AVENUE

Autonomous Vehicles to Evolve to a New Urban Experience

DELIVERABLE

D9.1 Recommendations for public authorities

Co-funded by the Horizon 2020 programme of the European Union

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769033.

Disclaimer

This document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

This document is aiming to be comprehensive, however not exhaustive, as many various chapters related to different areas are covered. Furthermore, in this dynamic world and complex domains, new or updated recommendations may arise or become more relevant. The most up-to-date deliverables and recommendations can be found on AVENUE's project website https://h2020-avenue.eu/. This deliverable has been updated until 5 August 2022.

Document Information

Grant Agreement Number	**769033**
Full Title	Autonomous Vehicles to Evolve to a New Urban Experience
Acronym	AVENUE
Deliverable	D9.1 Recommendations for public authorities
Due Date	31.07.2022
Work Package	WP9
Lead Partner	Etat de Genève – Office cantonal des transports (DI)
Leading Author	Lionel Binz
Dissemination Level	Public

Document History

Version	**Date**	**Author**	**Description of change**
0.1	23.12.2021	Lionel Binz	First draft.
0.2	04.01.2022	Lionel Binz	Integration of Philippe Chrétien's (CEESAR) comments regarding passive safety.
0.3	05.01.2022	Lionel Binz	Integration of comments provided by Benno Nager (FEDRO) regarding current technical capacities of automated minibuses.
0.4	13.01.2022	Lionel Binz	Draft chapter dedicated to accessibility circulated to Siemens AG.
0.5	12.05.2022	Lionel Binz	Integration of the GDPR article circulated by Meriem Benyahya (UNIGE).
1.0	02.06.2022	Lionel Binz	Second draft.

1.1	22.08.2022	Lionel Binz	Updated second draft with Appendix A. Integration of comments provided by following partners: • Philippe Chrétien (CEESAR); • Arthur van der Wees; • Constance Salomon (TPG); • Klaus-Peter Wegge (Siemens AG).
1.2	07.09.2022	Lionel Binz	Updated draft, creation of key recommendations table. Integration of modifications suggested by Daniel Kaeding (Sales Lentz), Klaus-Peter Wegge et al. (Siemens AG) and Dimitri Konstantas (UNIGE).

Table of Contents

Acronyms

ACEA	European Automobile Manufacturer Association
ADS	Automated Driving Systems
ADSE	Automated Driving System Entity[1]
AI	Artificial Intelligence
AM	Automated Minibus
AMSVR	Approval and Market Surveillance of Vehicles Regulation (EU Regulation 2018/858 of 30 May 2018)
API	Application Programming/Protocol Interface
ARTS	Automated Road Transport Systems[2]
AV	Automated Vehicle
CAD	Knowledge Base on Connected and Automated Driving
CAV	Connected and Automated Vehicles
CNIL	Commission Nationale de l'Informatique et des Libertés (France)
CRPD	Convention on the Rights of Persons with Disabilities
CSMS	Cyber Security[3] Management System
DDT	Dynamic Driving Task
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECOSOC	United Nations Economic and Social Council
EDPB	European Data Protection Board
EDR	Event Data Recorder
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCAD	European Conference on Connected and Automated Driving
ExVe	Extended Vehicle
FEDRO	Swiss Federal Roads Office
GC	Geneva Convention
GDPR	General Data Protection Regulation
GPSD	General Product Safety Directive (Directive 2001/95/EC of 3 December 2001)
GSR	revised General Safety Regulation
HF-IRADS	Human Factors in International Regulations for Automated Driving Systems Workgroup
HMI	Human Machine Interface
IGEAD	Informal Group of Experts on Automated Driving
ICT	Information and Communication Technology
IT	Information Technology
ITC	Inland Transport Committee
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
LIDAR	Light Detection And Ranging
MaaS	Mobility as a service
MID	Motor vehicles Insurance Directive (Directive 2009/103/EC of 16 September 2009)
MMTIS	Delegated Regulation 2017/1926 on Multimodal Travel Information Services

[1] Notion introduced by the Law Commission of England and Wales and the Scottish Law Commission in Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020.

[2] "*Système de transport routier automatisé*", see French Decree n° 2021-873 dated 29 June 2021.

[3] Cyber Security will also be spelled "Cybersecurity" in this deliverable.

MRM	Minimal Risk Manoeuvre
NAP	National Access Point
ODB	On-Board Diagnostics
ODD	Operational Domain Design
OEDR	Object And Event Detection And Response
PLD	Product Liability Directive (Council Directive 85/374/EEC of 25 July 1985)
PRM	Persons with Reduced Mobility
PSO	Transport operators under public service obligations
PTA	Public Transportation Authority
PTO	Public Transportation Operator
PTS	Public Transportation Services
RED	Radio Equipement Directive
RMI	(Vehicle) Repair and Maintenance Information
S-OTP	Secure On-Board Telematics Platform
SAE Level	Society of Automotive Engineers Level (Vehicle Autonomy Level)
SCA	Strong Customer Authentication
SLA	Sales Lentz Autocars
SoA	State of the Art
SOTIF	Safety Of The Intended Functionality
SR	Standardisation Request
SUMP	Sustainable Urban Management Plan
SUMS	Software Update Management Systems
TEN-T	Regulation 1315/2013 as regards Union Guidelines for the development of the trans-European Transport Network
TFEU	Treaty on the Functioning of the European Union
TPG	Transport Publics Genevois
UITP	Union Internationale des Transports Publics (International Transport Union)
UNECE	United Nations Economic Commission for Europe
V2I	Vehicle-to-Infrastructure communication
V2V	Vehicle-to-Vehicle communication
V2X	Vehicle-to-Everything communication
VC	Vienna Convention
VIN	Vehicle Identification Number
VPA	1958 Vehicle Part Agreement
VRU	Vulnerable Road User

Preamble

1. **WHY?**

Why this document?

This deliverable presents a list of recommendations for public authorities regarding automated vehicles and automated minibuses operating on-demand mobility services ("**AVs**"). They arose from AVENUE partners' work and experience as well as from researches from published legal literature and open source documentation dedicated to automated vehicles and minibuses.

2. **FOR WHOM?**

For whom is this document?

This deliverable might be of interest for the public sector, specifically persons and authorities interested in the deployment of automated on-demand mobility services wanting to have details on necessary steps in order to deploy automated on-demand mobility services like those that took place in Geneva, Lyon, Copenhagen and Luxembourg at a large scale in the future.

3. **WHAT?**

What can be read in this document?

The purpose of this deliverable was to identify the most important legislative and regulatory issues concerning the deployment of AVs. This deliverable therefore contains a wide variety of recommendations presenting issues and potential solutions and measures. They aim to enable the use of AVs in an orderly manner right from the start and create favourable framework conditions for the effective and desirable use of automated mobility technologies. Appendix A provides an overview of some of the legal frameworks that are relevant to AVs.

4. **WHAT NOT, YET?**

Is this document exhaustive?

This document is aiming to be as comprehensive as possible, however it cannot be exhaustive, as many different sectors were covered. Furthermore, in this dynamic world and complex domains, new or updated recommendations may arise or become more relevant. The most up-to-date deliverables and recommendations can be found on AVENUE's project website https://h2020-avenue.eu/.

5. **WHAT NEXT?**

Please use these recommendations at your own discretion. Feel free to share your thoughts, use cases, good practices, feedback or contributions to the coordinator of the project Dimitri Konstantas at dimitri.konstantas@unige.ch. Thank you in advance.

AVENUE D9.1 key recommendations

This deliverable's key recommendations for public authorities can be summarised in the table below.

Number	Title	Recommendation	Chapters	Pages
D9.1_1	Public transportation first	Push public transportation in the field of automated vehicles during the upcoming legislative processes	1.1.	25.
D9.1_2	Harmonisation and standardisation	Harmonise the legal branches concerned by automated vehicles and encourage standardisation as much as possible	1.2.1; 1.2.4; 1.2.5; 2.3.	28; 34; 35; 57.
D9.1_3	Prepare authorities	Type-approval and other authorities should coordinate themselves and collaborate with stakeholders in order to facilitate and anticipate the deployment of automated vehicles	1.2.2; 1.2.3; 2.2.	31; 32; 52.
D9.1_4	Specific type-approval	Create an ordinary type-approval framework for automated minibuses enabling commercial deployment for PTO's and remote supervision of automated minibuses	2.1.1; 2.1.2; 2.1.3; 2.1.6; 2.2.	37; 38; 39; 45; 52.
D9.1_5	Define passive safety requirements	Passive safety requirements for automated minibuses should be defined urgently and carefully	2.1.4.	41.
D9.1_6	Improve accessibility	Use the current momentum for improving accessibility standards and legislation, encourage development and researches in this field	3.1; 3.2; 3.3; 2.1.5.	59; 61; 62; 44.
D9.1_7	Ensure compliance with personal privacy provisions	Address the major personal privacy and cybersecurity threats posed by the deployment of automated vehicles	5; 2.2.3.	67; 55.

		through legislation and provide guidance on how to comply with the current privacy framework		
D9.1_8	Antitrust	Regulate access to automated vehicle's data and define open datasets and application protocol interfaces in order to avoid potential market distortions and anti-competitive behaviors	6.1; 6.2; 6.3.	82; 84; 85.
D9.1_9	Effective civil liability	Protect future victims by fair and quick compensation mechanisms; adapt and reform the existing liability mechanisms to the complexity of establishing liability in the context of accidents implying automated vehicles	7.1.	89.
D9.1_10	Define and create proper infrastructure	Automated vehicles will rely on updated road and communication infrastructures that should be discussed and defined today	8.1 to 8.5.	99 et seq.
D9.1_11	Driving permits	Amend the existing training of new drivers to the upcoming changes and new functionalities and requirements of automated vehicles	10.	106.
D9.1_12	Criminal liability	New undesirable behaviors will arise that need to be addressed through adequate criminal offences and potentially new liability schemes	11.1; 11.2.	108; 110.

Executive Summary

1 Overarching recommendations

Recommendation title and overview	*Concerned authorities*
1.1 Prioritising public transportation The current lawmaking momentum lies mostly with the regulation of privately owned automated vehicles and/or robotaxis. These vehicles and their use cases are promoted by private stakeholders with important resources wishing to enter in a new very promising market. These stakeholders are either tech companies or manufacturers of conventional vehicles. They can also be both type of actors, working together in the form of joint ventures and consortiums. Shared automated minibuses, which are more desirable automated driving use cases from a societal point of view, did not stand in the focus of lawmaking until recently. Priority should be given to their regulation, as researches within AVENUE (and other projects as well) have demonstrated that automated minibuses will provide greater and better societal benefits than privately owned automated vehicles or driverless robotaxis.	All, in particular authorities with (AV-related) lawmaking powers.
1.2.1 Harmonisation of rules and integration of cross-border dimensions Automated vehicles ("**AVs**") and the mobility services they provide encompass different branches of the law. Some branches requiring regulation and/or amendments in order to deploy automated vehicles rely on national legislation, while others are harmonised and regulated at international and/or regional (European) levels, with small to no room of regulation at national level. An aligned and holistic European approach to automated vehicles would be desirable for road safety as well from a single market perspective and for the promotion of European industrial leadership. Due to their moving nature, the regulation of automated vehicles should also take into account cross-border considerations.	All, in particular authorities with (AV-related) lawmaking powers.

1.2.2 Coordination between authorities At national level, automated vehicles stand in the focus of different legal regimes (for instance type-approval, data protection and cybersecurity, market surveillance etc.) and will therefore require the supervision of different authorities that will need to coordinate themselves. New competences and skills related to digitalization and automation will also be necessary within these authorities. At international level, mutual assistance and questions related to data sovereignty should be discussed, amongst others, as the current international flows of data might require to collect data related to a vehicle that is physically stored in another country, sometimes outside the European Union.	All authorities that will be concerned with AV-related matters in the future.
1.2.3 Cooperation between all stakeholders In order to cope with the fast evolving technologies and business models involving automated vehicles and minibuses, various governance models can be implemented, such as collaborative regulation, where all stakeholders get involved in the definition of the regulation/policy through an inclusive approach and with the sharing of knowledge and resources, or regulatory sandboxes through experimentation clauses. Such approaches are needed as private stakeholders (vehicle manufacturers, tech companies, software developers etc.), public transportation operators ("**PTO's**"), public transportation authorities ("**PTA's**") and further stakeholders (organisations in charge of accident analysis, insurers etc.) can identify their needs and legislative issues related to the deployment of automated vehicles through the experience already gathered while experimenting.	All authorities with AV-relevant competences.
1.2.4 Standardisation The industry often relies on proprietary standards and formats (for instance each vehicle manufacturer has its own format of a high definition map, which is generally not compatible with other manufacturers' maps). This creates high curation costs when data is transferred from one company to another and high costs to develop new services. Standardisation and interoperability should be encouraged as much as possible.	Authorities with lawmaking powers that can encourage (AV-related) standardisation.
1.2.5 Uniform terminology The vocabulary used to describe automated driving technologies should not mislead the public and create false expectations. A certain level of harmonisation that would increase the public's awareness and comprehension of these new technologies is desirable.	All, in particular authorities with (AV-related) lawmaking powers.

2 Type-approval framework of automated minibuses

2.1 Type approval and initial approval

Recommendation title and overview	*Concerned authorities*
2.1.1) Creation of a specific type-approval framework dedicated to automated minibuses In addition to experimentation clauses and regulatory sandboxes, the creation of a specific type-approval framework allowing automated minibuses to operate under an ordinary approval regime, without quantitative restrictions and enabling commercial operations, is of paramount importance for the development of automated minibuses (and AVs). This will create legal certainty for the various stakeholders and allow to scale up the deployment of automated minibuses in the long run. Experience (and enacted legislation in certain Member States) tends towards a type-approval in phases, with (i) the type-approval of the automated minibuses followed by (ii) the approval of the routes or areas where the automated minibuses will be deployed as well as (iii) the single vehicle registration in a third phase.	All, in particular authorities with (AV-related) lawmaking powers.
2.1.2) Adapted requirements for safety operators As of today, for automated minibuses operating under experimentation clauses (equivalent to SAE Level 3), the requirements and qualifications imposed to safety operators are often stringent, they do not provide demonstrated safety benefits and are not necessarily relevant to the reality of their task. The key requirement for safety operators is to receive an appropriate and comprehensive training for the specificities of the AV's on-site operation, to be provided (amongst others) by the vehicle manufacturer and the PTO.	Type-approval authorities and authorities with (AV-related) lawmaking powers.
2.1.3) Remote supervision of automated minibuses Enabling remote supervision of automated minibuses (e.g. without a safety operator located inside the vehicle) and creating a dedicated legal framework is a crucial step for PTO's to deploy automated minibuses commercially at large scale and to provide economically viable transportation solutions in the future. Some European Member States and the European Implementing and Delegated Regulations issued in July and August 2022 are paving the way, by permitting	Type-approval authorities and authorities with (AV-related) lawmaking powers.

Recommendation title and overview	*Concerned authorities*
experimentations and/or by enacting legal frameworks allowing remote supervision at distance under an ordinary approval regime.	
<u>2.1.4) Define passive safety requirements for automated minibuses</u> The particular (and new) architecture and features of automated minibuses require urgently the definition of passive safety requirements. Reflexions and studies are necessary in order to arbitrate on important trade-offs in this field.	Authorities with (AV-related) lawmaking powers in the field of active and passive safety.
<u>2.1.5) Accessibility impact assessment</u> In the long run, automated vehicles will increase the overall safety of their users, but the overall safety benefits should not be at the expense of increasing risks for vulnerable groups such as persons with disabilities and persons with reduced mobility. In order to ensure an equal impact of AV's on all users, applicants for approval of automated vehicles should be required to submit an accessibility impact assessment.	Type-approval authorities and authorities with (AV-related) lawmaking powers in the field of accessibility.
<u>2.1.6) Benevolent and proactive approach to the experimentation of automated minibuses</u> Regarding the current and upcoming deployment of automated vehicles and minibuses based on experimentation clauses and regulatory sandboxes: • the competent authorities (especially type-approval authorities) should be encouraging experimentations and follow a liberal approach when granting approvals. They should prioritise and process pending applications as fast as possible, create cooperation mechanisms with applicants (such as roundtables) and refrain from hiding between potential compliance issues with the existing type-approval framework; • administrative costs generated by the approval of experimentations should remain bearable for applicants and the financial burden should not impeach the deployment of experimentations by creating a cost barrier; • for the sake of legal certainty and transparency, public guidelines and checklists for experimentations should be created and published by competent type-approval authorities; • in order to improve coordination, a dedicated European legal knowledge platform and database should be created, in order to facilitate the framework conditions for applicants and other stakeholders.	Type-approval authorities and authorities with (AV-related) lawmaking powers.

2.2 Deployment of automated minibuses

Recommendation title and overview	*Concerned authorities*
2.2.1) Monitoring Unlike conventional vehicles, automated vehicles and minibuses might require continuous regulatory oversight throughout their lifetime in the future. Therefore, the relevance of creating an "in-use" safety authority, supervising and securing the continuing safety and legal compliance of automated vehicles while they are in use (and after their type-approval and registration), should be studied, as well as methods to audit algorithms before and after approval.	Type-approval authorities and authorities with (AV-related) lawmaking powers.
2.2.2) Software updates Automated vehicles and minibuses will receive software updates in between periodic inspections and these updates will also need to be monitored, due to their safety relevance. In addition to the existing UN Regulations, harmonised rules and technical requirements should be defined, so that software updates proposed by vehicle manufacturers can be authorised by Member States in accordance with a common European methodology.	Type-approval, data protection, cybersecurity, telecommunication authorities.
2.2.3) Mitigation of cybersecurity risks The digitalisation and connectivity implied by vehicle automation will drastically increase cybersecurity risks and the necessity of mitigating them. Type-approval authorities should be granted with new competences in this field, amongst others as regards cybersecurity audits, as well as with the possibility to withdraw a permit to bring vehicles onto the market in case of important cybersecurity issues. A duty for vehicle manufacturers to notify cybersecurity breaches to public authorities should also be created.	Type-approval, market surveillance, data protection, cybersecurity, telecommunication authorities.

2.3 Amendment of existing road traffic regulations

Recommendation title and overview	*Concerned authorities*
2.3.1) Amendment of road traffic rules The presence of a human driver performing the dynamic driving from inside the vehicle was a central assumption since the creation of motor vehicles, but it will be upset by automated vehicles in the next decade(s). Thus, public authorities shall proceed as soon as possible to an extensive audit of their road traffic rules and be prepared to amend (i) legal provisions implicitly or explicitly involving the presence of a human driver, as well (ii) as provisions that might pose interpretation problems with the introduction of AV's or (iii) rules involving human negotiation, interpretation or comprehension in specific situations.	Type-approval authorities and authorities with (AV-related) lawmaking powers as regards road traffic rules.
2.3.2) Definition of behavioural rules in case of trade-offs In road traffic, situations implying a trade-off between obstructing the traffic flow and infringing road traffic rules might occur. Unlike human drivers, automated vehicles are programmed in order to comply strictly with the road traffic rules and are hardly able to arbitrate such trade-offs. Therefore, solutions to potential problematic situations should be discussed with the various authorities (such as road safety, police, traffic law, politicians etc.), the developers of automated vehicles, researchers and stakeholders of the civil society.	Type-approval authorities and authorities with (AV-related) lawmaking powers, law enforcement authorities, legislative bodies.

3 Accessibility

Recommendation title and overview	*Concerned authorities*
3.1) Improving accessibility standards for automated public transport As of today, the vehicle construction of automated minibuses as well as the mobile applications related to services provided by automated minibuses do not or hardly comply with many accessibility requirements. Various solutions should be considered. Deployers of automated minibuses and PTO's should include accessibility as an important criterion in procurement processes. On their side, vehicle manufacturers shall apply accessibility requirements in the earliest phase of vehicle construction. The current standards and those under revision should integrate automated vehicles.	Type-approval authorities and authorities with (AV-related) lawmaking powers, in particular in field of accessibility and standardisation namely standardisation request of the European Commission to the European standardisation organisations: CEN, CENELEC, ETSI.
3.2) Legislation on accessibility There is a need for standardised and enforceable European legislation across the mobility chain, as no such dedicated legislation exists for multimodal transport, be it for long-distance or local transport. The existing sectorial legislation on air, maritime, railway and road transport does not fulfil this goal and various measures should be taken in this field.	Type-approval authorities and authorities with (AV-related) lawmaking powers, in particular in field of accessibility e.g. European Commission, European Parliament and the Council of Europe.
3.3) Development and research The emerging trend of automation will affect transport system accessibility either positively or negatively and this has not yet been properly researched. Amongst others, accessibility of future automated public transport needs to be thoroughly researched and design guidelines issued. Ongoing and upcoming experimentations should aim to improve the understanding of accessibility issues. Persons with reduced mobility need to become C-ITS nodes in order for AVs to recognise and protect them.	Type-approval authorities and authorities with (AV-related) lawmaking powers, in particular in field of accessibility, researchers and NGO representing persons with disabilities or older persons.

4 Public transportation

Recommendation title and overview	*Concerned authorities*
<u>4.1) Create a flexible and innovative public transport framework for automated minibuses</u> The existing legal framework for public transportation with fixed bus stops, fixed lines and fixed schedules needs to be amended and reformed in order to allow the introduction of new mobility services offered by automated minibuses, such as Transport-on-Demand ("**ToD**") and door-to-door services, as well as the creation of Mobility-as-a-Service ("**MaaS**") providers.	PTA's and authorities with public transportation lawmaking powers.
<u>4.2) Encourage shared mobility</u> Automated minibuses operating on-demand mobility services will provide shared mobility solutions. It is therefore necessary to ensure that the public is ready for the idea of sharing this mode of transport with other persons. Thus, all forms of shared mobility need to be actively promoted and incentivized today, in order to guarantee the acceptance of these new mobility solutions in the future.	PTA's and authorities with public transportation lawmaking powers.

5 Personal privacy

Recommendation title and overview	*Concerned authorities*
5.1) Promote data, algorithmic, AI literacy and public participation Explanations of privacy related terms and agreements are often complicated and may pose cognitive and technical challenges to users/passengers of automated vehicles and minibuses. The public needs to be informed and equipped with the capacity to claim and exercise their privacy rights and freedoms as well as to understand the stakes related to sharing their personal data with third parties.	Type-approval, PTA's, data protection authorities.
5.2) Mitigate the "privacy paradox" through granular decision making mechanisms Consumers express growing concerns about their privacy when using digital services, but they do not act consistently when using these digital services (the "privacy paradox"). Mechanisms to allow users and passengers of automated vehicles and minibuses to make informed and granular decisions about their privacy and control their privacy preferences should be studied and implemented as means helping to mitigate this inconsistency.	Type-approval, PTA's, data protection authorities.
5.3) Investigate measures to foster protection of individuals at group level and provide strategies as regards conflicts over data claims The communication channels used by automated vehicles and minibuses include the potential for a multitude of separate actors vying for general and specific personal data in real time or near-real time. Policymakers should develop legal guidelines that protect individuals' rights at group levels (e.g. driver/safety operator, passengers, pedestrians, other drivers or road users). In addition, they should outline strategies to resolve possible conflicts between data subjects that have claims over the same data (e.g. location data, sensor data etc.) or disputes between data subjects, data controllers and other parties (such as insurance companies etc.).	Type-approval, PTA's, data protection authorities.
5.4) Develop transparency strategies to inform particular road users about data collection and associated rights Transparency strategies to inform road users about data collection and associated rights should be researched, developed and implemented, as it is not possible to obtain consent for data processing from all single persons who appear in the vicinity of automated vehicles. It is also hardly possible to directly provide the identity and contact details of the data controller to these persons.	Type-approval, PTA's, data protection authorities.

Recommendation title and overview	*Concerned authorities*
5.5) Define appropriate anonymisation techniques and/or how successful anonymisation can be achieved in the field of AV's In the context of automated minibuses and mobility-related applications, what data is to be considered personal and non-personal (technical data) is not straightforward in all cases. Further guidance in this area would be necessary to avoid the proliferation of different interpretations of this concept, which has an important impact in practice.	Type-approval, PTA's, data protection authorities.
5.6) Increasing complexity of data processing schemes Automated vehicles and minibuses potentially involve multiple actors and complex data processing schemes, as described in the AVENUE vision's data loops. Their impact should be studied in details in order to provide and encourage appropriate legal solutions.	Type-approval, PTA's, data protection authorities.
5.7) Data minimization and purpose limitation principles Automated vehicles and minibuses have the possibility of processing personal data to a large scale, which may conflict with the GDPR's data minimization and purpose limitation principles. Solutions and best practices are needed to mitigate these conflicts.	Type-approval, PTA's, data protection authorities.

6 Competition

Recommendation title and overview	*Concerned authorities*
6.1) Regulate access to vehicle data As of today, vehicle manufacturers and/or tech companies developing automated vehicles and minibuses can control to whom and to which data they provide access to. This situation creates issues, such as the hindrance of both competition and technological development. Solutions should be debated and harmonised at political level.	Type-approval, PTA's, competition, data protection and cybersecurity authorities.
6.2) Anticipate the potential market power of MaaS providers Despite their numerous positive effects on mobility, MaaS providers will most likely gain important market power in the future. New players might enter the market with new business models and challenge established actors (especially in the field of public transport). It should be discussed and decided what role these players can and should play. Market distortions and monopolies/oligopolies that might take place in this field should be prevented.	PTA's, competition, data protection and cybersecurity authorities.
6.3) Creation of open datasets and open API's as public and open infrastructural resources Particularly useful and valuable data for the design, operation, use and deployment of automated vehicles should be identified and kept free and open, as they can be linked to infrastructural resources that support free innovation, competition and fair market conditions in the sector of automated vehicles.	PTA's, competition, data protection and cybersecurity authorities.

7 Civil liability

Recommendation title and overview	*Concerned authorities*
7.1) Ensure the existence of fair and quick compensation mechanisms Automated vehicles and minibuses will provide an overall increase in road safety and security in the long run, but in the short term they will inevitably be involved in accidents, possibly with the emergence of new kinds of accidents. In order to grant social acceptance, the existence of fair and effective mechanisms for granting compensation to victims of accidents should be ensured.	Authorities with (AV-related) lawmaking powers in the field of civil liability and proceedings.
7.2) Reversal or alleviation of the burden of proof Under the current European Product Liability Directive ("**PLD**") framework, the victim/affected party in an accident involving a product has to prove that the product was defective and that the defect caused the injury. In the context of automated vehicles, this solution is not satisfactory. The burden of proof (i.e. proving that the automated vehicle was not defective) should be alleviated or reversed and borne by industry operators, as they have access, control and information on the technical information and data related to accidents.	Authorities with (AV-related) lawmaking powers in the field of civil liability and proceedings.
7.3) Provide solutions to the complexity of value chains involving connected and automated vehicles The deployment of automated vehicles and minibuses implies a complex ecosystem with a plurality of actors involved in the services. This could result in increasing difficulties to assess where a potential damage originated and to assign liability. Forms of shared responsibility, as well as a shift towards liability of vehicle manufacturers and tech companies etc. should be studied, discussed and envisaged.	Authorities with (AV-related) lawmaking powers in the field of civil liability and proceedings.
7.4) Revise existing legal definitions and concepts The digitalisation of transports and the development of Artificial Intelligence have raised various points of discussions as regards central definitions of the PLD and the timeframe of its application. These definitions should be discussed, answered at a political level and regulated accordingly. A dedicated sector specific legislation (instead of the PLD) might be needed and should be studied.	Authorities with (AV-related) lawmaking powers in the field of civil liability and proceedings.

