personal data are obtained in a misleading way or where it is processed in a manner which is incompatible with the reasonable expectation(s) of the data subject.[51] Furthermore, related to the principle of fairness and transparency is the data subjects' expectation of privacy concerning how their personal data will be processed.[52] For the processing of personal data to be fair and transparent, it must therefore fall within the expectation of the data subjects as typically manifested in a privacy policy. Clifford and Ausloos argue that the intention of the GDPR to provide data subjects with better control over their personal data is best achieved through the vehicle of the fairness principle.[53] In order to comply with the fairness principle, 'data controllers must also take account of the interests and reasonable expectations of data subjects; they cannot ride rough-shod over the latter'.[54]

The transparency principle on the other hand 'empowers data subjects to hold data controllers and

38 Art 5 (1) (a) of the GDPR provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. See also: art 5(4)(a) of the Modernised Convention 108.

39 Recital 40 of the GDPR.

40 The European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, Adopted on 4 May 2020. <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> accessed 07 May 2020.

41 The European Data Protection Board, Guidelines 2/2019 on the processing of personal data under art 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, Adopted 8 October 2019. <https://edpb.europa.eu/our-work-tools/our-documents/lignes-directrices/guidelines-22019-processing-personal-data-under_en> accessed 07 May 2020.

42 European Union Agency for Fundamental Rights and the Council of Europe: Handbook on European data protection law, Publications Office of the European Union, Luxembourg, 2018, 151. Also available at: <https://andandfra.europa.euandsitesanddefaultandfilesandfra_uploadsandfra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 21 April 2019.

43 Handbook on European Data Protection Law (2018), 151.

44 See (n 52).

45 Art 4 (7) of the GDPR defines a Controller as a natural or legal person, that determines the purposes and means of processing of personal data. For AV, it is expected that the manufacturer of the vehicle will most likely be the controller of the processing activity. However, it is necessary to examine the nature of each personal data processing activity to determine the appropriate controller/processor on a case-by-case basis. For instance, in marketing activities which involves the combination of various data sources, it is necessary to examine each processing activity in order to determine the appropriate controller and/or processor as the case may be.

46 European Union Agency for Fundamental Rights and Council of Europe (2018) 152.

47 Carey (n 27) 33.

48 See: Information Commissioner's Office, Lawful basis for processing. <https://andandico.org.ukandfor-organisationsandguide-to-the-general-data-protection-regulation-gdprandlawful-basis-for-processingand> accessed 25 November 2018.

49 Art 13 of the GDPR requires that data subjects should be provided with information such as the identity and contact details of the Controller; the purpose of processing; recipients of the data etc. See also Recital 39 of the GDPR and European Union Agency for Fundamental Rights and the Council of Europe (2018) 120–22. The commonest way of complying with the transparency principle is through the use of a privacy notice. Carey (n 27) 44–46.

50 Art 13 of the GDPR requires that data subjects should be provided with information such as the identity and contact details of the Controller; the purpose of processing; recipients of the data etc. See also Recital 39 of the GDPR and European Union Agency for Fundamental Rights and the Council of Europe (2018) 120–22. The commonest way of complying with the transparency principle is through the use of a privacy notice. Carey (n 27) 44–46.

51 Carey (n 27) 42.

52 The 'expectation of privacy' requirement surfaced in the European Court of Human Rights in 1997. See: Gómez-Arostegui Tomas, 'Defining "Private Life" Under art 8 of the European Convention on Human Rights by Referring to Reasonable Expectations of Privacy and Personal Choice', 9–21. <https://andandwww.duo.uio.noandbitstreamandhandleand10852and20116andHTGA_Thesis.pdf?sequence=1> accessed 25 November 2018; The Information Commissioner's Office (n 12) 22–23, para 39–41.

53 Damian Clifford and Jeff Ausloos, Data Protection and the Role of Fairness (3 August 2017). CiTiP Working Paper 29/2017, 15. SSRN: <https://ssrn.com/abstract=3013139>

54 Lee A Bygrave, *Data Privacy Law, an International Perspective* (Oxford: OUP 2014), 146.

processors accountable and to exercise control over their personal data through, for example, providing or withdrawing informed consent and actioning their data subject rights'.[55] Recital 39 of the GDPR in describing the transparency principle provides that any information and communication relating to the processing of personal data shall be easily accessible and comprehensible with clear and plain language being used to describe them. The elements of the transparency principle under the GDPR include the following: information must be concise, transparent, intelligible, and easily accessible; clear and plain language must be used, particularly when providing information to children; it must be in writing 'or by other means, including where appropriate, by electronic means' where requested by the data subject it may be provided orally; it generally must be provided free of charge.[56]

In addressing the data protection concerns that arise in relation to the lawfulness principle, not all the legal bases for processing personal data will be applicable to AC particularly because some of the personal data that will be processed may be 'observed data' (ie data that is recorded automatically using sensors, radar, etc) and may not necessarily be collected with the knowledge of the data subject.[57] Though it is arguable that either the 'performance of a contract' or the 'legitimate interest of the Controller' may serve as a justifiable legal basis for processing the personal data collected by AC, this may not always be lawful within the scope of data protection law. For instance, it would appear that in the collection of personal data from pedestrians, the 'legitimate interest of the Controller' would be the most appropriate legal basis under the GDPR.[58] In order to determine the lawfulness of 'legitimate interest' as a justifiable legal basis for processing personal data, the processing activity must pass 'the three-step test' comprising the purpose test, the necessity test, and the balancing test.[59] In the processing of personal data of pedestrians by AC, the three-step test is hypothetically applied as follows:

Purpose test: In our hypothetical scenario, the purpose of the processing activity is to support and facilitate the safe operation of AC through (personal) data collection.

Necessity test: This test requires that individual processing activities are necessary for the realisation of the overall purpose of the processing activity. One of the main considerations in the application of this test is the availability of other less-intrusive ways of achieving the purpose of this processing activity. A processing activity will therefore fail this test when there are other less intrusive ways of achieving the purpose of the processing activity. The collection of the personal data of pedestrians is an essential component of the AC technology and there are no other less-intrusive ways of using AC without such personal data collection. The collection of (personal) data from pedestrians by AC therefore passes the necessity test for these reasons.

Balancing test: This test requires the balancing of competing interests which are — the interest(s) of the Controller to carry out the purpose of the processing activity on one hand and the rights and freedoms of the data subject, on the other hand. The hypothetical purpose under consideration may fail the balancing test when the interest of AC to use the images (for instance) of pedestrians is balanced against the rights of such pedestrians to privacy and data protection. This is because the purpose sought to be achieved by the processing activity may not necessarily outweigh the rights and freedoms of data subjects to data protection and privacy.[60]

The result of the application of the three-step test is that 'legitimate interest' will (based on the scenario above) not be a justifiable legal basis for the processing of personal data in AC. The failure of 'legitimate interest' as a lawful and justifiable legal basis for the processing of personal data in AC signifies a fundamental compliance flaw from the perspective of the lawfulness principle. It is therefore safe to conclude that it may be difficult to seek out a lawful legal basis for some of the personal data that will be processed by AC particularly those that will be collected from pedestrians. This principle may also be relevant to AV in respect of the extent to which the sensors and cameras attached thereon are capable of identifying persons on-shore (the identification of persons on other ships, man overboard situations, etc, as applicable to AS) and off-shore (depending on the closeness of AS to the shore at any given time). For AC, the lawfulness principle will also determine the limit of the views of the cameras and sensors attached on the cars. For instance, will AC be justified in taking images

55 Art 29 Working Party Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, 17/EN WP260 rev.01, As last Revised and Adopted on 11 April 2018.

56 Ibid. Art 12.1, art 12.5 of the GDPR.

57 For further discussions on 'observed data' as well as the other classifications of data, please see - Information Commissioner's Office (n 14), 12–13.

58 The performance of a contract, consent, public interests etc, will be inapplicable in this respect particularly in the light of the massive volumes of non-conflicting literature in this respect. See: European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union 2018), 117.

59 Information Commissioner's Office, Legitimate Interest: At a glance. <https://andandico.org.ukandfor-organisationsandguide-to-the-general-data-protection-regulation-gdprandlawful-basis-for-processingandlegitimate-interestsand> accessed 23 November 2018; Opinion of the art 29 Working Party: Opinion 06/2014 on the notion of legitimate interests of the data Controller under art 7 of Directive 95/6/EC.

60 For a detailed discussion of the factors to be considered in applying the balancing test, see: Opinion of the art 29 Working Party (ibid) 33–42.

of houses, compounds, etc. These factors may have consequences touching on the justifiability of the legal base being used in such contexts. The challenges earlier identified with AC in respect of the use of a lawful legal basis to justify the processing of personal data especially the observed personal data collected without the knowledge of the data subjects are also applicable for AS.[61]

As stated previously, the fairness and transparency principle are inextricably linked particularly in relation to the provision of data subjects with adequate information as it concerns profiling,[62] big data analytics,[63] and other similar processing practices which may naturally flow from big data processing. A data protection concern that may be encountered from a fairness and transparency principle perspective is the difficulty of providing adequate information to pedestrians in a way that would meet the requirements of data protection law.[64] The traditional method of providing the requisite information through a privacy notice may prove very difficult in the use of AC particularly as it concerns the accessibility of such information to the data subjects.[65] This difficulty arises because a large part of the personal data that will be processed by AC are 'observed data' such as IP addresses, images, etc, which are collected without the express knowledge of the data subject.[66] Therefore, it may be impracticable to provide data subjects with adequate information about the processing activity 'at the time when personal data are obtained'.[67] This means that such information should be provided at the point of image capture, IP address collection, etc. However, this may seem impracticable as data subjects are not readily waiting for their personal data to be collected. This data collection procedure is distinguishable from a scenario where a person logs onto a website; is provided with a privacy policy containing information about the processing activity/legal basis; and obtains consent if necessary; before personal data are collected from the data subject. This makes the provision of information to data subjects a bit more difficult thereby making it necessary for Controllers to improvise in order to comply with the law. These challenges are also relevant for AS.

Purpose limitation

The purpose limitation principle requires that personal data shall be collected for a specified, explicit, and legitimate purpose and shall not be further processed in a manner that is incompatible with such purpose.[68] This principle has two elements—first, the Controller must specify the legitimate purpose necessitating personal data collection (purpose specification); secondly, personal data must not be processed in a manner, which is incompatible with the purpose for which they were obtained (compatible use).[69] The prohibition of incompatible use sets a limitation on further use. It requires that a distinction ought to be made between further use that is 'compatible', and further use that is 'incompatible' and prohibited as a result. The implication of this is that every further processing activity, distinct from the initial purpose of processing, must have a justifiable legal base of its own (or must be compatible with the original purpose of processing), otherwise, such further processing activity would be unlawful.[70] The Article 29 Working Party notes that the purpose limitation principle is closely tied to the fairness and transparency principle. This is because the concept of purpose specification and compatible use contribute to the transparency, legal certainty and predictability of processing activities. The principle also protects the data subject by setting limits on how Controllers may use their data thereby reinforcing fairness in the process.[71] A practical application of this principle can be found in the Telesverige case,[72] in which the CJEU held, among other things, that it is unlawful to process personal data when the purpose of processing had not arisen at the point of personal data collection.