8 Traffic and communication infrastructure

Recommendation title and overview	*Concerned authorities*
8.1) Definition of minimum standards and harmonisation Automated vehicles are highly information dependent and if necessary information is missing, functional restrictions can occur. For the binding and reliable provision of decision-relevant data for automated driving, there is a need for a European legal framework coordinated across Member States as well as far-reaching investments. Discussions on the scope of a Europe-wide harmonisation of the road infrastructure (e.g. definition of a minimum set of standards for road traffic signs, markings or digital infrastructure) and the communication and interaction of automated vehicles with the infrastructure should take place quickly.	Authorities with (AV-related) lawmaking powers in the field of road infrastructure and road traffic rules
8.2) Road equipment characteristics and inspection procedures Various elements related to road equipment need to be investigated and clarified, such as the characteristics and minimum qualities for automated machine detection, the development of procedure for quality control and inspection procedures, as well as the location of road equipment in digital maps and their updating.	Authorities with (AV-related) lawmaking powers in the field of road infrastructure and road traffic rules
8.3) Ensure safe interaction channels with other road users The human driver's mutation into a mere passenger requires to find alternative and new means of communication between automated vehicles and other road users, replacing the "human" communication through gaze/gestures, traffic lights, horns, indicators etc. Development of procedures (e.g. best practices) for the safe interaction between automated vehicles and other road users, especially pedestrians/cyclists/PRMs are therefore necessary (for instance via communication with external users through displays).	Authorities with (AV-related) lawmaking powers in the field of road infrastructure and road traffic rules

8.4) Creation of "Digital twins" of the road traffic infrastructure The creation of a digital representation of the road traffic infrastructure should be studied – a so-called "Digital twin" that would store various conditions and information relevant for the vehicle guidance, that should also be suitable for cross-border traffic, therefore requiring harmonisation and standardisation.	Authorities with (AV-related) lawmaking powers in the field of road infrastructure and road traffic rules
8.5) Communication infrastructure The deployment of AV's will require various measures as regards communication infrastructure. An important task will be the creation of harmonised regulatory requirements in order to demonstrate interoperability between components, or the creation of regulations verifying performance of antennas. Periodic inspection of the communication infrastructure should also become mandatory.	Authorities with (AV-related) lawmaking powers in the field of road infrastructure and road traffic rules

9 Spatial planning

Recommendation title and overview	*Concerned authorities*
The large scale deployment of automated vehicles and minibuses has the potential to considerably change the architecture of existing road and traffic infrastructure, with potential gains in parking space, size reduction in vehicle lanes etc. The short term changes and measures to take, but also the medium to long term effects, should be studied and planned in details.	Authorities in charge of spatial planning

10 Driving permits

Recommendation title and overview	*Concerned authorities*
It will be necessary to examine if and how driving permits need to evolve in relation with the deployment of automated vehicles. For new drivers, modules related to the use of automated driving systems ("**ADS**") might be integrated in the existing cursus for instance. For current holders of a driving permit, the question of an additional training dedicated to ADS' should also be assessed, amongst others topics.	Authorities granting driving permits for conventional vehicles

11 Criminal liability

Recommendation title and overview	*Concerned authorities*
11.1) Investigate and define potential new criminal offences New undesirable behaviours will emerge with the deployment of automated vehicles and the existing cybercriminal activities will by no doubt target these vehicles. Their punishment through criminal law provisions will be necessary. In order to enact relevant provisions, these behaviours need to be identified soon enough and, ideally, anticipated though studies and monitoring of the use and misuses of this new technology.	Authorities with criminal legislative and enforcement powers
11.2) Shift towards corporate criminal liability Since an automated driving system instead of the human driver will perform the dynamic driving task, the question of a shift towards criminal liability of companies developing these systems should be examined, amongst others in the case of personal injury or damage to property.	Authorities with criminal legislative and enforcement powers

Executive Summary Conclusion

1 Since the beginning of the project in 2018 and its end in 2022, the legal landscape has started to change. In 2018, only few provisions dedicated to automated driving where existing – be it at international, European or national level. In 2022, national legal frameworks dedicated to the ordinary approval and deployment of automated vehicles and minibuses are in force in Member States like France and Germany, amongst others. The European Commission has published two promising regulations regarding the type-approval of automated vehicles and minibuses in the summer 2022. At international level, important bodies like the UNECE created AV-specific working groups. The signs are therefore positive, as politicians and lawmakers have now understood the necessity of monitoring, acting and regulating this rising industry that will very likely cause major disruptions in the coming years.

2 It is indeed particularly important to act today, as evolution of technology (and its speed in particular) is always hard to predict. The crucial point is not "if" automated vehicles will circulate on European roads in the future, but "when" and "how soon". Sudden deployments might potentially occur quickly and authorities as well as the public might face a "fait accompli" that should be avoided, as it would likely results (amongst others) in legal gaps that the concerned stakeholders might leverage for their own benefits. Some voices are anticipating important deployment of AV fleets at large scale by the year 2030, when others depict only mixed traffic by 2040, with many conventional vehicles still in circulation on European roads at this date. Industrial actors are currently planning the first large and commercial deployments for 2025 and following years, as European regulations might be updated by then and the European single market be opened to larger deployment than small series in 2024.

3 In this context, the partners of AVENUE agreed and consider of utmost importance to favour public transport solutions due to their positive outcome on our future societies. This should be reflected by policymakers giving priority to these solutions, amongst others through quick and favourable lawmaking and encouraging behaviour in this particular (sub)field of the AV industry.

4 The importance of acting now is also caused by the fact that budgets for public transportation of the coming years are already being discussed and decided today. Automated vehicles and minibuses will require very important infrastructural investments and changes that should be anticipated, planned and budgeted as soon as possible in order to maximise the positive outcome of vehicle automation.

5 From a legal point of view, the need to legislate encompasses different levels and branches. From a "vertical" point of view, legislative changes are required at all levels, be it international, regional/European, national and intra-national levels. From a horizontal point of view, legal amendments are not only necessary in the specific sector of type-approval regulations, but in many other branches, as briefly presented in this document.

6 Automated vehicles and minibuses will be one of the first industry where automation, advanced robotics, AI and IoT products will deploy and change the lives of millions of people. Therefore, orienting, monitoring and guiding these changes through legislation should be guaranteed from the beginning. Policymakers acting too late might result in undesirable effects and issues.

Introduction

AVENUE aims to design and carry out full-scale demonstrations of urban transport automation by deploying, for the first time worldwide, fleets of Automated minibuses in low to medium demand areas of 4 European demonstrator cities (Geneva, Lyon, Copenhagen and Luxembourg) and 2 to 3 replicator cities. The AVENUE vision for future public transport in urban and suburban areas, is that Automated vehicles will ensure safe, rapid, economic, sustainable and personalised transport of passengers. AVENUE introduces disruptive public transportation paradigms on the basis of on-demand, door-to-door services, aiming to set up a new model of public transportation, by revisiting the offered public transportation services, and aiming to suppress prescheduled fixed bus itineraries.

Vehicle services that substantially enhance the passenger experience as well as the overall quality and value of the service will be introduced, also targeting elderly people, people with disabilities and vulnerable users. Road behaviour, security of the Automated vehicles and passengers' safety are central points of the AVENUE project.

At the end of the AVENUE project four-year period the mission is to have demonstrated that Automated vehicles will become the future solution for public transport. The AVENUE project will demonstrate the economic, environmental and social potential of Automated vehicles for both companies and public commuters while assessing the vehicle road behaviour safety.

On-demand Mobility

Public transportation is a key element of a region's economic development and the quality of life of its citizens.
Governments around the world are defining strategies for the development of efficient public transport based on different criteria of importance to their regions, such as topography, citizens' needs, social and economic barriers, environmental concerns and historical development. However, new technologies, modes of transport and services are appearing, which seem very promising to the support of regional strategies for the development of public transport.
On-demand transport is a public transport service that only works when a reservation has been recorded and will be a relevant solution where the demand for transport is diffuse and regular transport is inefficient.
On-demand transport differs from other public transport services in that vehicles do not follow a fixed route and do not use a predefined timetable. Unlike taxis, on-demand public transport is usually also not individual. An operator or an automated system takes care of the booking, planning and organization.
It is recognized that the use and integration of on-demand Automated vehicles has the potential to significantly improve services and provide solutions to many of the problems encountered today in the development of sustainable and efficient public transport.

Fully Automated Vehicles

A self-driving car, referred in the AVENUE project as **a Fully Automated Vehicle** (**AV**), also referred as Autonomous Vehicle, is a vehicle that is capable of sensing its environment and moving safely with no human input.

The terms *automated vehicles* and *autonomous vehicles* are often used together. The Regulation 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles defines "automated vehicle" and "fully automated vehicle" based on their autonomous capacity:

- An "automated vehicle" means a motor vehicle designed and constructed to move autonomously for certain periods of time without continuous driver supervision but in respect of which driver intervention is still expected or required
- "fully automated vehicle" means a motor vehicle that has been designed and constructed to move autonomously without any driver supervision

In AVENUE we operate ***Fully Automated minibuses for public transport***, (previously referred as Autonomous shuttles, or Autonomous buses), and we refer to them as simply *Automated minibuses* or *the AVENUE minibuses.*

In relation to the SAE levels, the AVENUE project operated SAE Level 4 vehicles.

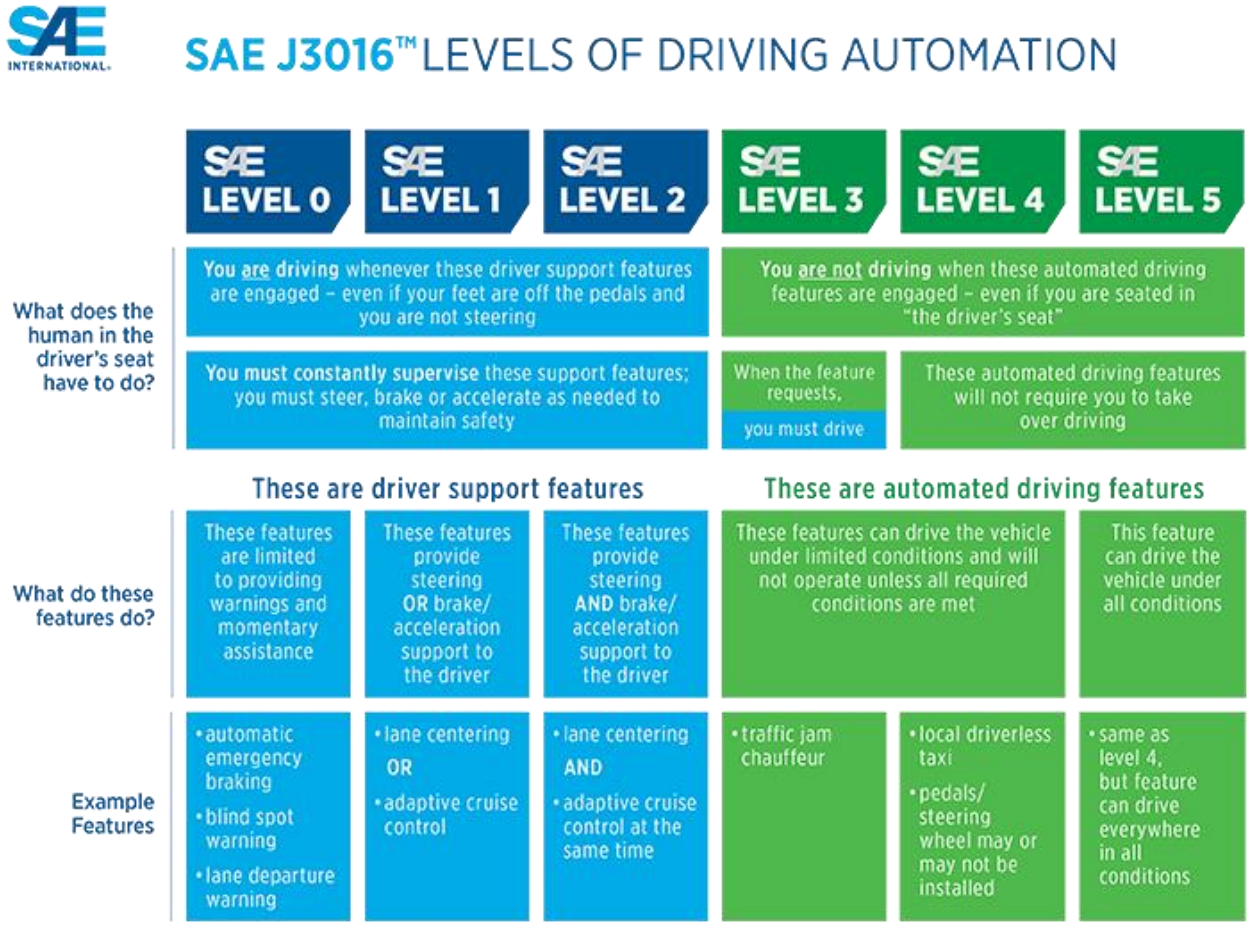

Table 1: SAE Driving Automation levels (©2020 SAE International)

Automated vehicle operation overview

We distinguish in AVENUE two levels of control of the AV: micro-navigation and macro-navigation. Micro navigation is fully integrated in the vehicle and implements the road behaviour of the vehicle, while macro-navigation is controlled by the operator running the vehicle and defines the destination and path of the vehicle, as defined the higher view of the overall fleet management.

For micro-navigation Automated Vehicles combine a variety of sensors to perceive their surroundings, such as 3D video, LIDAR , sonar, GNSS, odometry and other types sensors. Control software and systems, integrated in the vehicle, fusion and interpret the sensor information to identify the current position of the vehicle, detecting obstacles in the surround environment, and choosing the most appropriate reaction of the vehicle, ranging from stopping to bypassing the obstacle, reducing its speed, making a turn etc.

For the Macro-navigation, that is the destination to reach, the Automated Vehicle receives the information from either the in-vehicle operator (in the current configuration with a fixed path route), or from the remote control service via a dedicated 4/5G communication channel, for a fleet-managed operation. The fleet management system takes into account all available vehicles in the services area, the passenger request, the operator policies, the street conditions (closed streets) and send route and stop information to the vehicle (route to follow and destination to reach).

Automated vehicle capabilities in AVENUE

The Automated vehicles employed in AVENUE fully and automatically manage the above defined, micro-navigation and road behaviour, in an open street environment. The vehicles are Automatically capable to recognise obstacles (and identify some of them), identify moving and stationary objects, and Automatically decide to bypass them or wait behind them, based on the defined policies. For example with small changes in its route the AVENUE mini-bus is able to bypass a parked car, while it will slow down and follow behind a slowly moving car. The AVENUE mini-buses are able to handle different complex road situations, like entering and exiting round-about in the presence of other fast running cars, stop in zebra crossings, communicate with infrastructure via V2I interfaces (ex. red light control).

The mini-buses used in the AVENUE project technically can achieve speeds of more than 60Km/h. However this speed cannot be used in the project demonstrators for several reasons, ranging from regulatory to safety. Under current regulations the maximum authorised speed is 25 or 30 Km/h (depending on the site). In the current demonstrators the speed does not exceed 23 Km/h, with an operational speed of 14 to 18 Km/h. Another, more important reason for limiting the vehicle speed is safety for passengers and pedestrians. Due to the fact that the current LIDAR has a range of 100m and the obstacle identification is done for objects no further than 40 meters, and considering that the vehicle must safely stop in case of an obstacle on the road (which will be “seen” at less than 40 meters distance) we cannot guarantee a safe braking if the speed is more than 25 Km/h. Note that technically the vehicle can make harsh break and stop with 40 meters in high speeds (40 -50 Km/h) but then the break would too harsh putting in risk the vehicle passengers. The project is working in finding an optimal point between passenger and pedestrian safety.

Due to legal requirements a **Safety Operator** must always be present in the vehicle, able to take control any moment. Additionally, at the control room, a **Supervisor** is present controlling the fleet operations. An **Intervention Team** is present in the deployment area ready to intervene in case of incident to any of the mini-busses. In table 2 provides and overview of the AVENUE sites and ODDs.

	Summary of AVENUE operating sites demonstrators							
	TPG		Holo		Keolis	Sales-Lentz		
	Geneva		Copenhagen	Oslo	Lyon	Luxembourg		
Site	Meyrin	Belle-Idée	Nordhavn	Ormøya	ParcOL	Pfaffental	Contern	Esch sur Alzette
Funding	TPG	EU + TPG	EU + Holo	EU + Holo	EU + Keolis	EU + SLA	EU + SLA	EU + SLA
Start date of project	August 2017	May 2018	May 2017	August 2019	May 2017	June 2018	June 2018	February 2022
Start date of trial	July 2018	June 2020	September 2020	December 2019	November 2019	September 2018	September 2018	April 2022
Type of route	Fixed circular line	Area	Fixed circular line	Fixed circular line	Fixed circular line	Fixed circular line	Fixed circular line	Fixed circular line
Level of on-demand service*	Fixed route / Fixed stops	Flexible route / On-demand stops	Fixed route / Fixed stops	Fixed route / Fixed stops	Fixed route/Fixed stops	Fixed route / Fixed stops	Fixed route / Fixed stops	Fixed route / Fixed stops
Route length	2,1 km	38 hectares	1,3 km	1,6 km	1,3 km	1,2 km	2,3 km	1 km
Road environment	Open road	Semi-private	Open road	Open road	Open road	Public road	Public road	Main pedestrian road
Type of traffic	Mixed	Mixed	Mixed	Mixed	Mixed	Mixed	Mixed	Pedestrians, bicycles, delivery cars
Speed limit	30 km/h	30 km/h	30 km/h	30 km/h	8 to 10 km/h	30 km/h	50 km/h	20 km/h
Roundabouts	Yes	Yes	No	No	Yes	No	No	No
Traffic lights	No	No	No	No	Yes	Yes	Yes	No
Type of service	Fixed line	On demand	Fixed line	Fixed line	Fixed line	Fixed line	Fixed line	On Demand
Concession	Line (circular)	Area	Line (circular)	Line (circular)	Line (circular)	Line (circular)	Line (circular)	Line (circular)
Number of stops	4	> 35	6	6	2	4	2	3
Type of bus stop	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed	Fixed
Bus stop infrastructure	Yes	Sometimes, mostly not	Yes	Yes	Yes	Yes	Yes	Yes
Number of vehicles	1	3-4	1	2	2	2	1	1
Timetable	Fixed	On demand	Fixed	Fixed	Fixed	Fixed	Fixed	On-demand
Operation hours	Monday-Friday (5 days)	Sunday-Saturday (7 days)	Monday-Friday (5 days)	Monday-Sunday (7 days)	Monday-Saturday (6 days)	Tuesday & Thursday Saturday, Sunday & every public holiday	Monday - Friday	Monday – Saturday
Timeframe weekdays	06:30 – 08:30 / 16:00 – 18:15	07:00 – 19:00	10:00 – 18:00	7:30 – 21:30	08:30 – 19:30	12:00 – 20h00	7:00 – 9:00 16:00 – 19:00	11:00 – 18:00 11:00 – 18:00
Timeframe weekends	No service	07:00 – 19:00	No service	9:00 – 18:00	08:30 – 19:30	10:00 – 21:00	No Service	On Suterday only
Depot	400 meters distance	On site	800 meters distance	200 meters distance	On site	On site	On site	500 m distance
Driverless service	No	2021	No	No	No	No	No	No
Drive area type/ODD	B-Roads	Minor roads/parking	B-Roads/minor roads	B-Roads	B-Roads	B-Roads	B-Roads/parking	
Drive area geo/ODD	Straight lines/plane	Straight lines/ plane	Straight lines/ plane	Curves/slopes	Straight Lines/ plane	Straight lines/ plane	Straight lines/ plane	Straight lines / plane
Lane specification/ODD	Traffic lane	Traffic lane	Traffic lane	Traffic lane	Traffic lane	Traffic lane	Traffic lane	Open area
Drive area signs/ODD	Regulatory	Regulatory	Regulatory, Warning	Regulatory	Regulatory	Regulatory	Regulatory	Regulatory
Drive area surface/ODD	Standard surface, Speedbumps	Standard surface, Speedbumps	Standard surface Speedbumps, Roadworks	Frequent Ice, Snow	Standard surface, Potholes	Standard surface	Standard surface	Standard Surrface

Table 2: Summary of AVENUE operating site (+ODD components)

1 Overarching recommendations

1 Politicians and authorities must not simply leave the introduction of automated vehicles to themselves or to the market. Rather, they must steer the use of automated vehicles in an orderly manner right from the start and create favourable framework conditions for an effective and, from a transport policy perspective, desirable use of these promising new technologies[4].

2 Until now, a new technology was first developed and then standardised and regulated. The challenge with automated driving systems is that development, standardisation and regulation need to progress in parallel as much as possible in order to keep up with the pace of the technological developments[5]. Therefore, the (existing and upcoming) regulatory framework should be as flexible as possible[6] in order to avoid hindering the technological developments and without compromising on safety.

1.1 Prioritising public transportation

Issue: The current lawmaking momentum at international and national level lies mostly with the regulation of privately owned automated vehicles[7] (see for instance the 2020 UN Regulation 157 on ALKS and its 2022 extension to speeds up to 130 km/h) or robotaxis[8].

Proposed solution: Priority should be given to the regulation of shared automated public transport solutions such as automated minibuses, which will provide greater and better societal benefits.

Explanation: Legislative bodies and regulators have a short window of opportunity to take over the governance from private actors. The recent legal developments of automated vehicles are driven by important private stakeholders such as manufacturers of vehicles, who are developing automated driving systems for conventional vehicles, and/or new stakeholders within the automotive industry, namely "tech" companies who are developing software and working on solutions for retrofitting automated driving systems on conventional vehicles, transforming them into robotaxis. Both type of actors strive to have the technologies they are currently developing being regulated. Solutions such as robotaxis[9],

[4] Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, SVI 2017/044, 1691, October 2020, § 5.1 p. 51.

[5] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 3.1.1.2 p. 13.

[6] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 5 p. 23.

[7] E.g. automated vehicles that are deployed as privately owned automated cars for private use (for further details see AVENUE vision 2030: A citizen centric approach, Position paper, § 1).

[8] A robotaxi, also known as a self-driving taxi or a driverless taxi, is an autonomous car (SAE automation level 4 and beyond) operated for a ridesharing company (for further details see AVENUE vision 2030: A citizen centric approach, Position paper, § 1).

[9] In important federal States of the United States (such as California and Arizona, Florida lately), companies related to vehicle manufacturers (such as Cruise, acquired by General Motors) or tech companies (such as Waymo, a subsidiary of Alphabet Inc., parent company of Google) are currently deploying robotaxis in regular commercial operations (and not under an experimentation regime).

automated highway driving systems[10], valet parking etc. are currently or have already been regulated, although these solutions provide less societal benefits and even undesirable negative externalities[11].

3 This leaves small room to the regulation of shared automated public transport solutions, although positive signs are emitted from the various recent legislative acts of, amongst others, France[12] and Germany[13] and, at European level, the European Commission's Delegated regulation as regards fully automated vehicles produced in small series[14] and the Implementing regulation as regards the automated driving system of fully automated vehicles[15] published in July respectively August 2022[16].

4 For the public good, automated vehicles should be used collectively as far as possible. The existing regulatory framework must be adapted in such a way that the emergence of new collective forms of service in commercial private and public transport is possible. The public sector should create favourable conditions for the integration of collectively used automated vehicles into the overall transport system[17].

5 It is also important as foreign companies from the United States of America are currently dominating the volume of kilometres driven by automated vehicles via experimental or, more recently, commercial deployment of robotaxis. Asian countries such as China are focusing on shared automated minibuses, but often based on technological solutions and rely on infrastructures that raises concerns about personal privacy of individuals, amongst others. European companies could therefore position themselves as pioneers of automated minibuses between these two approaches through encouraging legislation.

6 In order to safeguard innovation at European level, a French parliamentary report published in 2021 has suggested to establish and define European positions and to translate them into regulations, and then to defend them at the international level at the UNECE in Geneva[18]. The same reports also suggests to create

[10] UN Regulation 157 on Automated Lane Keeping System (initially a "highway traffic jam assistant") has been extended end of 2021 in order to cover lane changes and a speed until 130 km/h (see Appendix A, N 322 and 333) .

[11] AVENUE vision 2030: A citizen centric approach, Position paper, § 1 and the quoted references.

[12] See Appendix A § 1.3.3 and § 5.3.1 for further information.

[13] See Appendix A § 1.3.4 and § 5.3.2 for further information.

[14] Commission delegated regulation of 20 June 2022 amending Annexes I, II, IV and V to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the technical requirements for vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update, C(2022) 3823 final, and its four Annexes ("**Commission delegated regulation as regards the technical requirements for fully automated vehicles produced in small series**").

[15] Commission implementing regulation of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles, C(2022) 5402 final, and its four Annexes ("**Commission implementing regulation as regards the type-approval of ADS**").

[16] See Appendix A § 1.2.3 and § 1.2.4 for further information.

[17] Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, SVI 2017/044, 1691, October 2020, § 5.2 p. 52.

[18] PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, p. 10.

an "Important Project of Common European Interest" ("**IPCEI**") dedicated to automated and autonomous vehicles, that would go beyond the experimental character of the CCAM project[19].

1.2 Harmonisation, coordination, cooperation and standardisation

Introduction

7 Harmonisation[20], coordination and cooperation in the development of automated vehicles are important topics. They are particularly needed in many sectors such as personal privacy, accessibility and liability, as exposed in the dedicated recommendations below.

8 This process already started with "soft law"[21] in April 2016 with the Declaration of Amsterdam on connected and automated driving[22]. In this Declaration, European Member States, the European Commission and representatives of the private sector have agreed on joint goals and joint actions to facilitate the introduction of connected and automated driving on Europe's roads[23].

9 Fragmentation of the legal frameworks of the Member States and uneven development of automated vehicles is a frequent issue within the European Union that should be avoided. Although national initiatives of Member States such as France and Germany to regulate automated vehicles and automated driving systems at their national level are a positive development and should be welcomed, as they may serve as a model for the development of upcoming legislative acts, but they also materialise the fragmentation and uneven development of legislation within the Member States. Fragmentation negatively impacts producers and other businesses in the supply chain, but also road users[24].

---

[19] PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, § 4.4 p. 107 et seq.

[20] In the European Union, "harmonisation of law" (or simply "harmonisation" or "harmonization") is the process of creating common standards across the internal market. Though each Member State has primary responsibility for the regulation of most matters within its jurisdiction, and consequently each has its own laws, harmonisation aims to (i) create consistency of laws, regulations, standards and practices, so that the same rules will apply to businesses that operate in more than one member state, and so that the businesses of one state do not obtain an economic advantage over those in another as a result of different rules, as well as (ii) reduced compliance and regulatory burdens for businesses operating nationally or transnationally (https://en.wikipedia.org/wiki/Harmonisation_of_law, last consultation 29 August 2022).

[21] The term "soft law" refers to quasi-legal instruments (like recommendations or guidelines) which do not have any legally binding force or whose binding force is somewhat weaker than the binding force of traditional law. Soft law is often contrasted to "hard law". The term "soft law" initially emerged in the context of international law although more recently it has been transferred to other branches of domestic law as well.

[22] Declaration of Amsterdam, Cooperation in the field of connected and automated driving, Navigating to connected and automated vehicles on European roads, 14-15 April 2016.

[23] https://www.government.nl/topics/mobility-public-transport-and-road-safety/question-and-answer/what-is-the-declaration-of-amsterdam-on-selfdriving-and-connected-vehicles (last consultation 29 August 2022).

[24] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4 p. 10.

1.2.1 Harmonisation of rules and integration of cross-border dimensions

10 **Issue:** In its Sustainable and smart mobility strategy[25], the European Commission has recognized that "the lack of harmonisation and coordination of relevant road traffic rules and liability for automated vehicles needs to be addressed".

Proposed solution: Proceed to assessments, comparative analysis' and discussions of the sectoral legislation that will be AV relevant, in particular road traffic rules, the experimentation and liability frameworks (amongst others), that are regulated at national level primarily (and not harmonised yet).
Explanation: An aligned and holistic European approach to global questions on automated driving, including road traffic rules, experimental or liability aspects would be desirable from a single market perspective and for promoting European industrial global leadership, as well as in terms of materialization of road safety benefits[26]. One of the important hurdles to tackle is that some sectors mostly depend on national legislations, while others are regulated at international and/or regional (European) level.

11 From a factual point of view, the international character of operating automated vehicles and the complexity it will imply for legislative works should not be underestimated, as showed by the following examples: a company based or operating from one state (potentially outside of the European Union) might provide automated driving services (including mapping, remote supervision etc.) for vehicles operating in another state (potentially an European Member State). Similarly, an individual physically present in one state might play a role in the provision of automated driving services for vehicles in another state etc.[27].

12 As regards national laws, they should be discussed and compared for three reasons at least. First, the comparative analysis of national rules helps to assess whether and to what extent existing national laws, if not adapted, will be able to adjust effectively to the challenges of new technologies[28].

13 Second, the comparative legal analysis also contributes to a better understanding of existing similarities and differences amongst jurisdictions, which in turn, helps to assess to what extent the existing differences may potentially lead to legal uncertainty and fragmentation[29].

---

[25] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 57 p. 12.
[26] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 617 p. 151.
[27] UNECE's Informal document No. 2 (GE.3-03-02), Initial thoughts on "road safety challenges posed by the use of automated vehicles in traffic that an international legal instrument could adequately address", Submitted by Professor Bryant Walker Smith, § 16 et seq. p. 3.
[28] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4 p. 10.
[29] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4 p. 10.

14 Finally, the comparative analysis of national law also provides an interesting regulatory test bed for possible public policy solutions[30].

15 As mentioned above, the experience gathered during the drafting of the French and German (amongst others) legal frameworks dedicated to automated vehicles was useful when drafting the European Commission's Delegated[31] and Implementing[32] Regulations published in 2022. The downside was that during the public consultation of spring 2022, it was requested to insert "opening clauses" in these European regulations[33] as investments were already made in the meantime, with the goal to comply with the already published national frameworks. Such "opening clauses" should allow for parallel applicability of the two European Regulations and the (prior) national regulatory frameworks, which might hamper the harmonising effect.

16 This being said, the existing and enacted national laws related to automated vehicles provide a wealth of information that can and should be used as a basis for discussions and researches for a common European approach.

17 Fragmentation increases compliance costs for companies operating in multiple Member States[34]. Due to their moving and movable nature, automated vehicles are designed to operate in multiple jurisdictions from a technical point of view with operational design domains able to be located in cross-border areas.

18 As an example of potential fragmentation, the horizontal General Data Protection Regulation ("**GDPR**") leaves room for different interpretations by each of the national Data Protection Authorities ("**DPAs**") and national courts, impinging on the cross-border provision of data-based services and resulting in legal fragmentation[35]. DPAs can adopt different types of sanctions in case of infringements to the GDPR and are for instance already applying different rules to visual personal data processed and recorded by in-

[30] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4 p. 10.

[31] Commission delegated regulation of 20 June 2022 amending Annexes I, II, IV and V to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the technical requirements for vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update, C(2022) 3823 final, and its four Annexes.

[32] Commission implementing regulation of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles, C(2022) 5402 final, and its four Annexes.

[33] See feedback published under https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12152-Automated-cars-technical-specifications_en (last consultation 23 August 2022), for instance of the Association of German Transport Companies (VDV e.V., Proposal 2) or Waymo, p. 9.

[34] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 123.

[35] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 198.

vehicle "dashcams"[36], which trigger similar issues that the cameras used by automated vehicles. As discussed further below, coordination between Member States should be ensured when it comes to the implementation and interpretation of the GDPR in the field of cooperative, connected and automated mobility[37].

19 In the sector of product liability, Member States have the possibility to regulate civil proceedings despite the material harmonisation resulting from the Product Liability Directive (see also N 259 below), which creates uneven and different practices between Member States[38].

20 The European Commission has already acknowledged in its Sustainable and Smart Mobility Strategy that further coordination capacity may be needed at European level in relation to the deployment and management of ITS and CCAM across Europe, including in areas such as:

- type-approval and market surveillance;
- roadworthiness inspection methods;
- road traffic rules for automated mobility;
- road infrastructure;
- other detailed European level safety and related tasks;
- software updates; and
- preparation of technical rules, coordination amongst national authorities' actions, and collection and analysis of relevant data[39].

21 Part of these works have already begun but further important efforts are urgently needed.

[36] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 198.

[37] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 198; see also BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 4.2 p. 16.

[38] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 5.1.2 p. 99 and § 4.2.1 p. 92; see also BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.3.2 p. 59.

[39] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 623 p. 152.

1.2.2 Coordination between authorities

Issue: The transport services operated by automated vehicles are at the intersection of different regulatory regimes and will require collaboration and cooperation between approval, data protection and competition authorities, at least.

Proposed solution: In a first step, create (new) formal or informal exchange platform(s) between the concerned authorities helping to understand where connections need to be made and identify potentially overlapping regulations or conversely gaps in legislation. In a second step, assess the need and relevance of creating new AV-dedicated authorities or centralizing tasks to a single (existing or new) authority.

Explanation: In the field of digital services, there is a need in Europe to better coordinate between regulators in charge of different legal regimes, for example the data protection regulator cooperating with competition authorities[40]. For automated vehicles, sectoral coordination between various authorities within the same jurisdiction will be necessary.

22 Automated vehicles will be approved by the existing type-approval authorities. Although the complete type-approval framework is not completely defined yet, it seems likely that the type-approval authority will have to process vehicle data for monitoring the cybersecurity of the automated vehicles and the software update management systems, which might also imply privacy questions related to personal data that would fall under the scope of data protection authorities (see Appendix A § 4.1 et seq.). In addition, in order to avoid any market distortion (see § 6 below and Appendix A § 3.2.5 et seq.), competition authorities might also have to monitor the processing and access to vehicle data that will potentially trigger competition issues.

23 The Law Commissions of the United Kingdom and Scotland discussed many questions related to an "in-use regulator" that would receive responsibilities to monitor the safety of approved automated vehicles and investigate infractions involving AVs, and powers to enforce its decisions. One of the questions left open was whether this authority should function under separate bodies or if it could be the same than the type-approval authority. Arguments in favour of centralization where the concentration of expertise and preventing issues from gaps between two entities. The existence of possible conflicts of interests was quoted against such centralisation[41].

24 At European/EFTA[42] level, coordination between authorities will be necessary and prove useful, due to their different levels of progression. The legislation in some Member States is at an advanced stage, while

[40] https://cerre.eu/publications/improving-eu-institutional-design/ (last consultation 29 August 2022), for further details see MONTI/DE STREEL, Centre on regulation in Europe (CERRE), Improving EU institutional design to better supervise digital platforms, Report, January 2022.

[41] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.11 p. 92 et seq.

[42] The European Free Trade Association ("**EFTA**") is a regional trade organization and free trade area consisting of four European states: Iceland, Liechtenstein, Norway and Switzerland. The organization operates in parallel with the European Union and all four member states participate in the European Single Market.

until recently, a few Member States did not even have experimental regulations allowing to test automated vehicles[43].

25 As an example, national type-approval authorities experienced with the approval of automated minibuses have assisted their counterpart in another country during the FABULOS project, where the Estonian Road Authorities provided insights about the process as executed in Estonia to their Greek counterparts[44]. The creation of dedicated advisory authorities, for instance similar to the European Data Innovation Board proposed by the Digital Governance Act or the European Artificial Intelligence Board proposed by the Artificial Intelligence Act, should be discussed.

26 Under the current state, at international level, an authority in one state might need to access safety-related data from another state (outside the European Union, such as the United States of America) in order to assess the performance or investigate an incident involving an automated vehicle. These data might include personally identifiable or business-proprietary information. A law enforcement authority in one state may need to issue, track and enforce a citation issued to an entity responsible for an automated vehicle that is based in another state[45]. Such constellations might trigger various issues. Considerations as to data sovereignty (and the tension with the principle of free flow of data) should be reassessed.

1.2.3 Cooperation between all stakeholders

Issue: Regulating automated vehicles in an efficient manner will require participation of all stakeholders involved: vehicle manufacturers, researchers, deployers, PTO's, public transport authorities, further service providers, road users and the public in general.

Proposed solution: Develop collaboration mechanisms, such as roundtables, forums and/or independent bodies involving all AV-relevant private and public stakeholders.

Explanation: In the context of automated vehicles, where the existing regulations are insufficient or not (yet) adapted, various models can be implemented to regulate fast evolving technologies and business models, such as collaborative regulation, where all stakeholders get involved in the definition of the regulation/policy through an inclusive approach, with the sharing of knowledge and resources[46].

27 Beyond the regulation through hard law, the European Union should identify and facilitate cross-sectoral communication across governance levels and industry sectors and drive consultations around common needs between public and private parties, amongst others by:

---

[43] FABULOS H2020, Policy paper, D5.6 – Future application and impact of project results and learnings, 30 March 2021, § 3.6 STCP Porto p. 50 and § 3.6.6 STCP Porto: Legal findings p. 53.

[44] FABULOS H2020, Policy paper, D5.6 – Future application and impact of project results and learnings, 30 March 2021, § 3.6.6 Lamia pilot: Legal findings, p. 50.

[45] UNECE's Informal document No. 2 (GE.3-03-02), Initial thoughts on "road safety challenges posed by the use of automated vehicles in traffic that an international legal instrument could adequately address", Submitted by Professor Bryant Walker Smith, § 20 and 26 p. 4.

[46] International Association of Public Transport (UITP), GECKO, Project Brief, Governance and regulation models to manage disruptive mobility services, Brussels, October 2021, p. 4 and 5.

- Encouraging the establishment of collaboration mechanisms or forums that include local and national governments and are organised at a regular interval;
- Providing guidance, best practices and communication support. This would also help the European Union to set policy directions[47].

28 Experimentation of automated minibuses represents a sector in need of private-public cooperation.

29 As they participate in filing requests in each jurisdiction where their automated vehicles have been deployed, vehicle manufacturers have gathered valuable experience in the approval of automated minibuses that they can share with authorities, amongst others to those not accustomed to granting approval for experimentations of automated minibuses. In addition of relying on their counterparts in other jurisdictions, type-approval and other concerned authorities deprived of experience in granting approval to automated minibuses should rely on the existing experience gathered from stakeholders in similar projects.

30 As suggested below (see below § 2.1.6.3), the advisable process of creating guidelines and checklists will also need the involvement of all stakeholders in order to produce a better output than following a traditional top-down approach.

31 For instance, it has been suggested to establish forums to consider how these road traffic rules and other traffic laws might be adapted for automated vehicles. This would allow vehicle manufacturers, tech companies, software developers, deployers, authorities and road user groups and other experts to identify, share and discuss together issues of concern. Such forum should not have lawmaking powers, but provide recommendations to the authorities[48].

32 Cooperation will also be needed in other sectors, such as the identification and protection of free, open and high-value datasets for CAV design, deployment, and use (see below Recommendation § 6.3) and in establishing transparency strategies to inform third parties of data collection (see below Recommendation § 5.4), for collision investigation (see below N 72) and for accessibility needs of PRM and their technical regulation (see below N 73 and N 0).

33 It has also been suggested to establish independent bodies including representatives of consumer organisations to systematically conduct audits on specific algorithmic applications in AV operation and use, amongst others in order to develop long-term standards and good practice recommendations to be communicated to manufacturers, deployers and PTO's[49].

[47] International Association of Public Transport (UITP), GECKO, Project Brief, Governance and regulation models to manage disruptive mobility services, Brussels, October 2021, p. 7.

[48] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 3.30 p. 16.

[49] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 45.

1.2.4 Standardisation

Issue: Vehicle and component manufacturers as well as service providers tend to rely on their proprietary standards, particularly in the field of data processing. As such, limited interoperability generates high curation costs when data are transferred from one company to another and, ultimately, high costs to develop new services[50].

Proposed solution: Interoperability in services based on vehicle-generated data can be fostered by:

- Establishing a European Telecommunications Standards Institute ("**ETSI**") task force on standardisation of in-vehicle data with a view to support data sharing, working closely with other standardisation bodies to produce and promote common standards. This standardisation work should engage different groups of stakeholders, including vehicle manufacturers, automotive suppliers, network operators, service providers, software developers but also representatives of other interest groups, outside of the industry, such as NGO's, civil society organisations, consumer associations and other actors. This task might also take place outside of the European Union at international level, for instance within the International Telecommunication Union ("**ITU**").
- Promoting initiatives to improve standardisation and interoperability in the automotive sector, with a focus on sharing best practices[51].

Explanation: Uniform international and/or European standards for the exchange of mobility data must be created, with the creation of binding specifications for the implementation of these standards, including quality-of-service levels. Only in this way can a simple and far-reaching networking of vehicles and their integration into a mobility ecosystem succeed[52].

34 This concerns also the payment and ticketing. The lack of common rules regarding fare dynamic data access and use for both public and private operators increases the complexity and reduces opportunities for integrated ticketing and payment systems to be developed[53].

35 Further, the AVENUE experimentation has identified the lack of standards regarding high definition ("**HD**") maps and the lack of interoperability between manufacturers' HD maps as an important hurdle to the scale-up of automated minibuses.

---

[50] IACOB/CAMPMAS/SIMONELLI (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Annex IV Recommendations to the EU and national policy makers and an action plan for the creation of shared EU-wide in-vehicle data platforms, EASME/COSME/2018/004, 20 April 2021, p. 255.

[51] IACOB/CAMPMAS/SIMONELLI (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Annex IV Recommendations to the EU and national policy makers and an action plan for the creation of shared EU-wide in-vehicle data platforms, EASME/COSME/2018/004, 20 April 2021, p. 255.

[52] Nationale Plattform Zukunft der Mobilität (NPM), Ergebnisbericht der Nationalen Plattform Zukunft der Mobilität – Ergebnisse aus drei Jahren NPM (2018-2021), October 2021, § 3.3 p. 46.

[53] FRAZZANI/TARANIC/JENSEN/ZAMBONI/NOTI/PIANTONI, Remaining challenges for EU-wide integrated ticketing and payment systems, Final Report, published by the European Commission, Directorate-General for Mobility and Transport, July 2019, § 5.6 p. 73.

36 Regarding the contractual relations between the parties, the creation of standard contracts for the integration of mobility services on platforms has been suggested, as it may help to create a uniform and thus more easily comprehensible legal framework[54].

37 As regards standardisation of AI (and within the proposal of the AI Act), it should be noted that scholars have considered that standardisation of AI systems is not a matter of purely technical decisions and that they imply a series of ethical and legal decisions to be made. Such decisions cannot be outsourced to private standard developing organizations, but require a political debate involving society as a whole[55].

1.2.5 Uniform terminology

Issue: SAE Levels are complicated to apprehend for the non-initiated public. The terminology used by vehicle manufacturers (amongst other stakeholders) to describe the automated driving technologies should not mislead the public and create expectations that are not met in reality by the actual technology.

Proposed solution: Provide a certain level of harmonisation that would increase the public's awareness and comprehension.

Explanation: As of today, there are numerous and redundant definitions and concepts. A cross-domain harmonisation should be pursued, without introducing new competing definitions[56].

38 Terminology influences the users' expectations of functionalities and operations. Therefore, the names must not mislead the users, for example by suggesting that the vehicle's system will drive itself (e.g. "Autopilot", "ProPilot", "Drive Pilot" etc.) such as a understood for a SAE Level 5 automated vehicle. The name must truly be a reflection of the functionality[57]. It has even been suggested to create criminal offences for commercial practices that would create a likelihood of confusion amongst the public licensed to drive[58].

39 In July 2022, the California Department of Motor Vehicles has accused a vehicle manufacturer to have "made or disseminated statements that are untrue or misleading, and not based on facts" in a pair of complaints filed with the state Office of Administrative Hearings[59].

---

[54] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Digitalisierung für den Mobilitätssektor, Plattformbasierte intermodale Mobilität und Handlungsempfehlungen zu Daten und Sicherheit, Dritter Zwischenbericht, Juli 2020, § 4.2.4 p. 12; Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppen 3 und 6, Daten und Vernetzung – Standards und Normen für eine intermodale Mobilität, Juli 2021, § 2.2 p. 12.

[55] EBERS, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022, § 6 p. 22.

[56] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, Standards und Normen für die Mobilität der Zukunft, Ergebnisse der Arbeitsgruppe 6 der NPM 2018–2021, Abschlussbericht 10/2021, October 2021, § 2.3 p. 21.

[57] TSAPI et al. (Haskoningdhv Nederland BV for FIA Region I), How to maximize the road safety benefits of ADAS?, BH3649-RHD-ZZ-XX-RP-Z-0001, 14 December 2020, § 4.4 p. 37.

[58] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 7.45 p. 130 et seq.

[59] https://www.latimes.com/business/story/2022-08-05/dmv-false-advertising-tesla (last consultation 29 August 2022).

40 Within the AVENUE project, terminology has also been discussed around concepts like the safety operator and remote supervision that have encountered various names. These concepts are a good example of the lack of uniformity, be it at legislative or experimental/deployment level.

2 Recommendations related to the type-approval framework of automated minibuses

Introduction

41 Due to their automated nature, automated vehicles and minibuses will need to be monitored both before and after the initial approval, to ensure their safety following their deployment. More so than with conventional vehicles, regulation will be required to ensure that automated vehicles continue to comply with road traffic rules and changes in road infrastructure, amongst others[60].

42 This chapter will be separated in two parts related to recommendations for the type-approval proceedings and the initial approval, and for their deployment period (also called "in-service"[61] or "in-use scheme"[62]). A third section related to the amendment of road traffic regulations closes this chapter. An overview of the international, regional (Europe) and national legal frameworks as regards type-approval can be found in Appendix A § 1.

43 For the sake of clarity, the scope of each recommendation is specified in this chapter as follows: automated vehicles encompassing all types of AVs and/or automated minibuses as a subtype of automated vehicles, as well as the respective SAE Level.

[60] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 2.14 p. 9; see also Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.1 et seq p. 91.

[61] Annex 3 to the Commission Implementing Regulation, part 5, p. 62 et seq.

[62] See Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 2.14 p. 9; see also Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.3 p. 91

2.1 Type-approval and initial approval

2.1.1 Creation of a specific vehicle type-approval framework dedicated to automated minibuses

Scope: SAE Level 3 and 4 automated vehicles and minibuses.

Issue: In most Member States and EFTA States like Switzerland and Norway, automated minibuses cannot be approved and registered for regular, commercial operations. Exemption regimes for the approval of new technologies and/or for experimentations exists, but these frameworks do not provide a viable and satisfying solution in the long run for the commercial deployment of automated vehicles and minibuses, as they have (amongst others) to undergo a new and different approval process in each Member State where they are used, with specific requirements in each jurisdiction.

Proposed solution: Creation of a legal framework for the approval and registration of automated minibuses via a procedure in two (or more) successive steps, for instance inspired by the recent French and German frameworks[63].

Explanation: The first suggested step would be to create a legal basis allowing the issuance of a general approval for automated minibuses by an existing type-approval authority that would be binding at a national level (operating permit for the vehicle, e.g. for model X of manufacturer Y). In addition to this first step, a second approval regarding the specific geographical area where the automated minibuses will be deployed would have to be granted by a local authority[64].

The recent European Commission's regulations published in 2022 do not seem to conflict with the creation of such legal frameworks by Member States[65].

---

[63] For Germany, see § 1.3.4 for the latest amendment to the German Road Traffic Act, in particular § 1e (1) *Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, Drucksache 19/27439,* Version of 9 March 2021, p. 7; and for France § 1.3.3, in particular the *Décret no 2021-873 du 29 juin 2021 portant application de l'ordonnance no 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation,* Art. R. 3151-1 et seq.

[64] Verband Deutscher Verkehrsunternehmen e. V., Eckpunkte zum Rechtsrahmen für einen vollautomatisierten und fahrerlosen Level 4 Betrieb im öffentlichen Verkehr, Positionspapier, September 2020, p. 6.

[65] According to Recital 7 of the Commission implementing regulation as regards the type-approval of ADS, "[…] this regulation is without prejudice to the right of Member States to regulate the circulation and the safety of operation of fully automated vehicles in traffic and the safety of operation of those vehicles in local transport services. Member States are not obliged to predefine areas, routes or parking facilities under this regulation. Motor vehicles covered by this Regulation can only operate within the scope of Article 1."; the Delegated Regulation as regards the technical requirements for fully automated vehicles produced in small series of 20 June 2022 also allows Member States to continue to apply alternative approval schemes (see Appendix A § 1.2.3 N 433 below).

2.1.2 Adapted requirements for safety operators inside the automated minibuses

Scope: SAE Level 3 automated minibuses.

Issue: Although automated minibuses require only occasional human intervention when the automated driving system is activated, the qualifications currently expected from safety operators[66] located inside automated minibuses are often as high or even higher than for drivers of conventional public transport vehicles, which generate important functioning costs.

Proposed solution: Adapt the requirements for safety operators to the reality of operating automated minibuses.

Explanation: Most of the current experimental frameworks and approvals for automated minibuses experimentation or deployment requires safety operators (called "on-board operator" in the European legislation[67]) to be located inside the automated minibuses and be ready to intervene, if necessary.

44 This requirement is a consequence of the technological development of automated minibuses, as it is often considered by authorities that these vehicles are currently not developed enough to be able to evolve autonomously and without additional human help/intervention in road traffic.

45 Besides, additional human help/intervention will still remain necessary in the short term to manage unpredictable scenarios, for instance with incorrectly parked cars, accidents etc.

46 The experience gathered during the AVENUE experimentations demonstrated that some of the specific requirements imposed to the safety operators do not increase the levels of safety and rather result from a lack of understanding of automated minibuses and the functioning of automated driving systems. Some requirements were even counterproductive and created new, undesirable safety risks for the safety operator.

47 As an example, it was required from the safety operator to stand up inside the cabin of the automated minibus when the automated driving system was performing the dynamic driving task, in order for safety operator to detect objects under the height of 35 cm from the ground.

48 Experience showed that this requirement created a risk of injury for the safety operator, as he or she might fall down inside the cabin of the vehicle in the case of unexpected braking triggered by the automated driving system. This requirement has not been requested in other jurisdictions of the AVENUE project.

[66] By way of a reminder, various names encompass the function of safety operators, such as safety driver, on-board operator etc. A safety operator is a natural person specifically trained for the operation of automated minibuses, most of the time professional drivers employed by the PTO's, that (amongst others) performs the dynamic driving task (when necessary).

[67] See Art. 2 § 24 Commission implementing regulation of 5 August 2022, C(2022) 5402 final.

49 Therefore, when reviewing applications for experimentations of automated minibuses, type-approval and other authorities should rely on the existing experience gathered from other projects and national level or in other countries.

50 Automated minibuses are specific vehicles, with different attributes than conventional public transport vehicles. Similarly, the skills required from safety operators in automated minibuses are different than the skills endorsed by holders of a minibus driving permit (D or D1 for instance) for public transport. Therefore, holding a driving permit for conventional private cars (motor vehicle of the category B) should be deemed sufficient for safety operators, as it attests of the knowledge of road traffic rules.

51 The key element for safety operators as regards safety consists in the specific and appropriate training performed by the manufacturer of the automated vehicle, that ensures good command of the automated minibus by the safety operator and constitutes the key of ensuring safety and security for the passengers and third parties, as well as its acquaintance with the roads and area where the automated minibus will be deployed.

52 During the drafting of the German Ordinance dedicated to autonomous vehicles that took place between 2021 and 2022, it was first required that the "*technische Aufsicht*" (i.e. the remote supervisor/the person performing the remote intervention, see Appendix A § 1.3.4.2.1 below) would hold an engineering degree or equivalent. This has been strongly disputed by stakeholders, as it would increase importantly the running costs without providing demonstrated safety benefit. This requirement was alleviated in May 2022 with the final version of the Ordinance: the "*technische Aufsicht*" only needs to have three years of professional experience in the field of transport or motor vehicles as well as an annual training in the use of automated vehicles[68].

2.1.3 Remote supervision of automated minibuses

Scope: SAE Level 4 automated minibuses.

Issue: Having a safety operator located inside each automated minibus generates important functioning costs and does not constitute an economically viable solution in the long run for commercial deployment[69].

Proposed solution: Promote further researches and allow automated minibuses to be deployed without a safety operator located inside the vehicle, the safety operator being replaced by a (human) remote supervision that monitors several automated minibuses in parallel and intervenes if/when necessary.

Explanation: Remote supervision can have different names and encompass various concepts[70].

53 According to Art. 2 para. 25 Commission implementing regulation as regards the type-approval of ADS, a "remote intervention operator" means, "where applicable to the ADS safety concept, person(s) located

[68] See https://www.roedl.de/themen/kompass-mobilitaet/2022/11/automatisiertes-fahren-afgbv (last consultation 30 August 2022).

[69] See PROBST, Das "selbstfahrende" Auto: entfernte Illusion oder nahe Realität?, Strassenverkehr 1/2021, Dike Verlag AG, 2021, pp. 52-58, § H N 1 p. 58.

[70] Such as "remote assistance", "remote management", "remote operation" etc.

outside the fully automated vehicle who may remotely achieve the tasks of the on-board operator provided it is safe to do so. The remote intervention operator shall not drive the fully automated vehicle and the ADS shall continue to perform the dynamic driving task".

54 As mentioned in this definition, it should not be confused with remote control or remote driving (i.e. performing the dynamic driving task from distance), which does not necessarily imply automation. These cases encompass various situations such as validating the overtaking of an obstacle on the lane for instance.

55 Remote supervision/intervention is allowed by various national legal frameworks in Europe such as France[71], Germany[72], Norway[73], the Netherlands[74] and Sweden[75] under various conditions. Switzerland is also currently revising its road traffic law with provisions allowing remote supervision[76]. In France and Germany, specific legal provisions are dedicated to remote supervision/intervention and France has approved the experimentation of a driverless automated minibus end of 2021. In both countries, remote driving is not part of the tasks performed by the remote supervisor: the automated driving system has to suggest manoeuvres to the (human) remote supervisor and the latter validates the manoeuvres, which materially correspond to the European definition seen above. France has published a detailed order in August 2022, regulating the remote supervisor's qualifications, mandatory training and certification[77].

[71] See Order dated 2 August 2022 as regards authorization of remote supervisors for automated road transport systems and Art. L. 3151-3 Décret no 2021-873 du 29 juin 2021 portant application de l'ordonnance no 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation.

[72] See § 1d (3) Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren vom 12. Juli 2021 (amongst others).

[73] According to HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[74] The driver outside the vehicle must not be more than 6 metres away from the vehicle and the vehicle speed is limited to a maximum of 10 km/h; see Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 11.

[75] Art. 7 Ordinance 2017:309; see AXHAMN, Look out – Self-driving vehicles are around the corner!, in P. Wahlgren (Ed.), 50 years of law and IT: the Swedish Law and Informatics Research Institute: 1968-2018, Scandinavian Studies in Law; Vol. 65, Stockholm 2018, § 3.2 p. 373 and Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 17.

[76] See Art. 25c Draft Road Traffic Law (FF 2021 3027 et seq.).

[77] See Titles II to V of the Order dated 2 August 2022 as regards authorization of remote supervisors for automated road transport systems, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046151685 (last consultation 31 August 2022).

56 Both frameworks in France[78] and Germany[79] require from the remote operator to hold a valid driver's permit corresponding to the category of vehicle for which remote operation will take place. Due to the fact that it is complicated to recruit suitable candidates for remote operation and that such requirement does not seem to provide evident safety benefits (the same issue applies for safety operators, as mentioned above, see N 46 et seq.), this requirement should be abandoned in order for automated minibuses to reach market scale up. Holding a driver's permit for a conventional private cars (type B) should be deemed sufficient, the specific training representing the key element.

57 During the discussions at European level, it was suggested that the training for remote supervision/intervention should be regulated at national level[80].

58 It was not possible to proceed to experimentations with the safety operator outside the automated minibuses during AVENUE, but this will be the objective of upcoming projects. At international level, driverless robotaxis with remote supervision are currently deployed in the United States (see Appendix A § 1.3.14.3 below).

59 Remote supervision/intervention raises many important questions that should be explored in further details, related to modalities of remote supervision (the number of automated minibuses to be supervised in parallel by one natural person, the training of the natural person performing the remote supervision, the image and data to provide for optimal decision-making etc.), the role and location of intervention teams (field assistants), the communication with passengers and third parties located outside the automated vehicle etc. Exploring and answering these questions are of paramount importance for the large scale deployment of automated minibuses in the future.

2.1.4 Define passive safety requirements for automated minibuses

Scope: SAE Level 3 and 4 automated minibuses.

Issue: The new vehicle architecture of automated minibuses such as those deployed in AVENUE does not match any existing passive safety regulation and the existing regulations for conventional cars, minibuses and buses are severe and inadequate to these new vehicles.

Proposed solution: Define urgently and carefully the passive safety requirements in order to be able to certify this type of vehicle.

---

[78] See Art. 6 Arrêté du 2 août 2022 portant application de l'article R. 3152-3 du code des transports relatif à l'habilitation des intervenants à distance dans le cadre des systèmes de transport routier automatisé "[…] *l'accès aux formations est conditionné à la présentation à l'organisme de formation d'un permis de conduire en cours de validité correspondant à chaque catégorie de véhicule faisant l'objet d'une mission d'intervention à distance* […]"

[79] See § 14 para. 1 (3) AFGBV "[…] *einen gültigen Führerschein besitzt, wobei die Klasse der Fahrerlaubnis der des Kraftfahrzeugs mit autonomer Fahrfunktion entsprechen muss* […]".

[80] See Draft Summary Report of the 6th meeting of the Subgroup of the Motor Vehicles Working Group on "Automated an connected vehicles", Grow I.2, 7 June 2021, § 3a p. 4 https://circabc.europa.eu/sd/a/ef3207fd-0535-42d6-aebb-d869c35c3a04/Draft%20summary%20report%20MVWG-ACV%20of%2007.06.2021%20final.pdf (last consultation 30 August 2022).

Explanation: As of today, automation of terrestrial vehicles has taken two forms:

- automation "kits" implemented on conventional vehicles ("retrofitting"), such as private individual cars that usually fulfil passive safety requirements without automation kits, or
- new type of vehicles, like automated minibuses, pods, AV's dedicated to the delivery of goods etc. with particular architecture, due amongst others to specificities stemming from automation such as the absence of a steering column, no driver's seat etc.