61 See (n 14).

62 Profiling is defined in art 4(4) of the GDPR as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. See also: The Information Commissioner's Office (n 12), 19–20, para 31–34; arte 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, (WP 203, April 2013), 45. <https://andandec.europa.euandjusticeandarticle-29anddocumentationandopinion-recommendationandfilesand2013andwp203_en.pdf> accessed 21 April 2019.

63 Big data analytics has been defined as a way of extracting value from huge data volumes with the aim of driving new market opportunities and maximizing customer retention. See: Zakir Jasmine, Seymour Tom and Kristi Berg (2015). Big Data Analytics, p. 81. <https://andandwww.researchgate.netandpublicationand301698587_Big_Data_Analytics> accessed 17 November 2018.

64 Arts 13 and 14 of the GDPR lists certain information to be provided to data subjects. Such information includes the name of the Controller and processor(s), the name of recipients of the data, transfer to third countries, etc.

65 See (n 14).

66 Ibid.

67 Art 13 (1) of the GDPR stipulates that data subjects should be provided with information about the processing activity 'at the time' when personal data is collected.

68 Recital 50 and art 5(1)(b) of the GDPR.

69 Carey (n 27) 34.

70 Art 6(4)(a)–(b) of the GDPR; art 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, (WP 203, April 2013), 11–13 and 23–27.

71 Ibid.

72 *Tele2 Sverige AB v Post- och telestyrelsen* (C-203/15) EU:C:2016:970; [2017] QB 771, paras 90, 102, 103, 108–110.

However, this principle also raises some data protection concerns as far as AC are concerned. One of the benefits of AC is the wide range of support services (such as GPS tracking, optimal route selection, autonomous delivery of goods, etc.) that could be provided to users.[73] With the aid of data analytics, big data (from AC) may be used for different purposes which may not have arisen or been envisaged at the time of data collection,[74] a practice widely known as the repurposing of data.[75] It is expected that a large volume of the big data that will be collected by AC will be further processed for the purpose of market research in order to understand the needs of AC users, etc. Therefore, new purposes for processing personal data may arise without a lawful legal basis for such further processing activities as such further processing activities may not have been anticipated at the beginning of the processing operation. Article 6(4) of the GDPR provides that except where the legal basis for processing personal data is consent and obligations imposed by law, the Controller shall not process personal data for a purpose different from that for which it was obtained, except the latter purpose is compatible with the purpose for which the personal data was originally obtained. The conditions for determining 'compatibility' are as follows: any link between the purpose(s) of collection and further processing of personal data; the context of collection of personal data, particularly the relationship between data subjects and the Controller; the nature of the personal data, particularly whether it includes special categories of personal data or personal data related to criminal convictions and offences; the consequences of further processing for data subjects; the existence of appropriate safeguards, etc.[76] It is expected that carrying out a compatibility test for every new purpose may prove to be a herculean task because of the voluminous size of big data and also the frequency with which such new purposes may arise.[77]

For AS, they will also process large volumes of big data being exchanged between the AS and the SCC and also the big data being exchanged between AS and phones, cloud systems, and other AS. Just like AC, the big data from AS will be subject to data analytics which will result in the repurposing of data thereby raising concerns relating to the purpose limitation principle.

Data minimization

Data minimization effectively means that only data which is adequate, relevant, and limited to what is necessary for the processing activity should be processed.[78] In order to ensure compliance with this principle, two steps have been identified: ascertaining the relevant purpose of the processing activity and ensuring that only personal data that are necessary for the achievement of the relevant purpose is collected. Therefore, personal data which are excessive when compared with the need for personal data in a processing activity should not be collected/processed. This principle does not require the reduction of data collection to an absolute minimum, but rather requires an obligation to minimize data collection to a level adequate for the purpose(s) of personal data processing. In other words, this principle seeks to reduce the extent of data collection to the lowest possible level for the purposes of processing.[79] Carey notes that in practice, organizations are more likely to breach the 'relevant' and 'limited to what is necessary' aspects of this principle than the 'adequacy' aspect, since organizations tend to collect too much information on people rather than too little.[80] This view is no less correct with AV. To be compliant with this principle, two steps must be met by data controllers: first, the purpose(s) of processing personal data must be clearly outlined, and secondly, each proposed processing activity must be seen to be necessary in respect of the purpose of the processing activity.[81] Technical and organizational measures which are sufficient in ensuring the minimization of data should be instituted throughout the life cycle of a processing operation. Measures such as privacy by design and default,[82] anonymization,[83] and/or pseudonymization[84] may be

73 Shep Hyken, 'Four Ways Self Driving Cars Will Improve Customer Service', February 2017. <https://andandwww.forbes.comandsitesandshephykenand2017and02and25andfour-ways-self-driving-cars-will-improve-customer-serviceand#4ed06ccd2938> accessed 04 December 2018.