60 Automated minibuses belong to the second category of vehicles with particular architecture.

61 Because of their low cruise speed and the limited routes they can drive on, where the encountered vehicles, vulnerable road users ("**VRU's**") and most of the safety hazards can be identified, it should be studied and decided if the crash test requirements for automated minibuses can be lower than conventional cars. The regulation should be realistic (i.e. feasible) but also stable (i.e. sufficiently demanding).

62 In terms of feasibility, for small series such as automated minibuses, crash tests do not seem appropriate: instead, some kind of self-certification, based on self-certified digital simulations and to be provided to type-approval authorities, should be allowed.

63 The European Implementing regulation as regards the type-approval of ADS mentions an indicative target of 10^{-7} fatality/hour[81]. This indicative target is the same as the (conventional) automotive target, coming from the same ISO norm, e.g. ISO 26262 on functional safety for road vehicles.

64 With 10 km/h as average speed, that means 10^{-10} fatality/km, which is much lower than the road safety state of the art: in the best countries, it is now close to 10^{-8} fatality/km, benefiting from decades of active safety effort (#10^{-4} accident/km) and passive safety effort (#10^{-4} fatality/accident). Fifty years ago, this state of the art was 10^{-6} fatality/km, which means that the same magnitude of improvement has to be obtained in some years (from 10^{-8} to 10^{-10} fatality/km, after 50 years to reach 10^{-8} from 10^{-6}). When increasing the average speed to 20 km/h, the target is lower ($0{,}5.10^{-10}$ fatality/km) and the injury risks are higher.

65 This target is clearly not feasible without passive safety requirements, at same level than for the car industry, structuring for vehicle architecture, but adapted to the specific usage of automated minibuses, such as:

- A front face design, to limit injuries to pedestrians or cyclists.

  This is fundamental when speaking about public transportation in the streets. The front face of automated minibuses will have to be vertical to optimise the ratio between space and length, critical for urban vehicles.

- A structure design, to protect the battery pack in case of a frontal accident.

[81] See Annex II European Implementing regulation as regards the type-approval of ADS, footnote 1 (ad Art. 7.1.1) p. 10.

Lithium-Ion technology can be dangerous in case of crash, as mechanical impacts can initiate fire with toxic gas emanations. Generally, such battery pack is placed under the passenger cabin, which hampers low floor construction of automated minibuses and requires expensive ramps for passengers with reduced mobility. Therefore, it is highly recommended to place the battery pack on top of the automated minibus for improved accessibility (as it is common practice with conventional electrical busses). This position seems to be even more protective for passengers in case of an fire and evacuation.

- Lateral structure, to protect passengers from a vehicle intrusion.

  This constraint is problematic, as such accidents can occur in a city centre, without any solution to avoid the accident from the automated minibus perspective. The vehicle intrusion can use the door side, which will be difficult to protect.

- Cockpit design, to protect passengers (eventually standing inside the automated minibus and not protected by a safety belt) from projections in case of harsh braking (see also above N 47).

  Harsh braking or accident avoidance can injure passengers, creating a risk which does not exist in conventional cars (with seated and belted passengers), as passengers might be standing inside an automated minibus.

66 In terms of vehicle development, even in terms of business feasibility, the passive safety regulation is more urgent than the active safety regulation, but not yet in visibility.

67 The experimentation of vehicles will have to be redesigned to satisfy such requirements, which is a process that is long to develop, and might penalise the service introduction. The needs are specific with high impact to vehicle architecture: many compromises are necessary, leading to risk analysis', computer simulations and huge work to be accomplished. This task has not really started yet and is urgent, as its impact on vehicle architecture is fundamental.

68 In the future, travelling at higher speeds than today, with a vertical front face to optimise the passenger capacity, these urban and costly vehicles will justify the development of dynamic systems to limit the pedestrian injury risk, using three functions:

- Getting the right cinematic against the vehicle;
- Absorbing the impact energy, for example with an "airbag";
- Maintaining the pedestrian by braking control or other means.

69 Questions such as (i) how to protect vulnerable road users and pedestrians and (ii) how to protect passengers in case of harsh braking or collision have to be answered.

70 Regarding vulnerable road users and pedestrians, the level of safety should be the same than conventional vehicles. For passengers, the use case scenario will play a determining role, and trade-offs will be necessary, as low operational speed (i.e. below 30 km/h) and usage restricted to urban areas might lower the impact speed and energy, which is not the case for higher speeds (i.e. above 50 km/h).

71 The AVENUE 2020 project has demonstrated the importance of accessibility for persons with reduced mobility and autonomy, which are directly linked to vehicle architecture and weight. There are also two different needs, which can be satisfied by different automated minibuses:

- Liaison between suburbs and cities, at higher speed and braking capacity on protected lanes, with passengers seated and belted.
- City usage at low speed with braking limitations, easy accessibility amongst pedestrians and vulnerable street users.

72 In their fourth report published on 26 January 2022, the Law Commissions of the United Kingdom and Scotland have recommended the creation of a new legal act that would "require the Secretary of State for Transport to publish a safety standard against which the safety of automated driving can be measured"[82]. The same report also highlights that an independent collision investigation unit should be given responsibility for investigating serious, complex and high-profile collisions involving automated vehicles[83].

2.1.5 Accessibility impact assessment

Scope: SAE Level 3 to 5 automated vehicles.

Issue: There are several ways in which automated vehicles could have an unequal impact on the basis of protected characteristics, both for their own passengers and for other road users. Overall safety benefits should not be at the expense of increasing risks for vulnerable groups such as persons with disabilities and persons with reduced mobility[84].

Proposed solution: The applicant for approval of automated vehicles should be required to submit an accessibility impact assessment[85].

Explanation: Such accessibility impact assessment should show how the applicant or the manufacturer, the software developer or any entity in charge has taken account of the needs of vehicle users and others using the road to ensure that persons with disabilities and persons with reduced mobility are not treated unequally[86].

73 It has also been suggested to establish an accessibility advisory panel in the approval process in order to advise on granting approvals and assist in the development of national minimum accessibility standards

[82] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 2.14 p. 9; see also Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 2.52 et seq. p. 23.

[83] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.149 p. 117 et seq.

[84] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 5.74 p. 82.

[85] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 5.74 p. 82.

[86] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 5.74 p. 82.

for passenger services involving automated minibuses. This panel should include members of the public transport authorities and operators, representatives for disabled and older persons, vehicle manufacturers and representatives from the industry[87].

2.1.6 Benevolent and proactive approach to the experimentation of automated minibuses

74 The following sections will focus on the short term with the desirable and required approach and framework conditions for experimenting automated minibuses in order to optimise their large scale deployment and encourage innovation. Amongst other benefits, experimentations will allow to understand the best use of automated minibuses in the mobility eco-system and how to integrate them efficiently into the public transport offer.

2.1.6.1 Creation of appropriate framework conditions

Scope: SAE Level 3 and 4 automated minibuses.

Issue: Depending on the jurisdiction, experience has shown that obtaining authorisations for experimentations with automated vehicles and minibuses proves to be burdensome, time consuming and costly for applicants.

Proposed solution: At legislative level, enact experimental regulations and regulatory sandboxes. At (executive) governmental/administrative level, encourage the type-approval and other involved authorities to adopt a liberal and enabling approach when reviewing requests for experimentation[88].

Explanation: In its Sustainable and Smart Mobility Strategy, the European Commission has already acknowledged that start-ups and technology developers need an agile regulatory framework to pilot and deploy their products[89].

75 Until the market ramp-up of automated vehicles and minibuses, Member States of the European Union, Switzerland and the other EFTA members should create and develop specific experimental regulations and regulatory "sandboxes"[90]. They should include a centralized experimentation approval or a unified approval process at national level for vehicles and experimental vehicles (such as automated minibuses)

[87] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 10.62 p. 206.

[88] Verband Deutscher Verkehrsunternehmen e. V., Eckpunkte zum Rechtsrahmen für einen vollautomatisierten und fahrerlosen Level 4 Betrieb im öffentlichen Verkehr, Positionspapier, September 2020, p. 8.

[89] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 64 p. 13.

[90] Regulatory sandboxes enable in a real-life environment the testing of innovative technologies, products, services or approaches, which are not fully compliant with the existing legal and regulatory framework. They are operated for a limited time and in a limited part of a sector or area. The purpose of regulatory sandboxes is to learn about the opportunities and risks that a particular innovation carries and to develop the right regulatory environment to accommodate it. Experimentation clauses are often the legal basis for regulatory sandboxes (https://www.bmwk.de/Redaktion/EN/Dossier/regulatory-sandboxes.html, last consultation 30 August 2022).

that cannot fulfil all the requirements of the technical catalogue of requirements for conventional vehicles or of existing/upcoming automated vehicle regulations[91]. They might for instance take inspiration of the regulations adopted by the European Commission in June and August 2022 (see Appendix A § 1.2.3 and § 1.2.4).

76 One of the important goals of experimentation is to collect data (i.e. information and experience) and to systematically report in the event of an incident in order to learn from it. Another will be to implement the suggestion of improvements and the feedback collected through experimentation and to consolidate it at European level.

77 Some stakeholders have called for the creation of a European-wide uniform assessment basis for experimentations as a reliable means for their introduction, with clear deadlines and rules for the submission of applications and the handling of queries[92].

78 Over the course of the past decades, the regulation of the transport sector has evolved to become very technically detailed and regulated. With the fast development of automated driving systems, it is not possible to continue with such regulatory processes, because the existing technical requirements rapidly create hindrances for future developments and innovation in the field of vehicle automation. Therefore, as mentioned, agile frameworks should be deployed, amongst others for the implementation of the feedback gathered during (upcoming) experimentation and research.

79 Amongst others, AV-legislation dedicated to experimentations should be:

- enabling;
- risk-based; and
- technology neutral[93].

80 **Enabling**: the competent approval authorities (in most jurisdiction the type-approval authorities potentially together with other authorities) should follow an encouraging and benevolent approach promoting experimentation. For instance, once the first approval for the experimentation of automated minibuses has been granted, on a particular demonstration site and for a limited period of time, the renewal (extension) of the experimentation under the same conditions after its expiration should be granted without having to provide the same amount of documentation, to proceed to the same assessments etc. than for the first approval. Only the relevant documentation should be required for renewals and ideally through simplified/accelerated proceedings[94].

[91] Verband Deutscher Verkehrsunternehmen e. V., Eckpunkte zum Rechtsrahmen für einen vollautomatisierten und fahrerlosen Level 4 Betrieb im öffentlichen Verkehr, Positionspapier, September 2020, p. 7.

[92] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 3.1.2 p. 14.

[93] Ministry of Transport and Communications (Finland), Conclusions from the 4th high-level meeting on connected and automated driving, Helsinki, 7 October 2020, p. 8.

[94] PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, § 1.6.1 p. 38.

81 Likewise, modifying the conditions during the experimentations should be allowed without applying for a whole new approval process again, if the modified conditions do not pose particular safety and security concerns.

82 As a general approach, the competent approval authorities should avoid creating unnecessary administrative burdens and, to a certain degree, accept the presence of legal uncertainties. Risk zero is a goal but should not form a prerequisite for experimentations. Some scholars[95] suggest that the regulation of artificial intelligence should apply the "better than human equivalent" principle: according to this approach, certain errors of an AI system should be overlooked, as long as their output is superior to human performance overall.

83 Due to the highly innovative and technological nature of automated minibuses (and AV's in general), the competent approval authorities should not rely and narrowly apply the existing approval framework for regular vehicles driven by human drivers, as it is not adapted to such vehicles. Non-compliance with certain technical and safety requirements (rear view mirrors, blinkers etc.) should be admitted in presence of adequate compensation measures. In addition, it should not be requested from the applicants to produce extensive lists of writing exemptions, as it has been experienced during the AVENUE project.

84 As an example, in a specific jurisdiction, the seat belts' anchor points for passengers of the automated minibuses had to be modified in order to receive the approval for experimentation. The three other jurisdictions did requested similar modifications, which slowed down the approval process and generated additional costs for the applicant in this specific jurisdiction.

85 A possibility to ease the conditions of experimentations would be to allow the competent authorities to rely on OEM's/manufacturers' "self-declarations" as long as certain new technical equipment and/or technologies cannot be assessed under the existing legal framework and standards. This approach has been followed by the German authorities with § 1f para. 3 (4) of the 2021 revised German Road Traffic Act.

86 Another possibility would be to enact national exemption requirements, but this solution might create an important workload on the side of the authorities, although this would have the advantage of promoting AV related knowledge within these authorities (see also Recommendation § 2.1.6.3 below).

87 In order to facilitate the experimentations, the competent authorities should also give high priority to approval requests and assess them swiftly.

88 **Risk-based**: The absence of full scientific certainty shall not be used as a reason for postponing the introduction of AV regulations or to refrain delivering experimental approvals. When regulating the introduction of new road technologies, states should apply a precautionary approach and take account of the relevant scientific evidence, in order to protect road safety, especially where there are threats of fatalities or serious injuries[96].

[95] HACKER, AI Regulation in Europe, 7 May 2020, p. 14 and quoted references.

[96] Automated driving, Draft text for a resolution on "activities other than driving", WP.1 ECE/TRANS/WP.1/2019/3, p. 3 N 6.

89 SAE Level 3 or 4 automated minibuses cruise at low to moderate speeds (≤ 25 to 30 km/h) on predefined routes or areas. Such low speeds imply reduced safety and security concerns (i.e. diminished threat of fatalities or serious injuries) and issues than, for instance, the use case foreseen in UN Regulation 157 for Automated Lane Keeping Systems, namely automated vehicles circulating at speeds up to 60 km/h in traffic jams on highways (and soon to 130 km/h as highway driving assistants).

90 Therefore, as the current use case of automated minibuses does not create major risks of fatalities or serious injuries, the experimentation of automated minibuses should not require heavy approval processes with extensive safety and security assessments, unless reasonable grounds would require such assessments. As of today, many experimentations have been deployed in European Member States by the manufacturers of automated minibuses. Although much progress still can be achieved, many efforts have been made and major steps achieved in order to improve the overall level of safety and security of these automated minibuses, with many issues being identified and risks mitigated.

91 **Technology-neutral**: this principle is explicitly mentioned by the European Commission in its Sustainable and Smart Mobility Strategy[97]. It means that the legal framework should be technology-neutral in order to be able to apply to new and potentially unexpected technologies and to stand the test of time. The framework should also provide clear guidance about what it takes to meet regulatory requirements, by focusing on the outcomes rather than prescribing how these requirements should be achieved[98]. The legislation should set goals, not technologies.

2.1.6.2 Appropriate administrative costs for approval proceedings

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: The administrative fees combined with the necessary indirect costs for obtaining the approval of experimentations can be very high and prevent PTO's and other actors from "entering the market" and proceed to experimentations of automated minibuses (and AVs in general).

Proposed solution: Ensure that the global costs generated by the approval of experimentations are related to the effective costs of the process and do not constitute a disproportionate or excessive burden for the applicant.

Explanation: The experimentations and the deployment of automated minibuses are expensive *per se* and hardly economically viable at the current stage. It is commonly admitted that vehicle automation will result in many positive societal outcomes in the long term, the most important being an increase in road safety.

92 High administrative fees might hinder innovation forces and should be avoided, by ensuring that they do not constitute disproportionate or excessive burden and comply with the principle of cost recovery.

[97] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, § 71 p. 14.

[98] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of responses to consultation Paper 3 and next steps, 2 July 2021, p. 4.

93 This is of particular relevance when third party assessors are involved in the approval process, as their costs can quickly become prohibitive for small or medium sized PTO's, which are precisely the entities that could benefit the most from the deployment of automated minibuses.

94 High administrative fees might also have the effect to favour important stakeholders with "deep pockets" (such as manufacturers of conventional vehicles or tech companies with a global presence) when the European industry building automated vehicles is closer to companies similar to SMEs.

2.1.6.3 Creation of public guidelines and checklists for experimentation

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: Before submitting their application, potential applicants for experimentations of automated minibuses can be confronted to a lack of visibility and information on legal and technical requirements to proceed to experimentations. On the other side, the national and/or local competent type-authorities might also lack of necessary skills and knowledge related to the process of granting *ad hoc* experimentation approvals when requested to do so.

Proposed solution: Create checklists establishing the technical prerequisites that automated vehicles and minibuses must met in order to receive approval, as well as guidelines for applicants defining the authorities (and third party assessors when applicable) that need to be involved within each jurisdiction and their field of competence and tasks.

Explanation: In some European Member States, more than 50 experimentations of automated vehicles have been or are currently deployed. This means that type-approval authorities of these Member States have become accustomed with experimentations of AVs and that the framework conditions should be clear to applicants, authorities and third parties (vehicle manufacturers, independent assessors etc.).

95 But other jurisdictions are not so familiar with these new technologies, and the existing legal framework might even not allow to proceed to experimentations, as it was the case encountered recently during the FABULOS project[99].

96 From a time perspective, experience has also taught that the first approval for an experimentation or of a particular model of automated minibus is often more complex and usually takes longer than the following approvals, once the various involved stakeholders have gained better knowledge of the respective processes and technologies.

97 The creation of guidelines and technical checklists by competent authorities turns out to be useful in both scenarios. For jurisdiction accustomed to experimentations, this process unifies and harmonises the requirements and proceedings, and provide gains in time and in efficiency for all stakeholders. For jurisdictions less accustomed with vehicle automation, this approach helps to anticipates issues and shortfalls, to gather new useful knowledge and to prepare the imminent (and inevitable) changes triggered by the upcoming automation of mobility.

[99] FABULOS H2020, Policy paper, D5.6 – Future application and impact of project results and learnings, 30 March 2021, § 3.6 STCP Porto p. 50 and § 3.6.6 STCP Porto: Legal findings p. 53.

98 All relevant stakeholders such as vehicle manufacturers, PTO's, deployers and local vehicle approval authorities (amongst others) should be involved in the process of creating such guidelines, which also encourages collaboration and common understandings between the different parties. Due to the often international nature of consortiums proceeding to experimentations, a translation in internationally spoken and written languages of this documentation is desirable.

99 For instance, in 2019 the European Commission released guidelines on the exemption procedure for the EU approval of automated vehicles[100]. Annex 1 of the French Order dated 26 May 2021[101] takes form of a questionnaire with questions, answers and details regarding the documentation to be provided by applicants. The Swiss Federal Roads Office has issued and updated a fact sheet for conducting pilot tests in Switzerland[102] in four languages. A "Method admittance procedure" description for connected and automated vehicles is available on the website of the Netherlands Vehicle Authority in Dutch and English[103]. The Swedish Transport Agency has also issued a description of the application process regarding the permit for experimental operation with self-driving vehicles[104]. In the United Kingdom, a non-statutory and non-binding "Code of Practice on automated vehicle trialing" has been issued in 2015 and updated in 2019 respectively 2022[105].

2.1.6.4 Creation of a dedicated European knowledge platform and database related to automated and autonomous vehicles

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: Applicants for experimentations of AVs and type-approval authorities might sometimes lack of knowledge and of the necessary overview on the often complex legal and technical questions and approval requirements related to automated vehicles.

Proposed solution: Create a dedicated platform at European level that identifies, amongst others, the relevant regulations and authorities in charge with automated vehicles in each European Member State, but also research, testing, piloting and deployment activities on automated vehicles and their results. This platform might also serve as orientation for further researches and deployment projects.

---

[100] European Commission, Guidelines on the exemption procedure for the EU approval of automated vehicles, Version 4.1 supported by the Technical Committee on Motor Vehicles of 12 February 2019, published on 5 April 2019.

[101] "Arrêté du 26 mai 2021 modifiant l'arrêté du 17 avril 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques", published at "JORF n° 0143" of 22 June 2021.

[102] Federal Roads Office (Switzerland), Automated driving – fact sheet for conducting pilot tests in Switzerland, Version 3.0, 26 January 2021, available in English, French, German and Italian.

[103] https://www.rdw.nl/over-rdw/information-in-english/about-rdw/connected-automated-vehicle/method-admittance-procedure-its (last consultation 30 August 2022).

[104] https://www.transportstyrelsen.se/globalassets/global/vag/fordon/automatiserade-fordon/description-of-application-process.pdf (last consultation 30 August 2022).

[105] https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling (last consultation 30 August 2022).

Explanation: The conclusions of the 4th High Level Meeting on Connected Automated Driving in October 2020 highlighted the need for more harmonisation to ease the testing of automated vehicles in different countries and to improve learning from the experiences of testing. It recognised the importance of having a central European database collecting relevant information on CCAM research, testing, piloting and deployment activities and its results in Europe and beyond[106].

100 The relevant legal framework for automated and autonomous vehicles is constantly evolving, at international and regional level (UN Regulations, European legislation) as well as at national and subnational levels with numerous Member States revising their legal frameworks in order to enable operations and/or experimentations of these new vehicles.

101 In addition, automated vehicles are subject to many different fields of the law that have not been interoperating until now. This generates complexity for stakeholders to gather an overview on all concerned fields, and harder to proceed with experimentations and/or to enter into the market.

102 The existing Knowledge Base on Connected and Automated Driving[107] seems very fit to play such role.

103 The US National Conference of State Legislatures contains a legislative database on federal and state AV-related bills enacted since 2012, as well as a description of federal and state actions and policies in this field, amongst other resources[108] and might serve as inspiration.

104 In addition, this platform might be used to encourage and leverage national and international exchange of information between national authorities and at European level, by allowing authorities to share and exchange their respective experiences from their national and local experimentations. The above mentioned collaboration of Estonian and Greek authorities during the FABULOS project[109] (see N 95 above) is an example demonstrating that such cooperation needs a communication channel and also a common understanding.

105 This would also make it possible to translate the relevant legislations and guidelines, as language barriers can often hinder processes, with for instance a lack of translation in English of the relevant national legislation.

106 One of the possibilities might be to compel Member States to publish information about the legal status of automated and autonomous driving in their own jurisdiction. The Member States have already engaged themselves to support the Knowledge Base on CAD by providing up-to-date information on ongoing programmes and projects[110].

---

[106] CCAM Strategic Research and Innovation Agenda, European leadership in safe and sustainable road transport through automation, Version 1.3, 1 December 2021, § 3 p. 15.

[107] https://www.connectedautomateddriving.eu (last consultation 30 August 2022).

[108] https://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx (last consultation 30 August 2022).

[109] FABULOS H2020, Policy paper, D5.6 – Future application and impact of project results and learnings, 30 March 2021, § 3.6.6 Lamia pilot: Legal findings, p. 50.

[110] Ministry of Transport and Communications (Finland), Conclusions from the 4th high-level meeting on connected and automated driving, Helsinki, 7 October 2020, p. 8.

107 In addition to the creation of such platform, another important aspect is to keep it regularly updated, as the legal frameworks are going to face important changes in the upcoming years.

2.2 Deployment

2.2.1 Monitoring

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: With changes to road traffic rules, the driving environment, software updates and technological evolution such as advanced algorithms, automated vehicles might require continuous regulatory oversight throughout their lifetime[111].

Proposed solution: Study the relevance of creating an "in-use" safety authority, in charge of ensuring the continuing safety and legal compliance of automated vehicles while they are in-use, by learning from mistakes and preventing their re-occurrence[112].

Explanation: After consultation of stakeholders and reviewing the international and national framework, the Law Commission of England and Wales and the Scottish Law Commissions recommended the creation of an "in-use safety regulator". This new authority should be in charge of evaluating the safety of automated vehicles (in comparison with conventional vehicles), of investigating breaches of road traffic rules committed by automated vehicles and of ensuring that vehicle manufacturers, tech companies and deployers of automated vehicles provide information to users in a clear and efficient way[113].

108 The existing type-approval authority might also be granted these tasks, as well as the existing authorities in charge of market surveillance and vehicle recalls[114], although such constellations might also raise questions related to conflicts of interest that should be studied and arbitrated.

109 One of the crucial points will be to investigate and develop methods to audit algorithms. Although acknowledged and addressed in other areas, the algorithmic bases for AV systems and operations evoke unique variables that alone or combined give rise to a number of specific concerns regarding black-boxed processes and biased outcomes. Algorithm-based operations can produce false correlations, assumptions and deductions, resulting in biased associations to certain objects or areas around the vehicle[115].

---

[111] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 3.19 p. 14.

[112] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 3.20 p. 14.

[113] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 3.20 p. 14.

[114] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 3.22 p. 15.

[115] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 45.

110 It has also been suggested that policymakers could establish independent bodies that include representatives of consumer or user organisations to systematically conduct audits on specific algorithmic applications in automated vehicles operation and use. The findings should be used in part to directly monitor and correct wrongful or unwanted designs and operations, and in part for the development of long-term standards and good practice recommendations to be communicated to vehicle manufacturers, deployers and PTO's[116].

2.2.2 Software updates

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: Automated vehicles and minibuses will most likely receive software updates with updates and/or upgrades in between the periodic inspections. These software updates have to be monitored by the type-approval (or another) authority, due to the fact that they are or might become safety relevant.

Proposed solutions: Establish harmonised rules and technical requirements so that the software updates proposed by vehicle manufacturers can be authorised by the Member States in accordance with a common European methodology. This implies, amongst others, the following:

- Concepts must be developed that can identify manipulation attempts and carry out automated integrity checks. This is necessary along the functional life and value chain, from production and operation/deployment to maintenance and repair (for example software updates, replacement of individual components in a workshop etc.);
- The communication requirements between the vehicle and the testing device should be standardized and laid down in the relevant European (or international) type-approval regulations;
- Approval authorities or third parties in charge of the periodic inspection need to have access to the vehicle electronics via standardised vehicle interfaces (on-board diagnostics, over-the-air and others) in order to fulfil their legal task (see also Recommendation § 6.1 below);
- With regard to the Software Update Management System ("**SUMS**"), in addition to a uniform interpretation and application, the qualification of the experts processing the periodic inspection must be ensured in order for them to be able to adequately audit the software update management processes[117].

Explanation: First, a distinction between software updates and upgrades needs to be made. Software updates serve to maintain functionality and are intended to close newly identified security gaps, so that the device can continue to be used as before without any functional restrictions and free of cyberattacks. Upgrades are improvements that go beyond maintaining the function and provide new functionalities and/or greater convenience when using products with digital content[118].

---

[116] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 45.

[117] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 3.3.2.1 p. 19.

[118] See https://www.boks-international.com/austria-the-pitfalls-of-software-updates-in-networked-cars/ (last consultation 30 August 2022).

111 The recent UN Regulation 156 on uniform provisions concerning the approval of vehicles with regards to software update and software update management system[119] requires vehicle manufacturers to have a clear system to assess and record software updates. It enables the identification of the software version used in the vehicle by means of the software identification number ("RxSWIN") and to ensure the update process in the vehicle through procedural specifications[120].

112 Once approved, a new software version may be implemented in vehicles produced from this date. In order to also upgrade vehicles already in circulation with the newer software version, this upgrade must be applied for in advance with the type-approval authority. However, the validity of such an approval is limited nationally; an update of the vehicles in other European or international countries must be applied for individually in the respective countries with reference to the national approval[121].

113 However, the way this will work in practice is unclear. Furthermore, there are no specific provisions to require vehicle manufacturers to issue updates when laws and circumstances change[122].

114 Harmonised rules and technical requirements should be issued, so that the software modifications proposed by vehicle manufacturers can be authorised by the various Member States in accordance with a common European methodology which should, in particular, make it possible not only to ensure that the modification of the software does not call into question the initial type-approval of the vehicle, but also to give a harmonised opinion on the addition (or blocking) of functionalities which were not included in the scope of the initial type-approval[123].

115 It has to be highlighted that the vehicle owner, which will often be a public transport operator in the case of automated minibuses, has no influence on the vehicle manufacturers' or the software developers' programming and the software updates/upgrades. Therefore, the PTO respectively the owner of automated minibuses should not be burdened with having to apply for a new approval after every software update, neither have a duty to report software updates to authorities[124], due to the fact that software updates will be initiated by the manufacturer and/or the software developer, and not by the PTO/the owner of the vehicle[125].

---

[119] UN Regulation No. 156 on uniform provisions concerning the approval of vehicles with regards to software update and software update management system, ECE/TRANS/WP.29/2020/80, 31 March 2020.

[120] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 3.3 p. 18.

[121] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 3.3 p. 18.

[122] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 10.22 p. 157 and quoted references.

[123] PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, § 1.4 p. 27.

[124] Such as, for instance, amended Art. 11bis Real Decreto Legislativo 6/2015 in Spain for instance.

[125] Rödl & Partner, Innovationspapier zur automatisierten und fahrerlosen Personenbeförderung, erstellt im Auftrag des Verband Deutscher Verkehrsunternehmen e. V., Hamburg/Nürnberg, March 2021, § 2.10 p. 11.

2.2.3 Mitigation of cybersecurity risks

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: The interconnection of different CAV components and communication channels increases the potential attack surfaces and the increase in level of automation leads to an exponential increase in cybersecurity risks.

Proposed measures:

- Type-approval authorities should have responsibility for developing and encouraging best practices with regards to ongoing cybersecurity of connected and automated vehicles. Where a lack of (cyber)security gives rise to a safety concern, the regulator's powers to deal with safety concerns should apply[126]. Depending on the situation, in presence of cybersecurity issues, it should be possible to withdraw a permit to bring automated vehicles onto the market[127] or to proceed to experimentations.
- Breach notifications (reporting duties), including a description of incidents, anticipated impacts and mitigation measures should be communicated to the type-approval authorities, the data protection authorities and/or other specific authority and to the affected data subjects[128], in a similar way than Art. 32 and 33 GDPR or than the revised NIS Directive[129].
- For a meaningful cybersecurity audit, acceptance and evaluation criteria must be defined, on the basis of which a review (Cyber Security Management System audit and inspection of the vehicle type with regard to a software and architecture type) can take place.
- Cybersecurity audits are challenging given the constant evolution of technology. Industry, inspection organisations and authorities should work together to explore certification options.
- The mutual recognition of Cyber Security Management System certificates shall be regulated[130].

116 The following cybersecurity related principles, that should be followed and implemented in the legislation, have been suggested recently in the legal literature:

- Unauthorised access to the vehicle's systems should be prevented.
- In case of unauthorised access, damage should be limited by technical means as much as possible.
- In case of unauthorised access, the state of cybersecurity should be restored.
- Injured parties should be indemnified.
- Those exploiting a cybersecurity vulnerability should be held responsible for their actions under both criminal and administrative law.

---

[126] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.165 p. 120.

[127] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 4.

[128] European Parliamentary Research Service (EPRS), The NIS2 Directive – A high common level of cybersecurity in the EU, PE 689.333, December 2021, p. 7.

[129] According to the revised NIS Directive, affected companies have 24 hours from when they first become aware of an incident to submit an initial report, followed by a final report no later than one month later.

[130] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 5.1.2 p. 22.

- The state of cybersecurity should be preserved throughout a vehicle's lifetime[131].

Explanation: Cybersecurity can be described as all activities that are necessary to protect network and information systems, their users and affected persons from cyber threats. A cyber threat is any circumstance/event that is capable of damaging the network and information systems, users or the persons affected by them[132] (for other definitions, see Appendix A § 5.1).

117 In order to apply data protection by design and by default (see Art. 25 GDPR and Appendix A § 4.2.7), organizations should first develop a comprehensive risk assessment, where the intended activity is mapped out from the personal data perspective. Subsequently, they should map the necessary technical and organizational security measures that would mitigate any high risks posed towards the rights and freedoms of data subjects[133]. Additionally, according to the principle of integrity and confidentiality (see Art. 5 para. 1 litt. f GDPR and Appendix A § 4.2.6.6), personal data must be processed in a manner that ensures appropriate security of the personal data, including the protection against unauthorised or unlawful and against accidental loss, destruction or damage, using appropriate technical or organisational measures[134].

118 A brief overview of the international and national legal frameworks related to (vehicle related) cybersecurity is provided in Appendix A § 5.

[131] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 3.

[132] See WIDMER, Wie sicher ist sicher genug? Sicht Datenschutz- und Cybersicherheit, Zulassungsrechtliche Herausforderungen des Autonomen Fahrens, Universität Basel, Tagung vom 10. Oktober 2019, slide 13.

[133] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.2 p. 6 and the quoted references and § 3 p. 11.

[134] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020,.

2.3 Road traffic regulations

2.3.1 Amendments to existing road traffic rules

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: During many decades, the presence of a human driver performing the dynamic driving task from inside the vehicle was a central assumption, respectively a postulate governing international road traffic conventions, as well as national road traffic laws. A fundamental paradigm change is currently operating and states should "absolutely depart from the 20th century approach to driving"[135].

Proposed solution: Proceed to an extensive assessment and prepare to amend (i) legal or technical provisions implicitly or explicitly involving the presence of a human driver inside the vehicle, as well (ii) as legal or technical provisions that might pose interpretation problems with the introduction of automated vehicles or (iii) legal or technical provisions involving human negotiation, interpretation or communication in specific situations.

Explanation: Many existing road traffic provisions contain obligations and injunctions addressed towards the human driver of a motor vehicle or imply situations requiring human interpretation and comprehension. They will need to be amended with the introduction of automated vehicles and minibuses, both at international and national levels.

119 As an example of the existing "driver-centric" approach of the existing regulations, the word driver appears over 140 times in the 56 articles of the Vienna Convention[136]. Art. 7 para. 3 Vienna Convention provides that "Drivers shall show **extra care** in relation to the most vulnerable road-users […]" and Art. 11 para. 4 that "When overtaking, a driver shall give the road-user overtaken **a sufficiently wide** berth […]" (emphasis added; see also Appendix A N 1.1.3.3 et seq.). Programming automated driving system in order to comply with such provisions will prove difficult.

120 Other examples of problematic situations have already been identified by dedicated workgroups, such as:

- priorities to the right at unmarked road intersections;
- right of way and indicator use in roundabouts;
- turning at intersections;
- emergency lanes on highways opened to the traffic only during specific peak hours;
- electronic speed limits or information displayed on screens etc.[137]

[135] SMITH, On remote driving, Blog post dated 16 May 2022, retrieved under https://cyberlaw.stanford.edu/blog/2022/05/remote-driving (last consultation 30 August 2022).

[136] VELLINGA, Automated driving and its challenges to international traffic law: which way to go?; *Law, Innovation and Technology, 11(2)*, 2019, § 1 p. 258.

[137] See https://circabc.europa.eu/ui/group/4273d650-b8a9-4093-ac03-18854fbba4b5/library/e00587b2-c129-4f6b-859c-db3ffe9a0d76/details, MVWG - Working Group on Motor Vehicles, 143rd meeting on 13 November 2020, file "04. Examples of complex or unclear traffic rules and infrastructure in Europe" (last consultation 30 August 2022).

121 This issue should be addressed at international[138], regional (i.e. European) and national levels and coordination will be of utmost importance, in order to avoid creating domestic rules that apply in one State but are unknown in another (in particular in fields such as interactions of vulnerable road users with AV's and responsibilities for individual users of AV's[139]).

122 At UNECE level, it has been suggested that the main focus shall lie with making the existing UN Regulations work for automated vehicles rather than introduce new concepts. In addition, it has been suggested to follow this procedure for each UN Regulation individually and to assess if:

- an amendment of each Regulation is possible, in order to make it apply to automated vehicles; or
- if a new Regulation should be created, based on the existing Regulation, but with major amendments; or
- a new Regulation should be created, covering more than one existing Regulation on a specific topic[140].

2.3.2 Definition of behavioural rules in case of trade-offs

Scope: SAE Level 3 to 5 automated vehicles and minibuses.

Issue: Automated vehicles are programmed in order to comply strictly with the existing traffic rules. In road traffic, however, situations occur that require a trade-off between obstructing the traffic flow and infringing road traffic rules[141].

Proposed solution: Solutions to such problematic situations requiring trade-offs and arbitrations should be discussed with the various concerned authorities (such as road safety, police, traffic law, politicians etc.), the developers of automated vehicles and researchers[142].

Explanation: The strict compliance of automated vehicles with road traffic rules provides a valuable contribution to road safety. On the road, however, situations occur that imply a trade-off between obstructing the traffic flow and infringing road traffic rules. In these cases, human drivers compare unavoidable risks and make appropriate decisions to disregard one traffic rule in order to comply with another[143].

---

[138] For instance at UNECE level, where a "Group of Experts on drafting a new legal instrument on the use of automated vehicles in traffic", amongst other working groups, has been established recently, see Appendix A § 1.1.5.5.

[139] See UNECE's Informal document No. 2 (GE.3-03-02), Initial thoughts on "road safety challenges posed by the use of automated vehicles in traffic that an international legal instrument could adequately address", Submitted by Professor Bryant Walker Smith, § 30 et seq. p. 5.

[140] Informal document GRVA-13-18, "Vision of an ADS road map and related future activities at UNECE/GRVA", Submitted by the experts from CLEPA and OICA, 13th GRVA, 23 - 27 May 2022, Provisional agenda item 4(f), pp. 4-5 https://unece.org/sites/default/files/2022-05/GRVA-13-18e.pdf (last consultation 30 August 2022).

[141] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.2 p. 10.

[142] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.2 p. 10.

[143] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.2 p. 10.

123 One example is the necessity of crossing a continuous line in order to circumvent an obstacle located on the lane. In this case, after weighing up all the risks, the circumvention is only possible if a traffic rule is disregarded in order to achieve a higher-value goal (for example, clearing a section of road for the preceding traffic)[144].

124 Another example: when an emergency vehicle is approaching with blue lights and sirens, an automated vehicle might only clear the lane by crossing a continuous line, the stop line of a red light or pulling onto the pedestrian walkway or cyclist lane[145].

3 Recommendations related to accessibility

Introduction

125 Automated vehicles and minibuses have a high potential to improve the mobility of persons with reduced mobility, including persons with disabilities and seniors ("**PRM**").

126 PRMs have reduced sensory (seeing, hearing, feeling), motoric (moving, grasping, handling, strength) or cognitive (recognition, thinking, decision to act) abilities. Automated minibuses and their related services shall be barrier-free if they are detectable, reachable, usable and reliable for persons with disabilities of all ages in the usual way, without particular difficulties and, as a rule, without help from others. The use of assistive technologies (e.g. walking frames, white canes, mobility applications on smart phones etc.) should be allowed.

127 The accessibility of automated minibuses covers following aspects:

- The physical and sensory accessibility of the vehicle (boarding, unboarding), operation of vehicle elements (buttons, door, seats/belts, emergency call) and the perceivability of provided information (visual, acoustic);
- The accessibility of related digital services (e.g. for booking, payment and management of the transport service);
- Protection of PRMs in and outside automated vehicles.

128 It should be noted that the accessibility needs of PRMs are in principle the same as for conventional, non-automated vehicles. But the reliability of the accessibility support needs to be massively higher, as the fallback personal assistance granted by the human driver of conventional vehicles (or the safety operator)

[144] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.2 p. 10.

[145] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.2 p. 10.

will not always be available, and in some situations no other passengers will be present in the automated minibus to provide assistance. These aspects are most important in emergency situations.

129 An overview of some specific legal frameworks as regards accessibility is provided in Appendix A § 2.

3.1 Improving accessibility standards for automated public transport

Issue: In the field of automated minibuses, the applicable accessibly requirements seem to be widely ignored by vehicle manufacturers, as demonstrated by the current vehicle constructions. Moreover, the mobile applications related to the services provided by automated minibuses services lack accessibility.

Proposed solutions:

- Deployers of automated minibuses and public transport authorities should include accessibility as an important criterion in the procurement process. In many countries accessibility is a prerequisite for refunding vehicles by public authorities.
- Vehicles manufacturers shall apply accessibility requirements from European standards in the earliest construction phase of vehicles ("accessibility by design" in a similar way than "privacy by design and by default" for data privacy). For example, an ultra-low floor automated minibus requires placing the batteries not under the floor but elsewhere. A low floor minibus would be a single selling point, while complying with regulation, user needs and saving live time cost by avoiding extra services and equipment.
- Vehicle manufacturers and deployers of automated minibuses should apply the process standard EN 17161 for reasonable accommodation of persons with disabilities when designing, manufacturing, operating and maintaining automated minibuses.
- As of August 2022, many European accessibility standards are currently being revised and this should be leveraged.
- National accessibility requirements in national standards or regulation for public transport should be avoided or replaced, especially for automated vehicles, by international or regional (European) provisions.

Explanation: The emerging trends of automation and digitalization will have a strong impact on the accessibility of public transport systems. European norms[146] are an effective method to create a common European understanding of the accessibility needs of PRMs by providing functional accessibility requirements. This approach prevents from diverse national standards, which create market fragmentation, which is a disadvantage for vehicle manufacturers, service providers and passengers with reduced mobility.

130 Many European accessibility standards are currently under revision (see Appendix A § 2.2.10) and this momentum should be seized to adapt them to automated vehicles and minibuses. One driver for upcoming improvements in the next three years is the European Commission's Standardization Request

[146] A list of accessibility standards also (partially) applicable to automated minibuses is listed in Appendix A § 2.2.10. This list includes also standards on ICT accessibility, because of the digitalization of public transport.

("**SR**") to the European standardisation organisations[147], as it requests new and amendments of existing standards for the support of the European Accessibility Act. This SR was finalized by the European Commission in July 2022. If the European standardisation organizations[148] accept the SR, the new standardisation work will start in October 2022.

131 Amongst others, this Standardization Request will have major impact on digital services, including public transport services, according to Art. 2 para. 2 litt. c European Accessibility Act (see Appendix A § 2.2.8).

132 The specific user accessibility needs and functional accessibility requirements of PRMs for automated vehicles in public transport should be incorporated when revising relevant standards. A very prominent candidate is the revision of the Regulation 1300/2014 "TSI PRM" (see Appendix A § 2.2.4)[149]

3.2 Legislation on accessibility

Issue: There is a need for standardised and enforceable European legislation across the mobility chain, as no such dedicated legislation exists for multimodal transport, be it for long-distance or local transport. The sectorial legislation on air, maritime, railway and road transport does not fulfil this goal as they:

- allow for exceptions that were used by Member States, at least for a transitional phase;
- focus on long-distance transport;
- do not support a wide range of the actual requirements of people with reduced mobility, such as:
  - the possibilities of spontaneous travel (i.e. duty of prior notification of assistance requirements, see Appendix A N 589 and N 593 below);
  - inadequate support during travel and compensation for loss or damage of accessibility equipment (cases of denial of travel and limited lost property compensations), etc.[150].

Proposed solutions:

- Harmonise the concepts of persons "with disabilities" and "with reduced mobility";
- Extend the applicability of Regulation 181/2011 on coach and bus passenger rights to local and urban transport (i.e. remove the scope of application to bus travels in distances over 250 km, see Appendix A § 2.2.6);

---

[147] https://www.edf-feph.org/edf-welcomes-the-european-commissions-draft-standardisation-request-in-support-of-the-european-accessibility-act/ (last consultation 30 August 2022); see also https://single-market-economy.ec.europa.eu/system/files/2021-11/Draft%20standardisation%20request%20to%20the%20European%20standardisation%20organisations%20as%20regards%20harmonised%20standards%20in%20support%20of%20Directive%20%28EU%29%202019_882.pdf (last consultation 30 August 2022).

[148] Namely the European Committee for Standardisation ("CEN"), the European Committee for Coordination of Electrical Standardisation ("CENELEC") and the European Telecommunications Standards Institute ("ETSI").

[149] See Commission Regulation (EU) No 1300/2014 of 18 November 2014 on the technical specifications for interoperability relating to accessibility of the Union's rail system for persons with disabilities and persons with reduced mobility (TSI PRM), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1300&from=DE (last consultation 30 August 2022)

[150] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 33 and references.

- Regulate and enforce the role of National Enforcement Bodies ("**NEB**"), to be able to impose compliance with European and national accessibility regulations on transport operators;
- Connect European and national accessibility regulations to national and local transport equipment, infrastructure and service procurement schemes;
- Extend assistance to PRMs to include real time and spontaneous travel requirements for all modes and main stations;
- Develop a National Transport Accessibility Strategy with the active involvement of transport operators and PRM associations, aimed at a modular and stepwise enhancement of public transport inclusiveness for all PRM groups and transport modes;
- Include transport accessibility in cities' Sustainable Urban Management Plans, linked to specific KPIs and monitoring processes[151];
- As regards the current proposal of the TEN-T Regulation[152] (see Appendix A § 2.2.9), it should include:
    - Accessibility requirements for automated vehicles and minibuses, including the related digital services;
    - Accessibility requirements for integrating automated minibuses in the travel chain of public transport;
    - References to relevant European accessibility laws, such as the TSI-PRM or the European Accessibility Act (see Appendix A § 2.2.4 and Appendix A § 2.2.9).
    - Accessibility requirements for automated vehicles which use the TEN-T infrastructure;
- And, as a general principle, prevent discriminatory service provision[153].

3.3 Development and research

Issue: The emerging trends of automation and electrification will affect transport system accessibility either positively or negatively and this has not yet been properly researched.

Proposed solutions:

- Accessibility of future automated public transport of all types needs to be thoroughly researched and design guidelines issued on public transport accessibility levels;
- PRMs need to become C-ITS nodes in order for emerging automated vehicles to recognise and protect them, given their potentially lower conspicuity and higher vulnerability;
- The impact of each new technology on PRM accessibility must be assessed during its design phase and appropriate adaptability/personalisation means and strategies should be supported[154];

[151] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 34.

[152] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A812%3AFIN (last consultation 24 August 2022).

[153] See Recommendation 11, Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.3 p. 42 et seq.

[154] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 40.

- Ongoing and upcoming experimentations should aim to improve the understanding of accessibility issues and approving experimentations might include requirements to proceed to researches dedicated to accessibility.

Explanation: It is important to consider the different needs resulting from various disability types. The use of automated vehicles without vision, impaired vision, without colour perception, without hearing, impaired hearing, without speech capability, with limited handling or strength, with limited reach or with cognitive impairment needs to be analysed, as well as the respective assistive aids.

133 Guidance on co-creation with disabled or older people has been developed in the European R&D Horizon 2020 project LIV_IN[155].

134 Information on user accessibility needs is available at ISO/IEC 29138-1 and ergonomic data on persons with disabilities and older persons are available at ISO TR22411:2021.

4 Recommendations related to public transportation

4.1 Create a flexible and innovative public transport framework for automated minibuses

Issue: The current legal framework for public transport (with fixed bus stops, fixed lines/itineraries, fixed schedules etc.) is often hardly compatible with innovations such as Transport-on-Demand ("**ToD**") and Mobility-as-a-Service ("**MaaS**"). This creates legal uncertainty and may lead to fragmentation, distortions of competition and loss of economic welfare[156] in the long term.

Proposed solution: Establish a flexible public transport framework allowing on-demand services operated with automated minibuses in specific areas (and not subject to line-based traffic, without pre-planned schedules and fixed bus stops).

Explanation: As presented in various AVENUE deliverables and in the AVENUE vision, the successful deployment of automated minibuses is highly related with a shift towards MaaS, ToD and a fully deployed Intelligent Transport System.

[155] See https://www.living-innovation.net/explore (last consultation 31 August 2022).

[156] See HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 6 p. 59.

135 Fleets of shared automated minibuses should be integrated into a complete mobility solution with high capacity public transport as a backbone/feeder in densely utilised areas to fulfil the lion's share of trips complemented by walking and cycling[157].

136 An important aspect is the connection of automated minibuses to fleets, especially integrated into public transport. Such fleet-based automated minibuses can interact more efficiently and consequently serve demand better. Fleet-based pooling, i.e. increasing the occupancy rate of automated vehicles by intelligently combining individual routes into an integrated trip, means more mobility with less traffic. In this way, vehicles can also become much more flexible and demand-oriented than classic scheduled services, as they are in principle capable of meeting the demand of different user groups at any time[158].

137 Furthermore, if designed properly, autonomous minibuses will enable people with mobility impairments to participate more in social life and facilitate the provision of services of general interest. This makes it possible to maintain or even expand the range of mobility services, especially in rural areas and in urban areas with low traffic volumes and a weak public infrastructure[159].

138 In order to become attractive and form a credible alternative to private (automated) car ownership, the different sustainable modes need to be coordinated, planned and delivered in an integrated way. From a physical perspective (coordinated network planning, stations, urban planning, and algorithmic optimisation of automated fleets) but also from an information perspective: a one-stop-mobility shop acting as a personal mobility assistant offering travel information, booking and ticketing[160].

139 The creation of multimodal mobility platforms offering Mobility as a Service is the way to connect urban mobility services now and in the future. Public transport authorities and operators are experts in organising urban mobility solutions. They should be allowed to lead the transition and take the lead in coordinating tomorrow's mobility[161].

140 As of today, commercial transportation of passengers requires concessions or permits in most countries, subject to specific requirements. Many legal systems distinguish between a general public passenger transportation permit, often coupled with the requisite of line-based traffic, fixed schedules etc., and a ride hailing (taxi) permit[162]. Automated minibuses are designed to operate on-demand and without predefined itineraries, like conventional taxis with drivers, but as a public transport service. Therefore,

[157] International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017, p. 6.

[158] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 1 p. 6.

[159] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 1 p. 6.

[160] International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017, p. 6.

[161] International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017, p. 6.

[162] Sohjoa Baltic, The Legal Framework, The Roadmap to Automated Electric Shuttles in Public Transport, IKEM — Institut für Klimaschutz, Energie und Mobilität e.V., May 2020, § 2 p. 23 et seq.

they blur the lines between existing categories subject to concessions or permits. France[163] and Germany[164], amongst others[165], have amended their legal framework in this direction.

141 The Law Commission of England and Wales and the Scottish Law Commission have suggested to grant interim passenger permits that would not be subject to taxi, private hire or public service legislation[166].

142 As regards MaaS and ToD, policy, regulation and legislation that enable and support are key to their successful implementation. In addition to the local framework, national governments as well the European Union have an important role to play. Some important regulatory areas include data security and privacy, open data standards, competition law frameworks but also market access of new mobility services, third party ticket sales, subsidization of transport etc.[167].

143 The right for third parties to sell tickets on behalf of a public transport operator is currently not possible in certain cities. Without regulations in place that allow this, the MaaS operator would not be able to act as an intermediary between the mobility service providers and the users. In some jurisdictions, the regulatory framework prescribes that no third party is allowed to sell tickets other than the operator itself. Also, in several countries, pricing for public transport is regulated. It is also worth noticing that in case the public transport operator is in a position of market dominance the chosen strategy (e.g. in terms of providing access to data or to existing ticket sales interfaces and the pricing practises) needs to be evaluated against of the provisions and principles of competition law[168].

144 The data derived from MaaS would help public authorities to make more efficient use of existing infrastructures, improve the traffic management and help enhance sustainable mobility and public transport planning (independently or combined with more conventional data sources, like survey data)[169].

145 As regards ToD, action at European level, by means of both binding and non-binding rules, seems necessary. Hard law could take the form of a directive of minimal harmonisation, leaving place for co-regulation; self-regulation could also be streamlined by means of hard or soft law[170].

---

[163] See amongst others "*Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités*".

[164] See amendements brough to the "Personenbeförderungsgesetz (PBefG)" entered into force in August 2021, in particular § 42, 44 and 50 PBefG.

[165] The Swiss Government has published a draft of a Federal law on the infrastructure of mobility data ("*Bundesgesetz über die Mobilitätsdateninfrastruktur*").

[166] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 10.26 p. 198 et seq.

[167] ERTICO – ITS Europe (editor), Mobility as a Service (MaaS) and Sustainable Urban Mobility Planning, September 2019, § 5.2 p. 28.

[168] ERTICO – ITS Europe (editor), Mobility as a Service (MaaS) and Sustainable Urban Mobility Planning, September 2019, § 5.2 p. 28.

[169] ERTICO – ITS Europe (editor), Mobility as a Service (MaaS) and Sustainable Urban Mobility Planning, September 2019, § 5.2 p. 28.

[170] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 6 p. 59.

146 Depending on its outcome, the ongoing works of the European Commission on a legislative proposal on multimodal digital mobility services might serve as a basis and a model[171], as well as the revision of the Delegated Regulation 2017/1926 of 31 May 2017 on multimodal travel information services (see Appendix A § 3.5.2.4)[172].

4.2 Encourage shared mobility

Issue: The use of automated minibuses will require an increase of shared mobility forms.

Proposed solutions: Public authorities need to take an active role in the roll out of automated vehicles so that they meet policy objectives:

- Measures to limit single car occupancy: road pricing (to the advantage of high occupancy vehicles), parking management, shared vehicle zones and dedicated lanes etc.;
- Make tendering/concessions for shared fleets of automated minibuses;
- Promote shared vehicle use in all forms through promotion and tax incentives;
- Measures to avoid empty private automated vehicles idling on the road;
- Enlarge the competences of public transport authorities to all urban mobility services;
- Prepare for the consequences on employment, as some driver/chauffeur positions could disappear and other positions requiring specific skills will be needed;
- Boost synergies between public transport and private shared mobility actors[173].

Explanation: It is necessary to ensure autonomous vehicles are shared and that people are ready for this idea of sharing and switching between different modes of transport. Therefore, all forms of shared mobility, mainly car- and ride-sharing, need to be actively promoted and incentivised as of today. Tax incentives for shared rides or shared ownership of vehicles, shared vehicle zones, promotional campaigns, priority parking places, promotion of pilot projects: preparing the public for shared automated vehicles in the future goes hand in hand with more car- and ride-sharing today. Measures to limit single car occupancy need to be taken, as well as measures to avoid having empty private automated vehicles on the roads[174].

[171] See https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-multimodal-digital-mobility-services (last consultation 30 August 2022).

[172] Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services.

[173] International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017, p. 8.

[174] International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017, p. 6.

5 Recommendations related to personal privacy

Introduction

147 Data[175] is playing an increasingly important role in the mobility sector, as it forms the basis for (new) business models, but also the foundation for local and municipal authorities' decisions regarding traffic management and control.

148 One of the major novelty of automated minibuses (and automated vehicles in general) is the fact that through their different sensors they are able to collect (process) large amounts of data of their (i) surrounding environment as well of (ii) their interior and passengers. AV's can either process and/or store data locally and/or communicate and transfer data through different channels of communication with the outside world. Much if not all of the data processed by AV's qualifies as personal data, which creates risks and issues as regards personal privacy (e.g. excessive and/or unlawful collection and processing of personal data, profiling etc.) and also increases complexity from a technical point of view.

149 Data collected by automated vehicles and minibuses stands in a field of tension of three interests, at least: safety (e.g. data is processed to ensure safe and secure trips), personal privacy (e.g. conditions and requirements stipulated by privacy protection laws for the collection of personal data) and innovation/commercial exploitation (e.g. providing new mobility services and processing personal data for commercial purposes, but also for public decisions regarding traffic management/control etc.).

The opportunity of providing answers to existing issues and gaps through a dedicated sector specific legislation (complementing the GDPR) should also be assessed and discussed, as the general data protection requirements foreseen amongst others by the GDPR have difficulties to prevail in specialized technical fields such as connected and automated vehicles[176]. The European Commission has also acknowledged that the upcoming cross-sectoral Data Act will most likely not be sufficient to regulate the sector of mobility data (see Appendix A N 669 below).

150 An overview of various data-related legal frameworks can be found at Appendix A § 3 and § 4 (for personal privacy).

[175] Although this usage is debated, the term "data" (which is the Latin plural of "*datum*") will be used with the singular in this deliverable.

[176] See WIDMER, Wie sicher ist sicher genug? Sicht Datenschutz- und Cybersicherheit, Zulassungsrechtliche Herausforderungen des Autonomen Fahrens, Universität Basel, Tagung vom 10. Oktober 2019, slide 31.

5.1 Promote data, algorithmic and AI literacy as well as public participation

Issue: Explanations of privacy related terms and agreements, as well as algorithmic operations and decisions may pose significant cognitive and technical challenges to users and passengers of automated vehicles and minibuses.

Proposed solution: Promote data, algorithmic and AI literacy as well as public participation[177].

Explanation: The necessary explanations related to privacy terms and agreements are often complex. Even with the most scrupulous implementation of user-oriented explainability requirements amongst vehicle manufacturers, service providers and public authorities, the explanations offered are likely to pose significant challenges to individuals with various degrees of prior knowledge and skill in privacy matters. Moreover, users and passengers may have unequal opportunities to acquire the necessary knowledge and competencies to understand the explanations offered[178].

151 As an example, in the field of internet cookies, many users just skip the informational contents about privacy terms and agreements in order to go as quickly as possible to the content of the website they want to consult (on this question, see the Recommendation related to the privacy paradox below § 5.2)

152 As the main stakeholders in and beneficiaries of the deployment of automated minibuses and vehicles, individuals and the general public need to be adequately informed and equipped with the necessary tools to exercise their rights, such as the right to privacy and the right to actively and independently scrutinise, question, refrain from using or negotiate AV modes of use and services[179].

153 Policymakers have a responsibility to inform and equip the public with the capacity to claim and exercise their rights and freedoms. Policymakers should formulate explicit roles and obligations for government, public and educational institutions, to adopt strategies and measures to inform and instruct the public on literacy in relation to artificial intelligence, algorithms and data, and to better equip persons of all ages with abilities to act as conscious users, passengers, consumers and citizens. Furthermore, they have the responsibility to foster active public engagement and facilitate the involvement of all stakeholders for responsible innovation of CAV technology[180].