74 Forgó Nikolaus, Hänold Stefanie and Schütze Benjamin, 'The Principle of Big Purpose Limitation and Big Data. In M Corrales and others (eds), *New Technology, Big Data and the Law* (Singapore: Springer Publishers 2017), 20. See also: Bart Custers and Helena Uršič, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6 (1) International Data Privacy Law 4–15,<https://doi.org/10.1093/idpl/ipv028>

75 Data repurposing is the processing of personal data for a purpose other than that for which it was initially obtained. See: David Loshin, 'Data Governance and Quality: Data Reuse vs. Data Repurposing', 22 February 2012. <http://andanddataqualitybook.comand?p=349> accessed 25 November 2018.

76 Art 6 (4) (a)–(b) of the GDPR; art 29 Data Protection Working Party (n 51) 23–27.

77 It is expected that new purposes for personal data processing will arise in the use of AC as the very nature of big data is best maximized when it is exploited for a plethora of purposes.

78 Art 5(1)(c) of the GDPR.

79 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (New York: Springer 2017), 90–91.

80 Carey (n 27) 35.

81 Ibid 36.

82 Privacy by design requires the incorporation of data protection principles and practices into data processing from the design phase of the processing operation. Art 25 of the GDPR. Recital 78 of the GDPR.

83 Recital 26 of the GDPR.

84 Art 4(5) of the GDPR.

helpful tools in the minimization of collected by the Controller. Adherence to the storage limitation principle (to be discussed subsequently) as well as the deletion of the excess data or data that have become irrelevant also play an important role in minimizing data.[85]

The processing of big data for the navigation of AV may result in the collection of more data than is ordinarily necessary to enable an AV to understand its surroundings and to also function appropriately.[86] This is because the sensors, radars, cameras, etc. that will be used by AV to collect (personal) data are capable of collecting far more data than is necessary to enable AV function appropriately, thereby resulting in the violation of the data minimization principle. The key consideration will be the extent to which the cameras of AV are allowed to capture its surroundings particularly residential houses, faces of pedestrians, etc. Such data collection will be unlawful where an AV can function properly with less data than collected. For instance, AV need to identify that there is a pedestrian around them; however, storing the image of such a pedestrian is not necessary in the prevention of an accident. The ability of the AV to detect and identify human presence will suffice for this purpose and the storing of the image of pedestrians solely for the purpose of identifying them will therefore amount to a violation of the data minimization principle. Data recorders could lead to the recording of all personal data being generated from AC including conversations, passenger experience(s), and other occurrences, thus raising grave concerns from the perspective of the data minimization principle.

Storage limitation

This principle requires that Controllers must only retain personal data when it is necessary for the purpose for which it was obtained.[87] It also ensures that personal data are not processed in perpetuity but are deleted once the intended purpose is extinguished. The principle therefore forbids the speculative retention of data, with the implication being that data cannot be retained 'just in case' it might be processed.[88] In order to determine the time frame for storing data, Controllers must assess each processing activity on a case-by-case basis depending on the purpose for which the personal data in question has been collected. Therefore, having a blanket rule that personal data will be deleted after a certain period of time may not necessarily be compliant with the principle under consideration if the determination is not made on the basis of whether or not such personal data can be retained in the light of its necessity to the purpose of the processing operation. In the Digital Rights Ireland case,[89] the CJEU invalidated the data retention directive[90] because it provided for a retention period set between a minimum of 6 months and a maximum of 24 months without providing an objective criterion upon which the determination of such retention period should be based.[91] A further application of this principle can be found in the case of *S. v Marper*,[92] where the European Court of Human Rights held that indefinite retention of the personal data (in this case, fingerprints, cell samples, and DNA profiles) of the applicants was disproportionate and unnecessary in a democratic society, particularly because the criminal proceedings against the applicants had been terminated. In other words, the court held that it was unnecessary to retain said personal data when the legal actions against the Applicants, which initially justified the data retention, had been concluded. In order to comply with the data minimization principle, time limits should be established by Controllers for the erasure of data or for a periodic review of the necessity of data retention.[93] This provision is further substantiated by the controller's obligation to erase personal data under Article 17 of the GDPR.[94]

A potential data protection concern for AC in respect of this principle is the retention period for which personal data collected from data subjects will be stored particularly in respect of the personal data collected from pedestrians who will be unknown to data Controllers, with the former being unable to demand accountability and/or access to their personal data from the latter (particularly as it concerns the storage limitation principle).

For AS, big data processing may raise data protection concerns as it pertains to the storage limitation principle particularly in respect to the data categories and analytics flowing therefrom (which could still lead to the

85 Voigt and Buusche (n 79) 91.

86 It is important that stakeholders in collaboration with data protection supervisory authorities formulate a framework on the extent of the personal data needed to make AV function properly.

87 Recital 39 GDPR; art 5 (1) (e) of the GDPR.

88 Carey (n 27) 39.

89 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (GC), April 2014. <https://andandeur-lex.europa.euandlegal-contentandENandTXTand?uri=CELEX%3A62012CJ0293> accessed 7 December 2018.

90 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

91 Digital Rights Ireland case (n 44) paras 63 and 64.

92 *S and Marper v the United Kingdom* [GC], Nos 30562/04 and 30566/04, 4 December 2008.

93 Voigt and Buusche (79) 92.

94 Ibid.

identification of natural persons). Controllers may not necessarily be fully aware of all the categories of personal data they have collected due to its large volume.