---

[177] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.3 p. 51.

[178] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.3 p. 50.

[179] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 50.

[180] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 50.

5.2 Mitigate the "privacy paradox" through granular decision making mechanisms

Issue: Consumers express growing concerns about their privacy when using digital services, but they do not act consistently when using these digital services.

Proposed solution: Study and establish mechanisms to allow users and passengers of automated vehicles and minibuses to make informed and granular decisions about their privacy and control their privacy preferences.

Explanation: The privacy paradox illustrates how internet users tend to express much concern in surveys about their privacy and coincide in the need and wish to protect it, but at the same time generously share and dispose of their (personal) data when consuming digital services, for instance by accepting cookies. Typically, the paradox points at two possible reasons: either users are not actually concerned about their privacy, although they declare so, or users lack real and effective means in practice to express their privacy preferences[181].

154 Services are used even though people do not fully trust them, and even when people say that privacy is important to them, they do not always act accordingly. If one's own advantage or the convenience of an offer is high enough, the use of data by third parties is often tacitly accepted. Of course, the fact that what is happening with the individuals' data is hardly visible to him/her and that no disadvantage is incurred immediately also plays an important role[182].

155 The benefits are often more immediate than the costs, which are only perceived *ex post* (afterwards). However, it should also be noted that modern societies are still in inception in terms of their perception of what digitalisation means. The societal dialogue about what digitalisation is supposed to be able to do, and not simply what it can do, is only beginning and will probably still go through several stages[183].

156 Empirical information collected during a recent study published end of 2021 indicated that connected vehicle users were not capable of making meaningful individual decisions about their privacy as regards to the processing of their data in the context of vehicle connectivity, despite their manifested concern about not being in a position to control their data or decide the agents with which it is shared[184].

[181] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 90.

[182] GYSIN (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation – UVEK), Datenschutz Mobilitätsdaten, Bericht, ASTRA-D-DB3D3401/359, 30 November 2020, § 1.3 p. 5.

[183] GYSIN (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation – UVEK), Datenschutz Mobilitätsdaten, Bericht, ASTRA-D-DB3D3401/359, 30 November 2020, § 1.3 p. 5.

[184] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 90.

157 The study indicated that, in the context of car connectivity, the reason behind the existence of a "privacy paradox" is that vehicle users' concern about privacy are not paralleled with mechanisms to allow them to make informed and granular decisions about their privacy and control their privacy preferences[185].

5.3 Investigate measures to foster protection of individuals at group level and provide strategies as regards conflicts over data claims

Issue: The Vehicle-to-Vehicle ("**V2V**"), Vehicle-to-Infrastructure ("**V2I**") or Vehicle-to-Everything ("**V2X**") communication channels include the potential for a multitude of separate actors vying for general and specific personal data in real time or near-real time[186].

Proposed solution: Develop measures to foster protection of individuals at group level[187].

Explanation: One particular challenge that arises in the context of connected and automated vehicles is the privacy protection of multiple concerned individuals (e.g. the driver/safety operator, vehicle passengers, other road users located outside the vehicle such as drivers of other conventional vehicles, pedestrians, cyclists etc.). The use of automated minibuses may include sharing rides from similar origins and destinations between different passengers. In such situations, all passengers sharing the same vehicle, as well as pedestrians and other road users in the vehicle's vicinity could, in principle, be identified (see also Appendix A § 4.2.4.7 below). This can occur without the awareness of those affected[188].

158 The European data protection rules (Art. 6 para. 1 GDPR in particular) require any such processing to rely on a valid legal basis and on transparent information about the processing being provided to all individuals concerned. The collection of data in public spaces may conflict with individual informed consent and realistic opt-out choices for the data subjects[189] mentioned above (see also Appendix A § 4.2.10 et seq. below). Besides consent, lawful grounds for processing personal data in the use case of automated

[185] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 90.

[186] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 39.

[187] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 39.

[188] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 40.

[189] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 40.

minibuses might be public interest and legitimate interest[190], but further researches as regards the legal basis in this field are necessary as well as discussing the opportunity of creating new legals basis'.

159 Besides, the use of videocameras by automated vehicles and minibuses triggers the issue of filming public places, which requires an assessment of the specific relevant legislative framework of each Member State[191].

160 Policymakers should therefore develop legal guidelines that protect individuals' rights at group levels. They should also outline strategies to resolve possible conflicts between stakeholders that have claims over the same data (e.g. location data, sensor data etc., see also Recommendation on access to vehicle data § 6.1 below from an antitrust point of view) or disputes between data subjects, data controllers and other parties (e.g. insurance companies)[192].

161 As conflicts of this type are rather new, stakeholder and policy actions need to be solidly grounded in work by researchers and extensive public deliberation. In particular, there is a need to support and mobilise researchers to study the ethically, legally, and socially justifiable resolutions of data-related conflicts of interest[193].

162 Policymakers should develop new legal privacy guidelines that govern the collection, assessment and sharing of not just personal data, but also non-personal data, third party personal data and anonymised data, if these pose a privacy risk for individuals. This is important because machine learning algorithms are able to infer personal private information about people based on non-personal, anonymised data or personal data from group profiles, over which the affected party might not have data protection rights. This is a new and significant privacy risk[194].

163 As regards existing solutions under the GDPR, it has been suggested to proceed to compliance measures such as data protection impact assessments (carried out by the European Commission before the

[190] BU-PASHA, Legal aspects, public interest, and legitimate interest in processing personal data to operate autonomous buses in the regular transportation system, Security and Privacy, 2022;e247, May 2022, § 4 p. 7.

[191] See European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 35 p. 11.

[192] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 39.

[193] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 39.

[194] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 39.

deployment of ITS services[195]), to issue codes of conducts and to develop data protection certification seals and marks[196] etc.

5.4 Develop transparency strategies to inform particular road users about data collection and associated rights

Issue: Mobility-induced conflicts of interest are largely unavoidable due to the need for automated vehicles and minibuses to move through public spaces, where intentional but non-consensual monitoring and collecting of traffic related data, and its later use for research and development or other public ends can occur[197].

An important question is to which extent it is necessary to obtain consent from potential third parties outside of the vehicle, for instance pedestrians and vulnerable road users. It is impossible to obtain consent for data processing from all persons who appear in the vicinity of the automated vehicle while it is in motion. It is also not possible to directly provide the identity and contact details of the data controller to these external road users[198].

Proposed solution: Investigate transparency strategies to inform particular road users about data collection and associated rights[199].

Explanation: Connected and automated vehicles moves through physical space and may select alternative routes without consulting the passengers prior to such choices. Therefore, depending on the use case and the operational design domain, an AV ride may result in personal data collection that could not have been anticipated from the outset, to which the data subjects may have not consented and of which they may never become aware. Thus, individual instances of travel are likely to cause its passenger(s) to intersect with, move through and thereby be subjected to a great number of geographical and personal spheres

[195] European Data Protection Supervisor (EDPS), Opinion 3/2022 on the Proposal for amending the Directive on the framework for the deployment of Intelligent Transport Systems in the field of road transport, 2 March 2022, § 3.5 p. 9.

[196] Valdani Vicari & Associati (VVA) Economics & Policy, Study on market access and competition issues related to MaaS, June 2019, p. 22 and the quoted references.

[197] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 41.

[198] Fernández Llorca/Gómez, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 42.

[199] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 41.

with potentially divergent and privacy intrusive personal, private (commercial), public or government related data interests, regulations and requirements[200].

164 To a certain extent, the GDPR, in particular Art. 5 para. 1 GDPR on purpose limitation (litt. b) and data minimisation (litt. c), addresses problems of this sort. Furthermore, the stricter the rule stating that only necessary data should be collected is applied, the less warning will be needed. Nevertheless, the numerous exceptions in the GDPR to consent-based personal data collection and processing (Art. 6 GDPR) may leave scope for privacy intrusive data practices. In addition, when legally enforcing the rights concerning purpose limitation and data minimisation, diverging interests between different data subjects, collectors and stakeholders may be afforded different weight, thus effecting power imbalances at these intersections[201].

165 Therefore, developing novel and creative transparency standards (e.g. via textual, visual, audio and/or haptic elements) to communicate those privacy risks effectively and to inform about associated privacy rights (e.g. opt-out, deletion of personal data, data access rights, recourse mechanisms, alternate routes and point destinations) are of paramount importance[202].

166 For instance, in Germany it has been suggested that automated vehicles should at least be equipped with a label that (i) identifies them as a vehicle with video-cameras and (ii) refers to a website containing the information required by Art. 13 GDPR[203]. Another scholar considers that providing data subjects in this constellation with all the mandatory information of Art. 13 GDPR seems hardly feasible and, in view of the minor impairment of privacy that can be ensured in the case of direct anonymisation, unnecessary[204].

167 Policymakers should consider this issue and work with vehicle manufacturers, deployers and PTO's to develop meaningful, standardised transparency strategies to inform road users, including pedestrians and vulnerable road users of data collection in the operating area of automated minibuses that may, directly or indirectly, cause risks to their privacy as they travel through such areas. This includes digital and near

[200] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 42.

[201] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 42.

[202] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 42.

[203] STEEGE, Datenverarbeitung beim autonomen Fahren – Schafft die StVG-Novelle 2021 Rechtssicherheit bei der Datenverarbeitung?, Cologne Technology Review & Law, CTRL 2/22, § C p. 37.

[204] ALGORIGHT e.V (HESSEL), Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, Saarbrücken, 30 April 2021, § 2 p. 8

real-time updates for road users when approaching, entering, and leaving zones where potentially privacy intrusive data collection occurs[205].

168 Such communication may occur through in-vehicle or wearable smart-device displays, audio-visual aids on roads (e.g. street signs, flashing icons, beeping sounds), or other minimally privacy-invasive communication modes with textual, visual, audio and/or haptic elements. This allows the communication of privacy risks and rights to a wide and diverse audience[206].

169 Only indirect methods are possible that allow these users, on the one hand, to clearly and easily identify that the vehicle is automated/autonomous (e.g. a colour code), the manufacturer (e.g. logo) or the mobility company (e.g. vehicle lettering), as well as other distinctive details such as license plate number, model, color etc. and on the other hand, to have public information (e.g. on websites) with all the data required by the regulation to easily allow to establish who the data controller is[207].

170 In any case, there are scenarios that can mitigate, or even avoid entirely, the requirement for consent from external users. For instance, if the images are only processed in real-time to generate non-identifiable metadata such as free space, anonymous vehicle and pedestrians locations and future motions etc. then they are neither stored (only the time needed to process them, and never reaching persistent storage) nor transmitted, which limits the intrusiveness. Controllers may in some cases also be able to argue that they rely on other grounds for lawfulness of their processing than consent. Finally, if appropriate privacy-by-design approaches, including image de-identification methods, are implemented to process, store or transmit images without personal data, data protection laws such as the GDPR would no longer apply[208].

171 As these suggested measures are new, stakeholder and policy actions and decisions need to be grounded in evidence from researchers and extensive public deliberation. Researchers should study:

- ethically, legally, and socially justifiable resolutions of data related conflicts of interest;
- the design of accessible and user friendly data collection and privacy intrusion related alert terms and symbols;
- mechanisms to communicate these clearly and efficiently in dynamically shifting and distracted road user situations; and
- the type of interfaces and notification options that most efficiently support user empowerment in setting preferences, choosing routes, and negotiating terms and conditions.

[205] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 41.

[206] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 41.

[207] Fernández Llorca/Gómez, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 42.

[208] Fernández Llorca/Gómez, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 42.

172 Policymakers should consider and, where relevant, apply the outcomes of this research. In all of these activities, there must be compliance with data protection laws[209].

5.5 Define appropriate anonymisation techniques and/or how successful anonymisation can be achieved in the field of AV's

Issue: With an abundance of different types of data processed by automated vehicles, what data are to be considered personal is not straightforward in all cases. This question has implications for data anonymisation and the (de-identification) techniques considered appropriate to avoid re-identification[210]. The threshold for anonymisation techniques in order to consider de-personalised data as anonymous data under the GDPR is not defined nor established. In the same way, the time relevant frame for successful anonymisation is only set in relative criteria that are not clear, which creates undesirable legal uncertainty.

Proposed solution: Further guidance issued by privacy authorities on these questions for instance would be useful to avoid the proliferation of different interpretations. Certification of anonymisation techniques[211] or legal provisions with more fine-grained definitions and a description of specific means preventing from re-identifying personal data within the automated vehicles ecosystem should be enacted[212] in a dedicated mobility data legislation, for instance.

Explanation: In its 2017 Resolution on Data Protection in Automated and Connected Vehicles, the International Conference of Data Protection and Privacy Commissioners seriously urged parties to utilize anonymisation measures to minimize the amount of personal data or to use pseudonymization when not feasible[213].

173 As of today, guidance on anonymisation techniques (and/or other de-identification methods) applicable to vehicle-generated data that are compliant with GDPR is limited and room for interpretation is left to

[209] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.2 p. 41.

[210] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 198.

[211] As suggested by HESSEL and MENZ, see https://www.managementcircle.de/blog/datenverarbeitung-automatisiertes-und-autonomes-fahren.html (last consultation 31 August 2022).

[212] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 5 p. 17.

[213] Resolution on Data Protection in Automated and Connected Vehicles of the 39th International Conference of Data Protection and Privacy Commissioners Hong Kong, 25-29 September 2017, N 2 p. 3.

national courts and data protection authorities, thus creating legal uncertainty and potential market distortions and fragmentation[214].

174 In its 2017 opinion dedicated to the processing of personal data within Cooperative Intelligent Transport Systems, the Article 29 Working Party explained that various technical possibilities exist in order to minimize the risks of re-identification, such as the improvement of the issuing policy of Public Key Infrastructure certificates, the frequency adjustment of broadcasting of Cooperative Awareness Messages, by application of the data minimization principle with remedies such as generalization or noise injection[215].

175 If anonymised mobility data is used, clear requirements for anonymisation must be established and further protection concepts that reduce as far as possible the risk of de-anonymisation must be developed[216].

176 The further development of anonymisation techniques (and/or other de-identification methods) is an essential building block in order to encourage the free flow of data within the different actors involved in the development of automated vehicles and minibuses[217] (on this topic, see also Recommendation § 6.3 below).

177 However, proper anonymisation is an extremely demanding challenge, especially when data is shared or even published over an indefinite time horizon, with indefinite recipients and can thus be merged from different sources. For some years now, there has been increased research into how strong anonymisation can be achieved with appropriate security concepts without compromising the quality of the analysis. This research into anonymisation procedures should be intensified and promoted[218].

178 The European legislator has refrained from an absolute concept of anonymisation in the GDPR. Anonymisation is therefore not to be understood in a binary way. Rather, there is a spectrum of different anonymisation measures that have different qualities and are therefore appropriate and suitable for

[214] IACOB/CAMPMAS/SIMONELLI (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Annex IV Recommendations to the EU and national policy makers and an action plan for the creation of shared EU-wide in-vehicle data platforms, EASME/COSME/2018/004, 20 April 2021, § 2.1 p. 225.

[215] Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (WP 252) 17/EN, Adopted on 4 October 2017 p. 7.

[216] Nationale Plattform Zukunft der Mobilität (NPM), Ergebnisbericht der Nationalen Plattform Zukunft der Mobilität – Ergebnisse aus drei Jahren NPM (2018-2021), § 3.3 "Datenschutz und Security", October 2021, p. 46.

[217] Verbraucherzentrale Bundesverband e.V. (Germany), Vertrauen stärken durch verbraucherfreundliche Daten-Governance, Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance, 12 January 2021, p. 7.

[218] Verbraucherzentrale Bundesverband e.V. (Germany), Vertrauen stärken durch verbraucherfreundliche Daten-Governance, Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance, 12 January 2021, p. 7.

different purposes. However, the GDPR does not provide information on the circumstances under which anonymisation can be considered sufficient[219].

179 Further protection concepts are needed to reduce the risk of de-anonymisation. Specific requirements for anonymisation as well as for the use of anonymised data should be defined through legislative requirements and the development of standards[220].

180 The creation of codes of conduct and similar initiatives, such as the UK's Information Commission's Office Anonymisation Code of Practice[221], is crucial to support data controllers and processors in assessing the risk of re-identification.

181 Updating opinions of the Article 29 Working Party that have not been endorsed by the EDPD, such as the opinion on anonymisation techniques, could be helpful to provide further legal certainty[222]. A dedicated EDPD opinion on the processing of data by automated vehicles would also be a helpful solution.

5.6 Increasing complexity of data processing schemes

Issue: The data processing scenarios and loops described in the AVENUE vision will involve numerous stakeholders and therefore increase the complexity of the data processing and defining the roles of each actor under the GDPR.

Proposed solution: Study the impact of schemes and loops such as the one described in the AVENUE vision, promote the use of multi-party "Data Management Agreements" or similar solutions to this issue and, if necessary, adapt the legal framework and the existing functions of controller and processor to these new schemes.

Explanation: As described in the AVENUE vision loops[223], the deployment of automated minibuses within Maas in a first step and within intelligent transport systems in a second step will involve numerous actors processing personal data:

- the owner/holder of automated minibuses (the public transport operator for instance);

[219] Verbraucherzentrale Bundesverband e.V. (Germany), Vertrauen stärken durch verbraucherfreundliche Daten-Governance, Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance, 12 January 2021, p. 7.

[220] Verbraucherzentrale Bundesverband e.V. (Germany), Vertrauen stärken durch verbraucherfreundliche Daten-Governance, Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance, 12 January 2021, p. 7; see also BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 4.2 p. 16.

[221] Information Commission's Office, Anonymisation: managing data protection risk code of practice https://ico.org.uk/media/1061/anonymisation-code.pdf (last consultation 31 August 2022).

[222] European Parliamentary Research Service (EPRS), Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?, Scientific Foresight Unit (STOA) PE 634.445, July 2019, Executive Summary p. IV.

[223] See AVENUE vision § 2 and § 3 and the loops depicted in Figure 15 amongst others.

- the vehicle manufacturer;
- the MaaS platform operator;
- the MaaS aggregator;
- the public transport authority;
- further public authorities, such as the road traffic supervision authorities, telecommunication authorities etc.;
- the manufacturers of sensors or other connected components (eventually);
- trusted organisations in charge of accident analysis for road safety improvement;
- other trusted third parties such as insurance companies;
- other upcoming trusted third parties such as data intermediaries (see Art. 10 to 15 DGA);
- Etc.

182 In this constellation, determining the functions of each party might become complex, potentially with several controllers sharing tasks and competencies, joint controllers etc.

183 This type of issue was already identified by the Article 29 Working Party in 2014 within the context of the Internet of Things, where Article 29 Working Party described that the complex mesh of stakeholders asked for the necessity of a precise allocation of legal responsibilities amongst them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions[224].

184 Such grey areas create both compliance and ethical complications with respect to accountability, where stakeholders feel that the responsibility for data protection compliance lies with another entity, and thus may feel free to process personal data in ways that they deem more convenient or beneficial, perhaps to the detriment of the data subjects concerned[225].

185 In its White Paper on AI, the European Commission has clarified that the principle of accountability lies with the actor(s) best placed to address risks. Therefore, the criteria of who is in the best position to address risks can help vehicle manufacturers, service providers and software developers etc. to take the appropriate data processing role in the different stages of the lifecycle[226].

186 Conventional agreements to regulate data processing relationships, such as Data Processing Agreements and joint controllership agreements may prove impractical to deal with these intricate relationships, as they may not suffice to cover all different roles which each of the parties involved in data processing plays. In order to address the grey area and the need to sign several Data Processing Agreements, stakeholders

[224] Article 29 Data Protection Working Party, Opinion 08/2014 on Recent Developments on the Internet of Things (WP223) 14/EN, Adopted on 16 September 2014, §3.3 p. 11.

[225] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.1 p. 5 and the quoted reference.

[226] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.1 p. 6 and the quoted references.

should consider engaging each other through more complex contractual frameworks (such as "Data Management Agreements")[227].

187 By properly configuring a "Data Management Agreement", the various actors involved can:

- Map out the different types of AV related data processing activities which they need to perform;
- Identify the role(s) – independent controller, processor or joint controller – which applies to them in relation to each defined processing activity; and
- Set out the obligations to which each of them are bound as a result of the roles identified for each specific activity[228].

188 This greatly reduces the risk of "grey zones" or undefined loopholes and ensures greater comprehensiveness and clarity of regulation of these complex processing relationships, for the benefit of AV stakeholders as well as the data subjects concerned[229].

189 In this context, other concepts, such as the co-creation of data and its impact on the data protection and privacy framework, should also be studied and explored.

190 As already mentioned, it should be avoided that stakeholders (that might also be data subjects) with no access to the data or the software are designated as controllers, as they have no means of understanding and shaping related processes and thus cannot comply with controller duties such as the provision of information, system design or the enforcement of data subject rights.

5.7 Data minimization and purpose limitation principles

Issue: The principle of data minimization requires to only process the personal data which is strictly necessary for the purposes of the processing, which has to be defined before the data collection. As described in the AVENUE vision, through their connectivity and numerous sensors such as videocameras, LIDAR etc. automated vehicle can collect a great deal of useful information, including personal data. Such large scale collection may conflict with the data minimization as well as the purpose limitation principles.

Proposed solution: Encourage and proceed to further researches in order to implement short and long term solutions and best practices that contribute towards purpose limitation and data minimisation.

[227] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.1 p. 6 and the quoted references.

[228] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 3 p. 11.

[229] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 3 p. 11.

Explanation: Like purpose limitation, data minimisation (see Appendix A § 4.2.6.2 and Appendix A § 4.2.6.3) is a risk-management measure as processing of excess data creates unnecessary risks, from "hacking to unreliable inferences resulting in incorrect, wrongful and potentially dangerous decisions"[230].

191 To support their continuous navigation, automated vehicles and minibuses use data permanently, including personal data. This perpetual data usage poses important challenges to the principles of purpose limitation and data minimisation: collecting large datasets of personal data to train the AI models (amongst other purposes) jeopardizes the data minimization principle and further collection, use, transmission, or storage of personal data may exceed the purpose limitation principle from the beginning of these data processing operations[231].

192 In order to be compliant with the data minimisation principle, controllers (such as vehicle and sensor/equipment manufacturers, service providers and software developers, amongst others stakeholders) must have a clear overview of the categories of data they need from a AV by utilising the two following criteria:

- It should be relevant for the intended specific processing;
- It should be necessary for the intended specific processing[232].

193 All AV-stakeholders should aim to carry out this assessment prior to the collection of personal data and be in the position of demonstrating that they have done so – specific obligations to perform data minimisation assessments (either specifically, or as part of wide data protection impact assessments) and to properly document and make those assessments available[233]. In addition, a distinction between data used for AV training and data used for the deployment of the automated vehicles[234] would be desirable.

194 The principle of purpose limitation also potentially stands in a tension with the current and ongoing practices. Purpose limitation seeks to reduce privacy risks by limiting the ways in which the data can be processed (see Appendix A N 909 et seq.). This limitation of data processing has been criticised in recent

[230] FINCK/BIEGA, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, Technology and Regulation, 2021, § 4.4 p. 55 and the quoted reference.

[231] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.1 p. 7 and the quoted reference; see also BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.5 p. 9.

[232] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.5 p. 9.

[233] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.5 p. 9.

[234] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.5 p. 9 and the quoted references.

years as potentially stifling an innovative European data economy, including in respect of artificial intelligence[235].

195 Scholars have argued that for big data "to reach its potential, data needs to be gathered at an unprecedented scale whenever possible, and reused for different purposes over and over again". Others noted that "there is one necessary condition for enabling innovation to flourish: allowing data to be processed without a pre-determined purpose" and that "due to social trends and technological developments (such as Big Data and the Internet of Things) the principle of purpose limitation will have to be abandoned"[236].

196 According to scholars, the principles of purpose limitation and data minimisation remain feasible, albeit challenging[237].

197 There is also an open debate on the relationship between Art. 5 para. 3 ePrivacy Directive and Art. 6 GDPR for subsequent processing operations[238] (see Appendix A § 4.3.3 N 995 et seq.).

[235] FINCK/BIEGA, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, Technology and Regulation, 2021, § 4.4 p. 55.

[236] FINCK/BIEGA, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, Technology and Regulation, 2021, § 2.1 p. 45 and the quoted references.

[237] FINCK/BIEGA, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, Technology and Regulation, 2021, § 7 p. 60.

[238] See amongst others Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 94; BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.4 p. 8 and the quoted references.

6 Recommendations related to competition

Introduction

198 Antitrust authorities have long been considering the application of competition rules to the digital sector. Different tools now exist and certain anti-competitive practices are monitored, but in terms of effectiveness of competition tools, following pitfalls are still encountered:

- competition authorities generally intervene *ex post* when, given the constant technological innovations, operators need strong signals to launch themselves on the market;
- with the increasing complexity of technological tools, problems of proof are recurrent;
- the definition of relevant markets, which is not always obvious[239].

199 These issues are likely to happen in the specific field of automated vehicles, although the type-approval framework might be reformed in order to integrate antitrust rules and provide a remedy to the *ex post* intervention.

6.1 Regulate access to vehicle data

Issue: Vehicle manufacturers and/or tech companies developing automated vehicles and minibuses have control over vehicle data, e.g. they can decide to whom and to which type of data they provide access to. This *de facto* access right places them currently in an undesirable gatekeeper position that should be avoided by creating a legal framework, as contractual arrangements between operators will not be sufficient.

Proposed solution: Regulate access to vehicle data, for instance through a dedicated mobility data act[240].

Explanation: Vehicle-generated data and data produced by the users (driver/safety operator, passengers etc.) of automated vehicles and minibuses are valuable not only to vehicle manufacturers and/or tech companies developing automated vehicles, but also to many third parties, such as the deployers of these vehicles (PTO's etc.), public authorities (the PTA's for road traffic management etc.), scientific entities studying incidents, insurance companies and independent service providers etc.[241].

---

239 https://cms.law/fr/fra/publication/la-loi-d-orientation-des-mobilites-lom-l-ouverture-des-donnees-et-le-respect-de-la-concurrence (last consultation 31 August 2022).

240 France in its "*Ordonnance no 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules*" and Germany in its "*Mobilitätsdatenverordnung vom 20. Oktober 2021*" have followed this path; Switzerland is currently discussing the introduction of a federal law dedicated to the mobility data infrastructure.

241 ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 10 and the quoted references.

200 However, vehicle manufacturers and/or tech companies deploying automated vehicles and minibuses benefit from a *de facto* access to and control of the vast amount of data collected by the myriad of devices and sensors placed in these vehicles[242].

201 As an example, the PTO's in the AVENUE project have described their automated minibuses (that were their property) as "black boxes", one of the PTO's mentioning that it had "no access to shuttle data"[243]. To get access to vehicle data, the PTO's needed to request access to the manufacturer of the automated minibuses, although they were the legal owners of the automated minibuses.

202 Different schemes for accessing in-vehicle data exists, but according to the current architecture promoted by vehicle manufacturers for connected vehicles, the Extended Vehicle concept ("**ExVe**"), vehicle manufacturers would have exclusive, direct, full and privileged control of data on their proprietary server and over who is granted access to the data[244].

203 This position has been compared to the position of gatekeepers regulated recently by the Digital Market Acts, as the vehicle manufacturers and/or tech companies can leverage this central position to data generated by connected and automated vehicles to any third party that would like to access to this data[245].

Alternative solutions (such as the Secure On-Board Telematics Platform[246] for instance) exists and should be studied, promoted and regulated with the purpose of avoiding important market distortions.

204 A similar situation occurred recently as regards the unrestricted access to vehicle repair and maintenance information ("RMI"), which has been regulated by the EU Regulation 2018/858, via a standardized format, in order to ensure effective competition in this market (see Appendix A § 1.2.2.4 below).

205 As recognized by the European Commission in March 2022, access to vehicle data should follow the same principles anchored in the Data Act, namely transparency, non-discrimination and technological neutrality. Approaches similar to the upcoming DGA's data intermediaries (see Appendix A § 3.2.2.3 below) might also be useful in this context and serve as inspiration. A dedicated mobility data act should include at minimum a list of data, functions, resources as well as governance rules on access to the vehicle data and establish interoperability through standardisation[247] (see also Appendix A § 3.2.5 below).

---

[242] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 103.

[243] AVENUE Deliverable D6.6 Second Iteration Cybersecurity and privacy control action plan and recommended technologies, 28 February 2021, § 3.3.1 p. 21 and § 3.3.3 p. 22.

[244] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 10 and the quoted references.

[245] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 103.

[246] See amongst others Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 97 et seq.

[247] See European Commission (DG GROW I2), Call for evidence for an Impact Assessment, Access to vehicle data, functions and resources, Ares(2022)2302201, 29 March 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en (last consultation 31 August 2022), p. 2 and 3.