Integrity and confidentiality

The crux of this principle entails the processing of personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.[95] This principle requires that personal data should be correctly stored and not marred by inaccurate information. Controllers and processors are tasked with ensuring that appropriate care is taken of personal data while ensuring adverse consequences in the event of non-compliance.[96] Controllers are also only permitted to engage the services of processors who can provide sufficient guarantees for the implementation of appropriate technical and organizational measures in accordance with the GDPR.[97] This effectively means that personal data should not be made available or disclosed to unauthorized persons.[98] Therefore, even within the Controller's establishment, only those employees who have a defined purpose for processing personal data should be provided with access to them. The provision of data access to every member of an establishment even when they do not have any lawful purpose for having such access will amount to a direct infraction of the confidentiality principle. It is typical to use technical and organizational measures such as pseudonymization, encryption, professional secrecy, confidentiality agreements, etc., to protect the integrity and confidentiality principle.[99]

This principle is important to AC because large volumes of (sensitive) personal data of car owners, passengers, and pedestrians are shared between AC, various IOTs, cloud services, etc. Considering the large sharing required for this data processing, personal data may be (unlawfully) accessed by persons (including hackers) who have no role or stake in its processing especially if the process is not properly managed. This may lead to the use of such personal data for nefarious activities. For instance, the home address of an AC user in the hands of the wrong person would amount to both a data breach and a security risk for such data subject.

The use of MVC in AC means that in driving such vehicles outside of the EU/EEA, personal data will be transferred outside the Union. The GDPR provides for various conditions which justify the transfer of personal data outside of the EU/EEA.[100] The implication of this is that except AC driven out of the EU/EEA meet their requirements of the GDPR for data transfers, the driving of such cars outside of the EU/EEA will amount to a violation of the rules that pertain to the transfer of personal data outside of the EU/EEA. A hypothetical example of this could occur if an AC is driven from Germany to Ukraine. Owing to the fact that Ukraine is a non-EU/EEA country, the requirements of the law as it pertains to data transfers must be met before an AC can be driven to the said destination. Therefore, Controllers must anticipate and prepare for scenarios where AC are driven out of the EU/EEA in the same manner as though they were transferring personal data to a third party outside of the EU/EEA. Failure to cater for this occurrence will result in a violation of the principles of data protection in relation to data transfer.

This integrity and confidentiality principles are also of particular significance to the use of AS because of the SCC which will operate as the 'on-shore deck' of AS. The implication of this is that the AS will be connected to the SCC and the (personal) data contained on the AS will also be accessible at the SCC. The personal data accessible from the AS could include the names and personal details of passengers of the AS, the ID numbers of the goods being transported onboard the AS, routes, destinations, etc. If not well protected, these (personal) data categories could fall into the hands of the unauthorized persons within and outside a shipping company, an occurrence which would result to the unlawful processing of personal data.

Techniques for the resolution of identified challenges

For AV to become a trusted technology, appropriate measures to ameliorate its data protection challenges must be put in place in order to mitigate the risks for all concerned identified parties. Recommendations which could aid the compliance of AV with the specific principles of data protection law earlier mentioned will be made below.

95 Art 5(1) (f) of the GDPR. An extension of the integrity and confidentiality principle can be found in art 32 of the GDPR where controllers and processors are required to implement appropriate technical and organizational measures so as to ensure a level of security appropriate to the risk with objectives which include the maintenance of the confidentiality, integrity, availability and resilience of processing systems and services.

96 Voigt and Buusche (n 79) 40.

97 S 28(1) of the GDPR.

98 ISO/IEC 27000:2016, Clause 2. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en:term:2.63> accessed 24 May 2020.

99 Handbook on European Data Protection Law (2018) 131–34.

100 Arts 44–49 of the GDPR.

Lawfulness, fairness, and transparency

Due to the possibility of 'legitimate interest' being an unlawful legal basis for processing the personal data collected by AC, it is necessary to create a less-speculative system for defining the legal basis for the processing of personal data in AV. It is posited that a probable way of achieving this may be the use of 'legal obligation' as the basis of such personal data processing in order to reduce the speculation that could arise in this regard. This could be achieved through the amendment of the extant data protection law(s) or the creation of specific laws for AV, which legally authorizes and defines the processing of personal data by AV throughout the life-span of the processing activity from personal data collection to deletion.[101] In this event, Controllers will be able to rely on 'legal obligation' as a legal basis justifying personal data processing in AV while taking away the speculation generated by the use of 'legitimate interest' and other legal bases herein.

From the perspective of the fairness and transparency principle, in order to communicate the privacy notice to the members of the general public particularly pedestrians, it is important to create massive awareness through the use of various (social) media outlets, sign posts, TV and radio jingles, social media communications, etc, in order to communicate to the general unassuming public that their personal data may be processed by AV. Due to the peculiarities of the processing operations of AV, data subjects must be made aware of the means and purpose of data collection at every available opportunity. Even though 'not on all fours' with the data processing operations of AV,[102] some support for the use of media outlets to provide information to data subjects in this scenario can be found in one of the Google street view cases which arose due to the collection of (personal) data by Google for its maps. In the case of *EDÖB v Google*,[103] the Swiss federal supreme court held (among other things) that in Google's collection of personal data for the street view, notice ought to be provided to data subjects in both the local and regional media. More specifically, the use of public signposts which will indicate that personal data will be processed by AV along particular routes may be a very effective way of communicating to data subjects that their personal data may be so processed.[104] In such an event, providing persons who do not want their personal data to be processed by AV with alternative routes is a way of providing legitimacy to the process.