206 In 2018, a resolution of the European Parliament had also identified the necessity of ensuring a level playing field and security as regards the storing and accessing of in-vehicle data and to grant access to in-vehicle data to third parties in order to promote competition in the market (see Appendix A § 1.2.6 below).

6.2 Anticipate the potential market power of MaaS providers

Issue: Similarly to the issues related to access to vehicle data, MaaS providers might achieve considerable market power in the future, which creates the risks of price "dictatorships" by MaaS service providers and a tendency towards monopolisation in the MaaS market, due amongst others to economies of scale[248].

Proposed solutions: Various regulatory policies are conceivable in order to prevent market distortions and monopolisation in the field of MaaS and should be discussed and decided at political level.

Explanation: In the future, most mobility services will be booked via MaaS platforms, which will establish themselves as the gateway to mobility. Due to the lack of other market access, it will be necessary for transport service providers to sell their offers via a MaaS provider and to accept his conditions. This creates the danger of "price dictatorships" by the MaaS service provider. The price pressure can be passed on to the transport service providers due to the market power of the MaaS service provider. There is also a considerable tendency towards monopolisation in the MaaS market, due to economies of scale[249].

207 On the other hand, an efficient offer of new mobility services needs precisely these economies of scale to be economical. A certain trade-off is therefore necessary here. What is critical about this development trend is that MaaS providers find themselves in a neuralgic position: they can both influence the prices for end customers and determine the compensation that transport companies and mobility service providers receive. Abuses of this market power must therefore be prevented[250].

208 In order to prevent market distortions and monopolisation in the field of MaaS, following regulatory policies are conceivable:

- The regulator can assume a strong controlling role and establish a legal monopoly on MaaS services as a public service. The operation can be awarded to third parties (through a concession or public tender), but by awarding the contract, the state can define prices, the processing of user data as well as contractual terms and conditions for transport service providers and users.
- The regulator may focus on setting guidelines and create a level playing field for MaaS offerings, with the aim of keeping the diversity of MaaS providers as high as possible. Conceivable would be the development of a generally applicable data standard, the stipulation of minimum standards

[248] Federal Roads Office (Switzerland) et al., Transport of the future 2060: New types of service – organization and diffusion, SVI 2017/006, October 2020, § 9.4.2 p. 110.

[249] Federal Roads Office (Switzerland) et al., Transport of the future 2060: Synthesis Report, SVI 2016/002, 1685, September 2020, § 10.3 p. 100.

[250] Federal Roads Office (Switzerland) et al., Transport of the future 2060: Synthesis Report, SVI 2016/002, 1685, September 2020, § 10.3 p. 100.

for MaaS providers (with regard to working conditions, consumer rights etc.) and the requirement for non-discriminatory access to mobility.

- Another possible solution is to support the existing private and public mobility providers in the sense of public-private partnerships and to develop common MaaS offerings[251].

209 In Europe, some Member States[252] have already enacted legal frameworks dedicated to MaaS, which might serve as examples.

210 Art. 101 and 102 TFEU (and their equivalent provisions under the national laws of Member States) prohibits anti-competitive practices and agreements and abuse of dominance. Cooperation between PTO's and MaaS providers could, under certain circumstances, be in violation of these provisions. For example, this could be the case if a cooperation arrangement led to an exchange of commercially sensitive information between competitors (e.g. between different transport operators of the MaaS system, provided that they are competitors or potential competitors) if it entailed price fixing or market sharing, also between competitors or potential competitors, or if it led to the application – within the MaaS system – of different conditions to competing transport operators, thereby placing some of them at a competitive disadvantage[253].

211 Competition concerns might also arise under certain circumstances when state aid (subsidisation) is granted to a public transport operator[254].

6.3 Definition and creation of open datasets and open API's as public and open infrastructural resources

Issue: Emphasising fairness in the context of (connected and) automated vehicles requires the identification and establishment of certain data and application programming interfaces ("**API**") as free and open resources[255].

[251] Federal Roads Office (Switzerland) et al., Transport of the future 2060: New types of service – organization and diffusion, SVI 2017/006, October 2020, § 9.4.2 p. 110.

[252] For instance Finland with its 2017 Act on Transport Services and France with the 2019 "*Loi d'orientation des mobilités*".

[253] Valdani Vicari & Associati (VVA) Economics & Policy, Study on market access and competition issues related to MaaS, June 2019. § 4.2 p. 10 et seq.

[254] Valdani Vicari & Associati (VVA) Economics & Policy, Study on market access and competition issues related to MaaS, June 2019. § 4.3 p. 17 et seq.

[255] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46.

Proposed solution: Proceed to researches in order to identify high-value datasets as public and open infrastructural resources[256] and promote and develop open or public APIs.

Explanation: Strenghtening fairness in the context of automated vehicles requires the identification and establishment of certain data and application programming interfaces as free and open resources[257], as recommended in the AVENUE vision[258].

212 Following data (amongst others) should be considered as high-value in the context of CAVs:

- geographical data;
- orthographic[259] data;
- satellite data;
- weather data;
- data on crash or near-crash situations[260];
- data on mobility, traffic patterns and participants[261].

213 Consequently, these types of (static and dynamic[262]) data should be identified and kept free and open, insofar as they can be linked to infrastructural resources that support free innovation, competition and fair market conditions[263]. Some of those datasets are already qualified as "high-value dataset" in Annex I of the Open Data Directive[264].

214 The successful identification and protection of such free, open and high-value datasets for CAV design, deployment and use will require a number of efforts involving multiple stakeholders[265].

---

[256] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46.

[257] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46.

[258] See AVENUE Vision § 5.1 and § 5.5 amongst others.

[259] Orthographic projection is a means of representing three-dimensional objects in two dimensions.

[260] Regarding the specific question of access to vehicle data within crash or near-crash situations in order to study it for safety purposes, see AVENUE Deliverable 9.2 "Transition roadmap for safety and service quality".

[261] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46.

[262] Dynamic data (or transactional data) is information that is periodically updated, meaning it changes asynchronously over time as new information becomes available. Data that is not dynamic is considered static (see also Appendix A § 3.4.1.2 below).

[263] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46.

[264] Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information ("PSI Directive" or "Open Data Directive"); see also Appendix A § 3.4.1.3 below.

[265] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46; see also Federal Roads Office (Switzerland) et

215 Policymakers should first detail what sorts of data could and should be deemed high-value in the context of automated vehicles and therefore be kept free and open. They should do this in dialogue with manufacturers and deployers of automated vehicles, as well as with third party data stakeholders[266]. This dialogue could for instance take place in the upcoming creation of the European Mobility Data Spaces[267] introduced by the European Data Strategy[268] (see Appendix A § 3.2.1.1 below).

216 Further, for functional open access, data formats and processing requirements will need to be harmonised and standardised in accordance with non-commercial, platform-neutral schemes and taxonomies. The successful establishment of these schemes will need to rely on extensive research and cooperation with open source and standardisation organisations[269].

217 In another step, policymakers should, to the extent possible, and in full compliance with personal and data privacy legislation, lead and support the establishment of high-quality high-value data infrastructure resources. Such infrastructural resources are essential for the creation of optimal conditions for analysis, response, decision-making, innovation and fair competition[270].

218 Finally, policymakers need to identify specific obligations for state, public and private actors to provide certain types of data as open data, in the interests of transparency, fair competition, financial and industrial development and competitiveness[271].

219 There are risks from unduly keeping such high-value datasets out of the public realm. Such risks are especially important if this data would help optimal analysis, decision-making, fair competition and

al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 3: Handling Data, SVI 2017/044, October 2020, p. 136.

[266] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46; see also Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 3: Handling Data, SVI 2017/044, October 2020, p. 136.

[267] See amongst others European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23 February 2022.

[268] https://digital-strategy.ec.europa.eu/en/policies/mobility-data (last consultation 31 August 2022).

[269] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46; see also Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 3: Handling Data, SVI 2017/044, October 2020, p. 136.

[270] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 46.

[271] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 47.

responsible innovation and if such data would benefit society and the planet in a more fundamental sense[272].

220 Stakeholders across various concerned sectors and industries will have different views, needs and interests concerning the same vehicle-generated and/or mobility-relevant data. Some of them could aim to pursue strategic partnerships for harnessing, enclosing and safeguarding proprietary data as business opportunities, for instance on the basis of intellectual property rights etc.

221 In a MaaS context, data sharing between the mobility service providers and the MaaS operator (and vice versa) are critical for MaaS to exist. Transport operators may feel concerned about opening their data, as they see different perceived risks: losing the customer relationship, the MaaS provider becoming the gatekeeper to all demand and usage data, disclosing the business model to competitors by sharing data or uncertainty that all transport operators are treated fairly by the integrator. These challenges need to be addressed when regulating. The quality and consistency of data shared and the data format are essential for MaaS. It must be easy for all mobility service providers, large and small players, to plug in the MaaS solution[273].

222 Thus, there are challenges emanating from the forces that drive commercialisation and privatisation of CAV-relevant data and tools that are, or could be, seen as being a public good[274]. According to some studies, mobility data, both public and private, must be collected under the aegis of the public transport authority, which is the only trusted third party capable of doing so[275].

223 Regarding APIs, the development of common APIs would be a considerable step towards MaaS. As explained in a recent study, the implementation of every new API by a platform requires almost 600 workdays, while the adaptation of an existing API to new uses demands only 20-30 workdays[276].

224 Developing a common API is more than a technical issue, because it encompasses two potentially highly political decisions:

- the qualitative and formal characteristics of data to be entered into the API; and
- the objective behind the optimization of the API: time, price, CO^2 emissions etc.[277].

[272] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 48.

[273] ERTICO – ITS Europe (editor), Mobility as a Service (MaaS) and Sustainable Urban Mobility Planning, September 2019, § 5.2 p. 28.

[274] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 13, p. 48.

[275] CROZET/SANTOS/COLDEFY (CERRE), La regulation de la mobilité urbaine à l'épreuve de la mobilité partagée et du "MaaS", Rapport, Septembre 2019, p. 8.

[276] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 4.6.2 p. 48.

[277] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 4.6.2 p. 49.

7 Recommendations related to civil liability

Introduction

225 The main opinion in the published legal literature is to consider that automated vehicles in their current stage of development will not create major gaps in the applicable European liability framework. However, various issues have been identified, mostly related to product liability, and they should be addressed, as it will presented in the next recommendations.

226 Further details related to liability and the product liability framework can be found under Appendix A § 6.

7.1 Ensure the existence of fair and quick compensation mechanisms

Issue: Under the existing product liability framework, the characteristics of AI products (amongst others automated vehicles) could render liability claims difficult or overly costly to prove for victims and consequently they may not be adequately compensated[278].

Proposed solution: Ensure the existence of fair and effective mechanisms for granting compensation to victims of accidents involving (connected and) automated vehicles[279].

227 **Explanation:** In accordance with the harmonised rules on motor vehicle insurance[280], the use of a motor vehicle must be insured and the insurer is always in practice the first point of claim for compensation for personal injury or material damage. According to these rules, the mandatory insurance compensates the victim and protects the insured person who is liable under national civil law rules to pay financial damages for the accident involving the motor vehicle[281].

228 Automated vehicles and minibuses are not treated any differently than non-autonomous vehicles as regards motor insurance in the legislation of the European Union. Such vehicles, like all vehicles, must be covered by the third party motor liability insurance, which is the easiest way for the injured party to get

[278] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13.

[279] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 20, p. 62.

[280] See Art. 18 Directive 2009/103/EC of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability ("**MID**").

[281] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13.

compensation[282]. It should be noted that within product liability, producers are not subject to mandatory insurance under the Product Liability Directive[283].

229 Gaps may exists, as the insured risk is assessed differently in different Member States[284]. In addition, new types of incidents might happen, with situations potentially falling out of the scope of existing regulations[285].

230 Taking out proper insurance can mitigate the negative consequences of accidents by providing for a smooth compensation for the victim. Clear liability rules help insurance companies to calculate their risks and to claim reimbursement from the party ultimately liable for the damage. For example, if an accident is caused by a defect of the vehicle, the motor vehicle insurer can claim reimbursement from the manufacturer after compensating the victim[286].

231 The characteristics of emerging digital technologies like artificial intelligence, the Internet of Things and robotics challenge aspects of European and national liability frameworks and could reduce their effectiveness. Some of these characteristics could make it hard to trace the damage back to a human behaviour, which could give grounds for a fault-based claim in accordance with national rules. This means that liability claims based on national tort laws may become difficult or overly costly to prove and consequently victims may not be adequately compensated[287].

232 It is important that victims of accidents of products and services including emerging digital technologies do not enjoy a lower level of protection compared to similar other products and services, for which they would get compensation under national tort law[288].

233 It will need to be assessed whether challenges of the new technologies to the existing frameworks could also cause legal uncertainty as to how existing laws would apply (e.g. how the concept of fault would apply to damage caused by artificial intelligence). These could in turn discourage investment as well as increase information and insurance costs for producers and other businesses in the supply chain, especially European SMEs. In addition, should Member States eventually address the challenges to national liability

[282] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13; PROBST, Das "selbstfahrende" Auto: entfernte Illusion oder nahe Realität?, Strassenverkehr 1/2021, Dike Verlag AG, 2021, pp. 52-58, § F N 1 p. 56.

[283] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[284] PUNEV, Autonomous Vehicles: The Need for a Separate European Legal Framework, European View 2020, Vol. 19(I) 95-102, 2020, p. 99 and the quoted reference.

[285] PUNEV mentions a case where the owner (e.g. the "driver") of a private automated vehicle may become the victim in an accident caused by its own car.

[286] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13; PROBST, Das "selbstfahrende" Auto: entfernte Illusion oder nahe Realität?, Strassenverkehr 1/2021, Dike Verlag AG, 2021, pp. 52-58, § F N 1 p. 56.

[287] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13.

[288] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13.

frameworks, it could lead to further fragmentation, thereby increasing the costs of putting innovative AI-solutions and reducing cross-border trade in the Single Market. It is important that companies know their liability risks throughout the value chain and can reduce or prevent them and insure themselves effectively against these risks[289].

234 In the field of automated vehicles, these issues are mitigated by the existence of the mandatory third party motor liability insurance.

235 In one of the first incidents involving automated driving features, a Tesla Model S with a driver using Tesla Autopilot collided with a trailer at an uncontrolled intersection in Florida in May 2016, resulting in the driver's death. The preliminary investigation was closed by NHTSA in January 2017 to conclude that it found no defects in the vehicle. This fatal accident suggests two critical issues:

- First, even an accident caused by automated vehicle of SAE Level 2 required more than half a year for the authorities to close the preliminary investigation, which indicates that more complexity of advanced automated driving systems may lengthen the term to clarify the root cause of traffic accidents.
- Second, depending on the legal framework and the circumstances, the victim(s) of the automobile accident may not be compensated for the loss in the meantime, suffering unexpected financial difficulties and mental distress, therefore deteriorating consumer acceptance of AV's[290].

236 Therefore, careful consideration towards the frameworks of not only liability but also the relief of victims of accidents is essential to nurture consumer acceptance of connected and automated vehicles[291].

237 Policymakers, in collaboration with researchers, manufacturers and deployers, should establish clear and fair legal rules for assigning liability in the event that something goes wrong with automated vehicles. This could include the creation of new insurance systems. They should also ensure a fair distribution of the costs of compensation[292].

238 In its Automated and Electric Vehicles Act of 2018, the United Kingdom has enacted that automated vehicles must hold an insurance where the insurance company has to pay compensation for any loss/damages caused by an automated vehicles when its automated driving system is performing the dynamic driving task. The insurance company can then in turn file secondary claims against anyone (else) liable against the victim.

239 Some voices are calling for a shift towards a no-fault insurance framework for damages resulting from automated vehicles with an appropriate insurance framework[293]. A compulsory no-fault insurance,

[289] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, § 3 p. 13.

[290] World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019, p. 10.

[291] World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019, p. 10.

[292] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, Recommendation 20, p. 62.

[293] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.2.1 p. 92.

supplemented by a shift of liability to the manufacturer, has also been suggested[294] (see also Appendix A § 6.2 below).

240 In addition, the potential issue stemming from accidents involving uninsured automated vehicles should also be assessed and addressed. Victims of accidents caused by uninsured automated vehicles should not be treated less favourably than insured automated vehicles. If necessary, the existing frameworks and funds should be modified in order to provide compensation for victims of uninsured automated vehicles[295]. The existing fund under the Motor Vehicle Insurance Directive[296] that compels Member States to set up compensation funds for victims of accidents caused by unidentified or uninsured vehicles might serve as a basis, for instance.

7.2 Reversal or alleviation of the burden of proof

Issue: Under the current Product Liability Directive ("**PLD**") framework, proving the existence of a defect in the context of products involving artificial intelligence (and thus also for automated vehicles) may be difficult[297], which might be problematic for victims due to, amongst others, information asymmetry.

Proposed solution: To ensure that strict liability be a vehicle of social policy, geared toward consumers'/victims' protection, the burden of proving defect and causation should be reversed and borne instead by the industry operators[298]. An alternative solution might be to alleviate the burden of proof in favour of the consumer/victim[299].

Explanation: In allocating liability amongst actors, causation should be seen as a key element. As a result, when determining the burden of proof, it should be considered which party is best positioned to understand the cause of a risk and to gather evidence on what (e.g. the end user has a better knowledge on the damage suffered; while the producer or service provider of the service provided or product manufactured has more knowledge on their characteristics, functioning, absence of defects, need for updates etc.)[300].

---

[294] PUNEV, Autonomous Vehicles: The Need for a Separate European Legal Framework, European View 2020, Vol. 19(I) 95-102, 2020, p. 99.

[295] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.20.

[296] Art. 7 to art. 11 MID.

[297] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55.

[298] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 80.

[299] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 56 and the quoted reference.

[300] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 79; see also European Commission (Expert Group on Liability and New Technologies - New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, p. 51 as well as European Parliament, Artificial intelligence and

241 The PLD requires injured parties to prove that the product was defective and that it caused the injury. This is not necessarily problematic, depending on the criterion to determine causality and the standard of proof used to determine the defect[301].

242 Outside the AI context, proving the defect may pose difficulties for the consumer because of "the technical complexity of certain products, the high cost of expert evidence, the parties' unequal access to information (particularly about the production process) and the fact that some products are not retrievable after they have been used[302].

243 In the example of AVENUE experimentations, access to vehicle data was problematic as only the vehicle manufacturer had access to data of the automated minibuses, which is an important issue already discussed above that should be discussed and regulated (see § 6.1 above).

244 National courts have developed ways to facilitate or lower the burden of proof in such situations, for instance:

- by including disclosure obligations for the producer;
- by allocating the costs of experts' opinions[303],
- by allowing *prima facie* evidence[304];
- by applying the theory of *res ipsa loquitur*[305, 306].

civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.3 p. 110.

[301] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted reference.

[302] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted reference.

[303] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted references.

[304] *Prima facie* evidence, which is based on a typical set of facts that, according to the general experience of life, justifies the assumption of a certain cause or consequence, is admissible. The claimant still has to prove (in compliance with ordinary evidentiary standards) some links in the alleged chain of causation, but is spared proving all of them if experience has shown that the missing link is typically given in other similar cases. The defendant can rebut this by proving (again adhering to traditional standards) that there is a (mere) genuine possibility of a turn of events deviating from the one expected according to said experience, so that the missing link may indeed have not been given in the present case. In this case, the claimant must meet the full burden of proof for establishing the facts underlying its claim or defense, because the *prima facie* evidence rule is no longer available.

[305] *Res ipsa loquitur* is the inference of negligence from the very nature of a harmful event, where the known circumstances are such that no other explanation for the accident seems possible than negligence within the sphere of the defendant, who had been in full control of the incident that may have caused the harm. A case of application is for instance when a hospital (defendant) is called for liability where the patient (claimant) was found having surgical instrument in his body after a surgery.

[306] European Commission (Expert Group on Liability and New Technologies - New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, p. 50 and the quoted references.

245 For AI products, proving a defect may nevertheless be difficult, given that the uncertainty about what constitutes a defect in an advanced AI system. Depending on the definition of a defect, users may be asked to show that harm was the result of a flaw in the AI device and not of its autonomous decision-making[307].

246 Causality is governed by national rules, given that the PLD does not define a causal relationship. Proving causality in the context of AI harm may be difficult, especially if some human supervision was still required. The injured party may have difficulty showing that the AI system, not his negligence, caused the harm[308].

247 Besides, the assessment of the causal link will often require expert advice, the cost of which may discourage injured parties from suing[309].

248 Reversing the burden of proof has been proposed to facilitate claims for parties injured by highly complex technologies. However, this would significantly alter the current distribution of risks to the detriment of the manufacturers. It would also depart sharply from the current principles of the PLD[310].

249 Given that AI systems will be equipped with event logging or recording systems, victims may moreover be able to get access to better data about the cause of an accident than they used to[311]. This will be the case of automated vehicles equipped with event data recorders, but the feasibility and efficiency of these solutions are not clear at the moment due to the lack of real-world experience.

250 According to some scholars[312], a better alternative to the reversal of the burden would be to facilitate the burden for the injured party by the introducing of a lower standard of proof. This could be accompanied by evidence disclosure duties, cost-shifting rules for expert advice, or – as far as data protection rules permit – requirements to collect data about the functioning of the system, allowing them to retrace possible causes for an error at a later stage.

251 In any case, promoting any specific measure relating to the burden of proof might be carefully assessed as it might run the risk of interfering with national procedural laws[313]. In addition, the practical implications might also need to be assessed, as the damages might be sufficiently compensated under the Motor Vehicle Insurance Directive.

---

[307] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted references.

[308] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted references.

[309] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted references.

[310] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted references.

[311] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 55 and the quoted references.

[312] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 5.2.5 p. 56 and the quoted references.

[313] European Commission (Expert Group on Liability and New Technologies - New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, p. 51.

7.3 Provide solutions to the complexity of value chains involving connected and automated vehicles

Issue: Connected and automated vehicles contain many complex interfaces, sensors, communications channels as well as multiple software interacting together. They will also integrate complex IoT environments where many different connected devices and services interact. Combining different digital components in such complex ecosystem with a plurality of actors involved can make it difficult to assess where a potential damage originates and which person is liable for it[314].

Proposed solution: Forms of shared responsibility instead of individual responsibility could be envisaged. The operators deemed liable in the first place should be those best positioned to *ex ante* (a) control, (b) minimize or reduce and (c) insure against the risks associated with the use of the technology, to grant prompt and adequate compensation *ex post*[315]. A shift towards liability of vehicle manufacturers should also be envisaged[316] and discussed.

Explanation: As recognized by the European Commission, there is a risk of uncertainty as regards the allocation of responsibilities between different economic operators in the supply chain. The European legislation on product safety allocates the responsibility to the producer of the product placed on the market, including all components and AI systems. But the rules can for example become unclear if AI is added after the product is placed on the market by a party that is not the producer. In addition, European product liability legislation provides for liability of producers and leaves national liability rules to govern liability of others in the supply chain[317].

252 The deployment of automated vehicles and minibuses will imply many stakeholders involved in the creation of both hardware and software components of the vehicle as well as digital services when operating. This might result in difficulties determining the origin of a damage and the stakeholder liable for it.

253 Due to their central position in design and development of vehicles, as well as to their position in the architecture related to data access, manufacturers of automated vehicles and minibuses seem in a

[314] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, European Commission, Brussels 19 February 2020, COM(2020) 64, p. 14.

[315] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 79.

[316] See BERTOLINI/RICCABONI, Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules, European Journal of Law and Economics (2021) 51:243–284, 20 November 2020; see also PUNEV, Autonomous Vehicles: The Need for a Separate European Legal Framework, European View 2020, Vol. 19(I) 95-102, 2020, p. 99.

[317] European Commission, White paper on Artificial Intelligence – A European approach to excellence and trust, Brussels 19 February 2020, COM(2020) 65 final, p. 14.

position where they could be placed in the first line of liability[318], with the possibility for them to have recourse against other responsible stakeholders in a second step.

254 Companies such as AV manufacturers and tech companies have been depicted as becoming the actual "drivers" and "operators" of the automated vehicles they operate. As a matter of fact, the company behind an automated driving system drives via its machine agents (namely the combination of hardware and software that enables automated driving) and its human agents (namely the remote assistants/supervisors who support and supplement that hardware and software). Indeed, while "automated driving system" in SAE J3016's narrow technical sense refers only to that hardware and software, in a broader sense this "system" might also properly encompass these human roles[319].

255 In its report, the Expert Group on Liability and New Technologies recommends a strict liability regime that lies with the person in control of the risk connected with the operation of emerging digital technologies and benefitting from their operation (i.e. the operator). In the situation where two or more operators can be identified strict liability should lie with the operator who has the more control between the person deciding and benefitting from the use of the product and the person continuously defining the features of the technology and providing continuous backend support[320]. In line with this, vehicle manufacturers or tech companies operating a fleet of automated minibuses could be considered as having more control over the vehicle than the public transport operator and/or (if applicable) the safety operator respectively the remote supervisor, and thus should assume liability for damages resulting from their use[321].

256 From a public relations point of view, this approach has already been followed by some European manufacturers, such as Volvo, which announced early in 2015 that it will "accept liability for its self-driving cars"[322]. After having obtained the first approval of its SAE Level 3 ALKS technology (in application of UN Regulation 157), Mercedes Benz also claimed in March 2022 that it will accept liability when its new Drive Pilot system is engaged[323], although under conditions. How these declarations will apply in practice in real-world cases still remains to be seen assessed.

---

[318] As suggested by PUNEV, Autonomous Vehicles: The Need for a Separate European Legal Framework, European View 2020, Vol. 19(I) 95-102, 2020, p. 99; see also BERTOLINI/RICCABONI, Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules, European Journal of Law and Economics (2021) 51:243–284, 20 November 2020.

[319] See SMITH, On remote driving, Blog post dated 16 May 2022, retrieved under https://cyberlaw.stanford.edu/blog/2022/05/remote-driving (last consultation 31 August 2022).

[320] European Commission (Expert Group on Liability and New Technologies – New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, § 5 p. 39 et seq.

[321] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.2 p. 92.

[322] https://www.forbes.com/sites/jimgorzelany/2015/10/09/volvo-will-accept-liability-for-its-self-driving-cars/ amongst other press clippings (last consultation 31 August 2022).

[323] https://insideevs.com/news/575160/mercedes-accepts-legal-responsibility-drive-pilot/ amongst other press clippings (last consultation 31 August 2022).

7.4 Revise existing legal definitions and concepts

Issue: The digitalisation of transports and the development of AI have raised various points of discussions in relation with civil liability, amongst others relating to definitions included in the liability framework and in the PLD in particular, such as:

- The definition of a product;
- The definition of a producer;
- The definition of a defect;
- The definition of a damage;
- The timeframe of product liability.

Proposed solution: In the context of connected and automated vehicles, these definitions should be discussed, answered at a political level and regulated accordingly. The opportunity of providing solutions through a dedicated sector specific legislation (instead of the PLD) should also be assessed and discussed.

Explanation: According to recent publications[324], the legal framework of product liability should be revised in order to deal with the challenges of software and digitalization, in respect of all products, not only for connected and automated vehicles[325]. Thus, to ensure technology-specific regulation, the PLD shall constitute a general and residual rule, covering both traditional products and new technologies, while narrow tailored regulations should be adopted at the European level, for specific classes of applications[326].

257 In case of AV's, different bodies of law may overlap – the PLD and traffic liability – in case of accidents caused by automated driving systems up to SAE Level 4 that still allow, at least partially, for user's control of the dynamic driving task. Thus, imposing duties to insure is insufficient, so long as it is not clarified which party bears what risk, and who is to be held liable for each kind of accident[327].

258 As mentioned above, the high number of potentially responsible parties, the strong interplay of the CAV components and the high level of technicality required to analyse information data and technical evidence submitted in proceedings exacerbate the PLD criticalities. Thus, proving the causal nexus in such a scenario

[324] Amongst others: European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 7 p. 65 and the quoted references; LOHMANN, Ein zukunftsfähiger Haftungsrahmen für Künstliche Intelligenz, in: HAVE 2021 S. 111, Schulthess Juristische Medien AG, p. 111 et seq., § VI p. 119.

[325] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 16.4 p. 277.

[326] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.3 p. 47.

[327] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.3 p. 110.

will most likely become disproportionately burdensome. As a consequence, litigation costs and time increase, thus hindering an effective access to justice[328].

259 Furthermore, even if the attribution of liability and the causal nexus can be determined, the diverse producers' defences provided by Art. 7 PLD substantially reduce a victim's incentive to claim damages based on the PLD[329].