Figure 3 reflects the (Article 13 GDPR) information which ought to be provided to data subjects at the point of data collection. Owing to the potential sensitivity of the personal data that will be processed by autonomous cars, it is necessary to ensure that data subjects are always informed about the contact details of the Controller's Data Protection Officer (DPO) as well as the contact details of the appropriate data protection supervisory authority. This will ensure that data subjects can easily contact the DPO and (if no remediation action is implemented) the appropriate supervisory authority. The image depicted above can be specifically adapted for AV.

Purpose limitation

With the use of data analytics in the processing of big data, new purposes to which such data could be applied are bound to arise continuously as that is the very essence of big data analytics. It is therefore important that Controllers check the compatibility of new processing activities (as they arise) with the initial purpose for which the personal data were collected. Adequate information must then be provided to data subjects. In order to cope with the volume and frequency with which new purposes for processing personal data may arise, a dedicated data management platform could be created with data subjects being requested (through provision of relevant information) to regularly look up new purposes of processing, with such data subjects having the right to opt-out, object, and exercise their data protection rights thereon. The use of such a platform shall not act as a substitute for the provision of adequate information and seeking express consent from data subjects who do not log into or provide the request information on the platform. The advantage of using such a platform is that it could be a very efficient data governance system[105] for AV and other rights of the data subject could also be exercised thereon. It is important

101 Such law will regulate all matters that relate to data protection as it concerns autonomous vehicles including the specific applicability of the principles of data protection law to AVs.

102 The purpose of the core processing activity between AV and Google maps differs to some extent. In AV, the main purpose of data collection is to enable vehicles navigate the roads properly by being able to understand and interpret the elements present in the environment. In the data collection of Google for its street view, personal data is collected, transferred to servers in a foreign country, placed on a foreign website and accessible for users of the Google maps.

103 BGE 138 II 346.

104 A potential challenge in the use of the signage above (Figure 3) is the fact that multiple AC manufacturers will be Controllers for various AC on the roads. This means that there may be multiple signages on the roads belonging to various AC manufacturers. Such a result will negate the transparency principle as information overload will be as good as not providing data subjects with any information. In such a case, it will be necessary to turn to mass media (TV and radio jingles, social media communications, etc) as an alternative means of providing the necessary information to data subjects.

105 Data governance has been defined as the exercise of authority and control over the management of data assets. A high standard of data governance

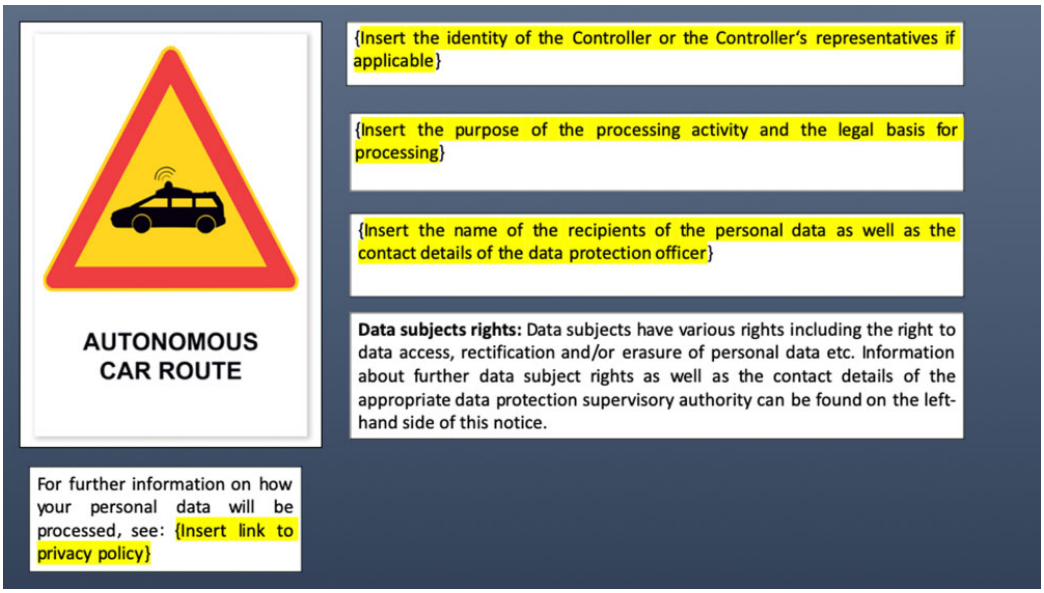

Figure 3. Suggested image for informing persons that specific routes are being used by AV.

to note that such a platform is only meant to properly manage personal data and the compliance requirements of data protection law. At no time will the use of such a platform render compliance with the requirements of Article 6(4) of the GDPR on data repurposing irrelevant. Data subjects cannot also be deemed to have consented to new processing activities by not been responsive on the platform as this will render such consent unlawful.[106] The platform is only meant to ease the process of complying with the requirements of the law for data repurposing.[107]

Data minimization

In the use of drive and data recorders, the use of 'crash data recorders' (which record only vehicle crash-related information) as against the use of 'journey data recorders' which are capable of recording all events, particularly conversations, during a trip is an effective way of ensuring that only (personal) data that are necessary for the purpose sought to be achieved by the processing activity are collected. A viable practice may be gleaned from the use of data recorders in aircrafts where compliance with the data minimization principle is achieved through the recording of only relevant information like airspeed, altitude, fuel flow, etc, and about two hours of cockpit voice recording, with all these (personal) data stored on data recorders which have a storage capacity of about 25 h of flight data.[108] The adoption of such strict and regulated storage of only necessary (personal) data will be a compliant way to ensure compliance with the principle of data minimization.

If the data minimization principle is ever to be ingrained into the use of AV, there must be a conscious effort by manufacturers to incorporate privacy by design principles into the development phase of AV. Therefore, data protection principles would have been put in place from the very inception of the process, thus ensuring that only personal data which are necessary for the functioning of AV will be collected and processed. For instance, the range of cameras, sensors and radars will have been set in a way as to capture personal data only within a distance necessary for the operation of the AV.[109]

will foster the incorporation of data ethics and helps an organization take proper actions in respect of data processing. For further readings, please see: Katherine O'Keefe and Brien O Daragh, *Ethical Data and Information Management* (London: Kogan P Limited 2018), 98–102.

106 Art 4(11) GDPR.

107 See (n 76).

108 Cristen Tilley, Eight things you might not know about black boxes, January 2015. <https://andandwww.abc.net.auandnewsand2014-03-26andblack-box-flight-recordersand5343456> accessed on 27 December 2018.

109 For further readings on PbD particularly in a big data context, See: Thomas J Shaw, *DPO Handbook: Data Protection Officers Under the GDPR* (Portsmouth, USA: IAPP, 2018), 130–35.

Furthermore, another means of complying with this principle is through the blurring of all human faces that will be captured at any time by AV. Flowing from the data minimization principle, AV (for instance) only need to know that a person is crossing the road and do not need to capture such a person's image. In order to achieve this purpose, the face of such pedestrians and road users is not necessary for the processing activity and ought not to be captured. In the event that such practice is yet to be adopted, such faces ought to be blurred out or darkened using silhouettes in order to prevent the unnecessary identification of pedestrians and road users. Regulation can also be put place to ensure that the manufacturers of cameras and sensors incorporate the data minimization principle into their products in order to ensure that more information than is necessary is not collected. For instance, the reach of the cameras to be used by AV can be limited to an agreed distance while the cameras may also be designed to capture only silhouettes by default. In determining the reach of cameras and sensors placed on AV, some lessons can be learned from the decision regarding Google Street View which was reached in the case of *EDOB v Google*.[110] In that case, the Swiss federal Supreme Court insisted among other things on the collection of only necessary data and anonymizing data categories which are unnecessary for the purpose of the processing operation. The court further held that people should be able to demand for the deletion of their property garden furniture, toys, etc., are no longer clearly recognizable.[111] In applying the finding of the court to the case of AV, it is generally expected that AV will not require access to private spaces except in those cases where houses are so close to the road that it is almost impossible to capture the surrounding of the cars. In such an event, beyond blurring human faces, it is necessary to blur private properties to make them unrecognizable in line with the recommendation of the court.

Storage limitation

The CJEU in the Digital Rights Ireland case noted, among other things, that Controllers must ensure that retention periods are decided per processing activity with the important consideration being the necessity of retaining such data for each processing activity.[112] Therefore, having a blanket retention period without categorically stating the justification and necessity of the data retention to the Controller's processing activities may be effective in achieving compliance with the relevant principle. The large volume of big data involved in the use of AV means that Controllers must adopt a high data governance standard in order to keep track of the personal data in their custody and the necessity of retaining such personal data in order to determine the appropriate time to delete the relevant personal data in accordance with the requirements of this principle. Such data governance system must include an accurate and well-updated data mapping system. Failure to adopt such high data governance standards means that Controllers may find it harder to keep track of personal data leading to the avoidable consequence of violations of the data retention principle.

Integrity and confidentiality

Due to the large volume of personal data that will be collected and processed by AC, there is a need to have a consensus standard of applicable technical and organizational measures for AV in order to guarantee a minimum standard of protection for data subjects whose personal data will be processed by AV. The use of MVC in AC must also be regulated to prevent unlawful data transfers should AC be driven outside the EU/EEA. The GDPR lists conditions which must be met before personal data can be transferred outside the EU/EEA.[113] Likewise, AC must comply with these rules for data transfers before they can be driven outside the EU/EEA. It would appear that from the conditions which ought to be met to transfer personal data under the GDPR,[114] the adequacy decision granted to a non-EU/EEA member state will be the most justifiable legal basis for carrying out such data transfer.[115] The rationale for this view is that AC that will be driven outside the EU/EEA will not be targeted to any specific controller/processor at any given time when the car will be in the third country. It is therefore difficult to protect such personal data through the standard contractual clauses, binding corporate rules, and other similar conditions for data transfer as it becomes more difficult to assign the responsibility for the data (particularly data security) on any Controller. It is therefore necessary that third countries where AC may be driven to guarantee some wholistic level of data protection capable of justifying

110 See (n 104).

111 BGE 138 II 346, 355, 373.

112 See (n 90).

113 Arts 44–49 of the GDPR lists adequacy decision, appropriate safeguards, binding corporate rules, standard contractual clauses of the European Commission are some of the conditions for transferring personal data outside of the EU.

114 Ibid.

115 European Commission, Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_lt> accessed 20 May 2020.

such data transfer and this is best proved through the existence of an adequacy decision of the European Commission. Once an adequacy decision is in place, such AC can be lawfully driven to such countries as though they are being driven with the EU/EEA.[116] Another alternative in an attempt at achieving compliance would be to restrict the driving of AC to only data protection compliant countries, which are basically countries in the EU/EEA and/or countries with an adequacy decision. For this purpose, it may suffice to set up a committee which will include stakeholders in the AV industry as well as other industry experts. Such committee will be responsible for aligning the provisions of the GDPR with the realities of AC so as to justify data transfers through AC on a case-by-case basis. In all cases of data transfers involving AC, the restriction of access to relevant data on a strictly need-to-know basis should always be the priority.[117]

Asides from data protection principle-specific recommendations made above, the enthronement of data ethics in the use of AV may result in the protection of the right to data protection of data subjects. Data ethics has been defined as the branch of ethics that studies and evaluates moral problems related to data processing and corresponding practices in order to formulate and support morally good solutions.[118] The fact that a processing activity is lawful does not make it ethical, as other factors such as human dignity, freedom and the sustaining of democratic principles as well as their legal, engineering, philosophical, and moral implications have to be considered. Data ethics is very important for AV because of the inter-relation between ethical concerns arising therefrom and the right to the dignity of the human person which invariably affects the right to data protection. The right to dignity of the human person requires that persons are able to 'develop their own personalities, to lead independent lives, to innovate and to exercise other rights and freedoms'.[119] From a data protection perspective, the respect for the dignity of data subjects will ensure that data Controllers view data subjects as human beings worthy of respect and not merely objectifying them as data generating entities. To be effective, data ethics ought to be incorporated into AV at their design phase in accordance with the principle of privacy by design.[120] It is expected that a lot of novel processing activities (comprising the anticipated and the non-anticipated) will arise from the use of AV. As identified in earlier parts of this article, some of the data protection concerns that may arise from the use of AVs may not have any direct remedies under the extant data protection laws.[121] This possibility necessitates the deployment of a more flexible moral code in the form of data ethics so as to ensure that no matter the interpretation that is adduced to the law, controllers will always act in the data subjects' best interest. This can best be achieved when Controllers themselves deem their relationship with data subjects as a fiduciary relationship[122] of some sort, which necessitates that they make the best efforts to protect the rights of the data subjects irrespective of any possible lapses in the law. Furthermore, controllers will also benefit from data ethics as research has revealed that more consumers favour transacting with Controllers that prioritize the right to privacy and data protection of its consumers.[123] If properly executed, the adoption of data ethics may birth lawful data processing practices which may influence future legislations through the introduction of lawful industry-tailored practices.

It is proposed that a committee of experts and stakeholders to oversee data protection law and ethical concerns in the use of AV be constituted in the EU/EEA. This AV-specific committee of experts and stakeholders should be involved in drafting future (AV-themed) data protection legislations and resulting amendments. This will further ensure that sufficient industry-specific practices and ethical considerations are infused into the

116 Art 45 of the GDPR.

117 For some design and architectural measures to ensure the protection of personal in the context under discourse, See: Kai Rannenberg, 'Opportunities and Risks Associated With Collecting and Making Usable Additional Data' in Markus Maurer and others (eds) *Autonomous Driving. Technical, Legal and Social Aspects* (2016), 511. <https://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8.pdf> accessed 09 June 2019.

118 Luciano Floridi and Taddeo Mariarosaria, *What is Data Ethics?* (Oxford Internet Institute, University of Oxford 2016), 5; O'Keefe and O Daragh (n 105) 39–49.

119 Buttarelli Giovani (European Data Protection Supervisor) (2015), 4, para 1.

120 For further readings on ethical concerns in the use of AV, See: C Gerdes and S Thornton, 'Implementable Ethics for Autonomous Vehicles', in Markus Maurer and others (eds) *Autonomous Driving. Technical, Legal and Social Aspects* (2016), 511. <https://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8.pdf> accessed 09 June 2019.

121 Para 3 above.

122 '"Fiduciary duty"' connotes an obligation to refrain from self-interested behaviour that constitutes a wrong to the beneficiary as a result of the fiduciary exercising discretion with respect to the beneficiary's critical resources'. For further reading, see: D Gordon Smith, 'The Critical Resource Theory of Fiduciary Duty', 55 Vanderbilt Law Review 1399. SSRN:<https://ssrn.com/abstract=339100>.

123 Thomas Redman and Robert Waitman, *Do You Care About Privacy as Much as Your Customers Do?* (Harvard Business review), 28 January 2020. <https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do> accessed 24 May 2020.

124 The use of figures in this article is in accordance with the principle of legal design which is aimed at making legal principles more easily comprehensible particularly to members of the general public who have no legal background. Legal design has been defined as the application of human-centered design to the world of law, to make legal systems and services more human-centred, usable, and satisfying. See Hagan M Law by Design. <http://andandwww.lawbydesign.coandenandhomeand> accessed 20 May 2019.

applicable laws while also taking actions on complaints of ethical and related violations in relation to AV.

Conclusion

This article concludes that though requiring some diligent effort, AV are capable of attaining compliance with the principles of data protection law. Recommendations are also made regarding how compliance with these principles can be possibly attained. However, there is a need for regulators and stakeholders to have a forum where basic rules and standards can be formulated in this regard. This would ensure that the principles are in sync with the framework of data protection law and compliance with them would be very helpful in achieving a high level of data protection compliance as far as AV are concerned. It is not expected that data protection law would re-invent itself for AV. However, necessary modifications and conscious regulation must be put in place if AV are to ever become a daily part of our legitimate human existence. The institution of proper data protection measures will ensure that when legal actions challenging the legality of AV start pouring in, Controllers will be fully ready to defend the legality of their processing activities thereby aiding the acceptability of AV as a regular piece of necessary technology.

doi:10.1093/idpl/ipaa017
Advance Access Publication 28 November 2020