260 As indicated by existing case law in other jurisdiction (such as the United States of America and China), access to data and its evaluation are critical for establishing whom, between the driver/safety operator and the producer, should be held responsible. The duty to record data (through a black box i.e. logging) and make it available to the victim is relevant, but insufficient[330] for the reasons seen above (complexity, costs etc.).

261 Under the PLD, the fact that automated vehicles and minibuses may change and be altered during their lifecycle should also be taken into account and implemented. The consequences of changes/software updates brought to the automated vehicles and minibuses and the potential evocation of "later defect defence" and "development risk defence" by vehicle manufacturers, as well as the consequences of the failure to implement changes/updates by the owner of the automated vehicles and minibuses should be assessed[331].

[328] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.3 p. 110.

[329] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.3 p. 110 and quoted references.

[330] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.3 p. 110.

[331] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, European Commission, Brussels 19 February 2020, COM(2020) 64, p. 14.

8 Recommendations related to traffic and communication infrastructure

8.1 Definition of minimum standards and harmonisation

Issue: In order to ensure cross-border operations and interoperability, standards and harmonisation are required as regards road and communication infrastructure.

Proposed action: Proceed to discussions on the scope of a Europe-wide harmonisation of the road infrastructure (e.g. definition of a minimum set of standards for road traffic signs, markings or digital infrastructure) and the communication and interaction of automated vehicles with the infrastructure (V2I)[332].

Explanation: In the case of automated functions with Vehicle-to-Vehicle (V2V) or V2I communication, it is absolutely necessary to specify the communication interfaces before market launch, to ensure interoperability between vehicles from different manufacturers and in different countries. For these new functions, appropriate requirements must be defined[333].

262 Automated driving systems are dependent on information and their functionality depends on the necessary and available information. The technical requirements on infrastructure increases with the level of automation. If necessary information is missing, functional restrictions occur[334].

263 For the binding and reliable provision of decision-relevant data for automated driving systems, there is a need for a European legal framework coordinated across Member States and far-reaching investments. In order to enable automated driving across national borders, the harmonisation of the safety-relevant infrastructure (such as, amongst others, road markings, signalisation etc.) is necessary. To achieve this, harmonisation should be as global as possible, or at least EU-wide, including common standards[335].

264 The focus should lie on following questions:

- Which infrastructure is absolutely necessary and therefore represents a minimum requirement?
- Which infrastructure can provide support and is considered as a supplementary measure?

[332] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 9.
[333] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 8 and the quoted reference.
[334] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 8.
[335] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 8.

- How can the existing infrastructure be further developed and what requirements are placed on the quality of the infrastructure[336]?

265 In principle, and not least because of the European and international dimension of the issue, technical solutions to be preferred are the ones that require as little intervention in the infrastructure as possible and that can be used flexibly. At the same time, the road infrastructure must not become the limiting factor. The comprehensive compliance with or implementation of the existing standards of the traffic infrastructure is an important building block for the deployment of automated vehicles and minibuses[337].

8.2 Road equipment characteristics and inspection procedures

Issue: With regard to the inspection procedures of the road equipment for automated vehicles, the need for adaptation cannot be stated with certainty at present[338] due to a lack of knowledge, which highlights the necessity to carry on AV experimentation.

Proposed actions:

- In particular, the following aspects need to be clarified:
  - Relevant characteristics and minimum qualities for (automated) machine detection (of road equipment);
  - Development of procedures for network-wide quality control and digitalisation of road equipment;
  - Location of road equipment elements in digital maps, as well as their updating[339];
- In addition, appropriate inspection procedures of the equipment must be prescribed;
- Automated driving will mean that the principle of independent inspections might have to extend to the traffic infrastructure (and not only to the automated vehicles)[340].

Explanation: For the foreseeable future, and depending on the use cases and operational design domains, lane markings will be a crucial element for the transverse positioning of automated vehicles. Certain requirements must be met with regard to the quality and availability of lane markings for a proper machine detection. Wear, abrasion, dirt and critical environmental conditions such as fog, snow, rain,

[336] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 8.

[337] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 8 and the quoted reference.

[338] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 11.

[339] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 11.

[340] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 10.

varying light conditions must be taken into account in addition to the different sensor types (e.g. videocameras, LIDAR's etc.)[341].

266 For the further development of existing procedures and regulations, there is an urgent need to gather basic knowledge about the requirements of new markings. The implementability in practice must also be taken into account, for example, the feasibility and cost for the comprehensive provision of markings with minimum quality as well as their monitoring[342].

8.3 Ensure safe interaction channels with other road users

Issue: Automated vehicles will increasingly take part in road traffic, together with conventional vehicles. Whereas with conventional vehicles the person driving can take over communication with other road users by means of gaze/gestures and with the support of on-board devices such as lights, horns or indicators, this human component is missing to automated vehicles[343].

Proposed actions: Investigate and development of procedures (e.g. best practices) for the safe interaction between automated vehicles and other road users, especially VRU's such as pedestrians and cyclists[344].

Explanation: Today, the safe communication between drivers and other road users for various situations that can be safety-critical is not an issue. An example is a pedestrian at a zebra crossing, who tries to assess whether an approaching vehicle has recognised him or her and is going to stop or not. In conventional vehicles, this "safeguarding" is done, for example, by means of eye contact between the pedestrian and the driver, with an additional hand signal from the person driving. Many communication scenarios between road users also function without eye contact or gestures[345].

267 If the driver disappears as a communication sender or receiver, the technology must take over this role in order to continue to ensure road safety and traffic flow. Various research projects are already investigating different possibilities, such as communication via displays[346].

268 For communication, especially with weaker road users such as pedestrians and cyclists, a solution that is easy to understand, as uniform as possible, accepted and adapted to the needs of the user groups will be

[341] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 10.
[342] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 10.
[343] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 9.
[344] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 12.
[345] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 9.
[346] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 10 and the quoted reference.

required in the future, whereby digital and networked infrastructure elements will continue to be available[347].

8.4 Creation of "Digital twins" of the road traffic infrastructure

Issue: As regards higher levels of automation, a digital representation of the road traffic infrastructure should be created – a so-called "Digital twin". This "Digital twin" must store various conditions and information relevant for the vehicle guidance.

Proposed actions:

- From the beginning, it should be aimed to have:
  - a European-wide availability of the "Digital twin" as well as
  - an international standard for its design;
- In addition, European-wide specifications for the continuous securing of updated and correct contents of the digital twin should be created;
- The "Digital twin" must be suitable for cross-border traffic, so that foreign vehicles harmonise with the domestic twin, and vice versa[348].

Explanation: The introduction of automated vehicles will very likely trigger numerous tasks related to the traffic infrastructure. Especially with regard to higher levels of automation, a digital representation of the infrastructure should be created – a "Digital twin". This "Digital twin" must include traffic regulations as well as structural, operational and other conditions relevant for the vehicle guidance. This applies, for instance, to lane markings as well as traffic signs, traffic lights, variable traffic signs and their sensors[349].

269 This "Digital twin" could be created using a highly accurate, layered digital reference map. It could then often replace or at least supplement a costly retrofitting of the physical infrastructure. For instance, by displaying markings on the digital map, it could create the required redundancy for the detection of markings by the vehicle. This would extend the horizon of knowledge beyond the range of the sensors[350].

270 There is an increased need to create regulatory requirements for the underlying processes and structures. Standards for functional security, but also for trustworthiness must be taken into account, for example the accuracy of the map information or the handling of errors. Furthermore, it is necessary to establish procedures and a precise distribution of tasks for the continuous updating, as well as the involvement of road operators, road traffic authorities and traffic control centres. This is of high relevance for safety.

[347] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021, § 3.1 p. 10.

[348] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 11.

[349] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 10.

[350] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 10.

Therefore, requirements for the provision of relevant information and processes have to be developed, especially regarding the qualification of stakeholders and the quality and verification of information[351].

271 Various scenarios are conceivable for the establishment of a digital twin. The focus can either be on the time horizon for implementation, on the benefits for automated vehicles, on the need for a twin due to little developed real infrastructure or on the costs[352].

272 For instance, sections of routes that are easy to create due to their lower complexity (rural roads for instance) could first be doubled in the "Digital twin". The "Digital twin" could also be created first for routes where the first use cases of automated driving can realistically be expected (for example the deployment sites of automated minibuses or highways where the use of ALKS is or will be allowed). While it is assumable that the "Digital twin" would be of great use in very complex traffic environments (e.g. in the centre of cities), this would be associated with high costs. An optimal implementation scenario therefore still needs to be determined[353].

273 An important issue currently, amongst others faced during the AVENUE experimentation, is the lack of standards and interoperability between high definition maps of different vehicle manufacturers, as well as the complexity of updating these maps.

8.5 Communication infrastructure

Issue: The current regulations cannot ensure whether a radio product in daily use or in the current installed state guarantees the desired connectivity to another subscriber. Various factors can lead to significant operational failures. A number of private certification organisations[354] are currently endeavouring to cover such enormously important aspects in use by means of supplementary specifications. In addition, network operators and service providers are defining their own requirements[355].

Proposed actions:

- Internationally harmonised regulatory requirements must be created to demonstrate interoperability between different components if they are produced by different manufacturers;
- Regulations are also needed to verify the performance of the antennas used – especially in combination with on-board units of automated vehicles;
- Periodic inspections of the communication infrastructure will become mandatory;

[351] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 10.

[352] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 11.

[353] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.2.3 p. 11.

[354] For instance the Global Certification Forum (GCF), PTCRB, Bluetooth Special Interest Group (Bluetooth SIG), Wi-Fi Alliance amongst others.

[355] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.1 p. 6.

- The verification of the software versions used has to be regulated at international level. There is a need for international harmonisation in the version of the interface used and the version of the communication protocol[356].

Explanation: For the components of the communication infrastructure and for the frequencies used, the manufacturer declares compliance with applicable standards. If these conditions are fulfilled, the component is marked in Europe with the CE mark. The Radio Equipment Directive ("**RED**")[357] forms the basis of these proceeding[358].

274 Accredited test laboratories can be used to demonstrate compliance with standards. The basic communication protection objectives (spectrum, electromagnetic compatibility, health and safety) are covered by standards listed in the RED[359].

275 If only drafts of new standards are available when modern technologies are introduced, authorised test laboratories support the manufacturer's declaration of conformity with their expertise. For example, they point out standards that were not directly created for the new products and technologies, but are applicable in the case at hand[360].

276 All requirements that go beyond the current regulations must be agreed between the manufacturer and its purchaser (e.g. network operator, service provider). This also applies to security-relevant applications that are not covered by other regulations[361].

277 For future automated and networked mobility, it must be ensured that communication is available at all times with sufficient performance and as far as possible without errors. This must also be ensured over the entire intended period of use of the communication-relevant vehicle and infrastructure components. For this purpose, periodic inspections will be absolutely necessary in the future[362].

[356] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.1 and § 2.1.3 p. 7.

[357] Directive 2014/53/EU of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment.

[358] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.1 p. 6.

[359] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.1 p. 6.

[360] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.1 p. 6.

[361] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.1 p. 6.

[362] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 2.1.3 p. 7.

9 Recommendations related to spatial planning

Issue: The use of automated vehicles and minibuses might considerably change the architecture of existing roads and cities, but this question has hardly been studied yet.

Proposed solution: Considering the medium to long-term transition period leading toward automation, it is critical to reflect upon:

- which changes could be implemented irrespective of vehicle automation and which changes need further investigation;
- short-term issues that cities should address include:
  - strategies for curb management;
  - prioritizing pickup and drop-off zones over on-street parking;
  - increased cycling and micromobility lanes, and
  - enhancing the integration between shared mobility and transit networks[363].

Explanation: Automated vehicles tend to require less lateral clearance, so lane widths could become smaller. Since automated vehicles, used appropriately, will lead to fewer vehicles with higher mileage, the demand for parking spaces is also likely to decrease[364]. This regain of urban space from parking facilities might be allocated to other uses in the future[365].

278 According to a recent study for Switzerland, the risk of urban sprawl created by vehicle automation can be regarded as very small in this country[366].

279 Other studies have shown that in the urban regions considered[367], the changes would have an uneven impact from the city core to the suburbs[368].

280 In order to concretise potentials and risks of spatial development paths, further studies that take into account the spatially differentiated modes of impact of automated vehicles and show the extent of

[363] MARTIN/BRUCK/SOTEROPOULOS, Transformations of European Public Spaces with AVs, Mitteregger et al. (Hrsg.), AVENUE21. Politische und planerische Aspekte der automatisierten Mobilität,§ 3 p. 176.

[364] HUONDER/RAEMY, Autonomes Fahren, Rechtlicher Anpassungsbedarf: ein Werkstattbericht, 4. Zürcher Tagung, Dike Verlag AG, Strassenverkehr 1/2016, p. 48.

[365] International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017, p. 8.

[366] Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 6: Spatial impacts, SVI 2017/044, 1680, August 2020, p. 16.

[367] Namely Atlanta and Singapore.

[368] BRUCK/SOTEROPOULOS, Automatisiertes und vernetztes Fahren: Berücksichtigung des lokalen, räumlichen Kontextes und räumliche Differenzierung, Mitteregger et al. (Hrsg.), AVENUE21: Politische und planerische Aspekte der automatisierten Mobilität, pp. 7-16, § 4 p. 14 and the quoted references.

potential effects in different urban structures and areas should be conducted. This does not only refer to the changes in land use or parking demand, but also to potential changes in public space or transformations of certain types of areas[369].

10 Recommendations related to the issuance of driving permits

Issue: The upcoming use of automated vehicles of SAE Level 3 to 5 implies new use cases and scenarios that are currently not instructed nor tested when granting conventional driving permits.

Proposed solutions: Various questions arise with regards driving permits and the development of automated vehicles:

- For new drivers, it should be examined whether their training should generally be supplemented with, for instance, a module that teaches the particularities of AVs human machine interfaces, i.e. how to deal with handover requests, the criticalities of regaining control of the dynamic driving task when the automated driving systems is engaged etc.;
- For persons already holding a driving permit, it should be assessed if they should complete an additional training in order to be allowed to use automated vehicles;
- The introduction of a separate driving permit category for automated vehicles might also be questioned;
- The impact of automated vehicles on drivers with restrictions (such as a driving permit holder requiring eyesight correction or prosthetic devices for the limbs, persons only being able to drive automatic transmission etc.) should also be assessed, as automated vehicles might be able to alleviate or even remove these restrictions;
- It should also be discussed and defined which other activities than driving are allowed when the dynamic driving task is performed by an automated driving system[370].

Explanation: According to the European Committee on Crime Problems, the introduction of a general obligation to train users of AI systems could be the subject of negotiations amongst Member States, with for instance driving schools being required to provide training in automated vehicles as part of the process of obtaining a driving permit[371].

[369] BRUCK/SOTEROPOULOS, Automatisiertes und vernetztes Fahren: Berücksichtigung des lokalen, räumlichen Kontextes und räumliche Differenzierung, Mitteregger et al. (Hrsg.), AVENUE21: Politische und planerische Aspekte der automatisierten Mobilität, pp. 7-16, § 4 p. 14.

[370] See Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 3.80 p. 52.

[371] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.4 p. 14.

281 The French Ministry of Transports considers that in order to enable the driving of conventional vehicles and of vehicles with partial, then later quasi-total "delegation" of driving (i.e. automation), it will be essential to add the necessary elements ensuring a proper knowledge of new technologies equipping these vehicles and to verify their proper use and control[372].

282 In relation to this control, various approaches are possible. They need to be explored in greater depth, in view of the continuous evolution of technology and in particular the option of profoundly modifying the training of young and new drivers. The content of the training and, therefore, of the driving tests has to be adapted in order to:

- enable them to drive vehicles with increasing levels of automation;
- make them capable of regaining control of the said vehicle at the request of the system and even – and this is a more 'acute' case to be managed, and managed well – in the event of an emergency[373].

[372] Ministère de la transition écologique et solidaire (France), Ministère chargé des transports, Développement des véhicules autonomes, Orientations stratégiques pour l'action publique, Un an d'actions publiques, Mai 2018 – Avril 2019, p. 39.

[373] Ministère de la transition écologique et solidaire (France), Ministère chargé des transports, Développement des véhicules autonomes, Orientations stratégiques pour l'action publique, Un an d'actions publiques, Mai 2018 – Avril 2019, p. 9.

11 Recommendations related to criminal liability

Introduction

283 Criminal law issues fall within the scope of the exclusive competence of each Member State and will thus be dealt with on at national level[374]. Coordination and exchange of information between states is nonetheless desirable, as some Member States such as France[375] have already enacted criminal law provisions related with the use of automated vehicles and will therefore gain knowledge in this field quicker than other countries.

11.1 Investigate and define potential new criminal offences and provisions

Issue: The emergence of automated vehicles with new use cases comes along with potential new criminal offences that can be committed during connected and automated driving (intentionally and by negligence). In accordance with the cardinal "*nulla poena sine lege*"[376] principle, criminal offences need to be precisely defined in order to be enforceable.

Proposed solution: Proceed to researches related to potential new offences related to connected and automated driving and define them, in order to enact them in criminal provisions. Collect feedback (for instance through the dedicated AV-platform mentioned above or other institutions) on new undesirable behaviours linked with automated vehicles.

Explanation: The "*nulla poena sine lege*" principle states that a person cannot be punished for doing something that is not prohibited by law. This principle is accepted and codified in modern democratic states as a basic requirement of the rule of law[377].

284 The existing criminal framework related to conventional driving with a human driver behind a steering wheel might become at least partially unfit, as it is based on normative principles developed during the pre-digital era and needs to be amended (similarly to the issues described above for road traffic rules).

---

[374] PUNEV, Autonomous Vehicles: The Need for a Separate European Legal Framework, European View 2020, Vol. 19(I) 95-102, 2020, p. 97.

[375] "*Ordonnance no 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation*" (in English: Ordinance no 2021-443 dated 14 April 2021 on the criminal liability in case of use of a vehicle with "delegated driving functions" and its conditions of use).

[376] "*No penalty without law*".

[377] https://en.wikipedia.org/wiki/Nulla_poena_sine_lege (last consultation 31 August 2022).

285 Certain countries have already begun tackling this issue with studies (such as the reports published beginning of 2022 by the Law Commission of England and Wales and the Scottish Law Commission[378]) or by enacting provisions related to criminal liability (for instance Sweden[379] or France[380]).

286 As examples of offences, the European Committee on Crime Problems has mentioned the possibility of dangerous interferences with road traffic by hacking[381]. The Law Commission of England and Wales and the Scottish Law Commission have also suggested to create specific criminal offences related to the breach of the "duty of candour"[382], amongst others where misrepresentations and non-disclosure of stakeholders have implications for safety[383].

287 Criminal offences might also be defined against other road users in their relation with automated vehicles if, for example, they take advantage of the defensive programming of automated vehicles to gain an advantage in the road traffic[384] or if they maliciously "test" the reaction of automated vehicles by throwing various objects in front of the vehicle (as it has sometimes been encountered during AVENUE experimentations). Further examples will be given in the next section (see N 294 below).

288 In addition, for SAE Level 5 automated driving systems, the question of whether a non-human entity, namely the AI responsible for driving the vehicle, should be subjected to criminal law liability, perhaps in a similar way than a corporation may be liable as a "legal person", should be investigated, as this would have complex conceptual and legal implications[385].

289 From a procedural point of view, as mentioned above, automated vehicles generate valuable data while driving which can be of interest for law enforcement and criminal investigations. Questions arise as to whether the vehicle's data can be used as evidence in criminal proceedings. For instance if an automated vehicle creates an accident when the ADS was performing the dynamic driving task, can the vehicle's data be used as evidence against the human driver/owner (in light of the *nemo tenetur se ipsum accusare* principle[386]). In addition, the credibility of the sensors that process the data or their reliability as evidence

---

[378] See Chapter 11 of the joint report of the Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022.

[379] BJELFVENSTAM, The path to automated driving – market introduction (SOU 2018:16), Report presented to the Swedish Minister for Infrastructure on 7 March 2018, Summary in English, § 3f p. 4.

[380] See Ordinance no 2021-443 dated 14 April 2021 on the criminal liability in case of use of a vehicle with "delegated driving functions" and its conditions of use, Chapter 1, Art. L. 3151-4 et seq.

[381] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.2 p. 13.

[382] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 11.1 et seq. p. 209.

[383] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 11.14 et seq. p. 212.

[384] HUONDER/RAEMY, Autonomes Fahren, Rechtlicher Anpassungsbedarf: ein Werkstattbericht, 4. Zürcher Tagung, Dike Verlag AG, Strassenverkehr 1/2016, pp. 46-55, p. 54.

[385] Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Rapporteur Mr. Ziya ALTUNYALDIZ, Legal aspects of "autonomous" vehicles, Doc. 15143, 22 September 2020, N 23 p. 9.

[386] "No one is bound to incriminate himself".

might also pose questions, as the traditional procedural provisions might not necessarily be fit to adequately assess the reliability and credibility of these new digital evidences[387].

11.2 Potential shift towards corporate criminal liability

Issue: Depending on the frameworks, the question of criminal liability in case of personal injury or damage to property should require attention and amendments. Similarly to civil liability, a (potential) shift in liability might arise towards the vehicle manufacturer, the software developer and the vehicle owner/deployer (amongst others) in the future, since no human driver (mutated into a mere passenger) will perform the dynamic driving task. As of today, the human driver of a vehicle is often the primary addressee of criminal offenses.

Proposed solution: Investigate the impact of automated vehicles (e.g. with the disappearance of the figure of a human driver) and adapt this factual evolution into the criminal legislation, amongst other by defining duties of care for the manufacturer of automated vehicles, the software developer, the owner/deployer and other stakeholders.

Explanation: In most Member States, criminal law is generally considered to relate to the conduct and intentions of humans only, whether natural persons or individuals acting on behalf of entities (corporate liability)[388]. As regards criminal provisions dedicated to road traffic, corporate liability seems to have only a small room, with most provisions directed towards infringements committed by a natural person.

290 Because they are so complex, automated vehicles (and all high-tech systems in general) are apt to be misunderstood or insufficiently apprehended by designers, manufacturers, regulators and users, obliging all the parties concerned to be aware of their respective rights and duties. In this context, criminal liability deriving from situations where AI systems cause serious harm to humans needs to be made clear by unambiguous procedural safeguards and well-defined rule of law principles[389].

291 The existence and development of artificial intelligence raises the question whether a new approach to criminal liability is needed, in cases where the offence is committed when the robot acts completely

[387] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 1.4 p. 7.

[388] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 1.3 p. 6.

[389] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 1.3 p. 6.

autonomous and/or the user has complied with all instructions, but the specifics of AI employment lead to harm[390].

292 Taking AI as an acting counterpart into consideration when allocating criminal liability, at first blush, conflicts with basic principles of criminal law, which has been tailored for human action. However, if the human driver has vanished from the driver's seat entirely, the now passenger can no longer be held entirely responsible for accidents caused by the vehicle[391].

293 Some want to draw a parallel to corporate liability. However the parallel is not obvious, as corporations are legal persons in all Member States, and thus liable under the law, but not competent to stand a criminal trial in all. Furthermore, in most countries, corporate criminal liability connects to wrongdoing of a human representing the corporations[392].

294 However, it seems obvious that the issue must be addressed, and the points to be discussed are: could a vehicle manufacturer or a service provider be liable, as a question of principle and if so, what level of negligence on its part and/or what degree of damage would be required in order for that provider to be criminally liable? Examples might include cases of criminal liability resulting from feeding incorrect map data or sensor information, or designing an AI system that is dangerous[393].

295 As mentioned previously (see N 254 above), the company behind an automated vehicle might be considered as driving it via its "machine agents" (namely the combination of hardware and software that enables automated driving) and its human agents (namely the remote assistants who support and supplement that hardware and software)[394]. This approach might provide a solution towards creating a criminal liability towards vehicle manufacturers, service providers etc. that have been suggested by scholars[395] and that should be discussed.

---

[390] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.2 p. 13.

[391] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.2 p. 13.

[392] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.2 p. 13.

[393] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.2 p. 13.

[394] SMITH, On remote driving, Blog post dated 16 May 2022, retrieved under https://cyberlaw.stanford.edu/blog/2022/05/remote-driving (last consultation 24 August 2022).

[395] See WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022, footnote 78 and the quoted references for Spain.

296 In this context, Member States could agree on a normative framework for the multiple forms of criminal liability that could be triggered by a combination of failures to exercise due care, resulting in an offence. This framework would then pave the way for nationwide reform of road traffic offences that currently focus on human action[396].

297 The Law Commission of England and Wales and the Scottish Law Commission have suggested the creation of a new legal actor called the Authorised Self-Driving Entity ("**ASDE**"), defined as "the vehicle manufacturer or software developer who puts an automated vehicle forward for authorisation as having self-driving features[397]" or "a partnership between the two[398]".

298 This ASDE would need to fulfill various requirements and would bear criminal liability as a corporate body[399] for new specific offenses suggested by the Law Commissions. In addition to this corporate liability, it was also recommended that "senior managers" should also be liable for criminal liability[400].

[396] Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020, § 4.2 p. 13.

[397] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 2.41 p. 20.

[398] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 2.41 p. 20.

[399] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 11.33 p. 215.

[400] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 11.33 p. 215 et seq.

12 Conclusion

299 Since the beginning of the project in 2018 and its end in 2022, the legal landscape has started to change. In 2018, only few provisions dedicated to automated driving where existing – be it at international, European or national level. In 2022, national legal frameworks dedicated to the ordinary approval and deployment of automated vehicles and minibuses are in force in Member States like France and Germany, amongst others. The European Commission has published two promising regulations regarding the type-approval of automated vehicles and minibuses in the summer 2022. At international level, important bodies like the UNECE created AV-specific working groups. The signs are therefore positive, as politicians and lawmakers have now understood the necessity of monitoring, acting and regulating this rising industry that will very likely cause major disruptions in the coming years.

300 It is indeed particularly important to act today, as evolution of technology (and its speed in particular) is always hard to predict. The crucial point is not "if" automated vehicles will circulate on European roads in the future, but "when" and "how soon". Sudden deployments might potentially occur quickly and authorities as well as the public might face a "fait accompli" that should be avoided, as it would likely results (amongst others) in legal gaps that the concerned stakeholders might leverage for their own benefits. Some voices are anticipating important deployment of AV fleets at large scale by the year 2030, when others depict only mixed traffic by 2040, with many conventional vehicles still in circulation on European roads at this date. Industrial actors are currently planning the first large and commercial deployments for 2025 and following years, as European regulations might be updated by then and the European single market be opened to larger deployment than small series in 2024.

301 In this context, the partners of AVENUE agreed and consider of utmost importance to favour public transport solutions due to their positive outcome on our future societies. This should be reflected by policymakers giving priority to these solutions, amongst others through quick and favourable lawmaking and encouraging behaviour in this particular (sub)field of the AV industry.

302 The importance of acting now is also caused by the fact that budgets for public transportation of the coming years are already being discussed and decided today. Automated vehicles and minibuses will require very important infrastructural investments and changes that should be anticipated, planned and budgeted as soon as possible in order to maximise the positive outcome of vehicle automation.

303 From a legal point of view, the need to legislate encompasses different levels and branches. From a "vertical" point of view, legislative changes are required at all levels, be it international, regional/European, national and intra-national levels. From a horizontal point of view, legal amendments are not only necessary in the specific sector of type-approval regulations, but in many other branches, as briefly presented in this document.

304 Automated vehicles and minibuses will be one of the first industry where automation, advanced robotics, AI and IoT products will deploy and change the lives of millions of people. Therefore, orienting, monitoring and guiding these changes through legislation should be guaranteed from the beginning. Policymakers acting too late might result in undesirable effects and issues.

Appendix A:

1 Overview of the international and national legislation related to the type-approval of road vehicles and road traffic rules

305 This section will provide an overview the relevant legislative framework relate to the type-approval of vehicles at international, European and national levels.

1.1 International treaties and bodies

306 Most States involved in the development of automated vehicles are contracting parties to international treaties, which, from a legal point of view, are considered to be a higher norm than their own national law. Accordingly, domestic legislation in each state may be required to conform to the respective part of the relevant international agreements[401].

307 Therefore, the most important treaties that have direct influence on the laws of European Member States and members of the European Free Trade Association ("**EFTA**") such as Switzerland and Norway will be presented in the following lines, in chronological order.

1.1.1 Geneva Convention on Road Traffic of 19 September 1949

1.1.1.1 Introduction

308 The Geneva Convention on Road Traffic ("**Geneva Convention**" or "**GC**") is an international treaty promoting the development and safety of international road traffic, by establishing certain uniform rules amongst the contracting parties. It should not be confused with the Geneva Conventions of 12 August 1949 and their additional Protocols that establish standards for international humanitarian law.

309 The Geneva Convention on Road Traffic addresses minimum mechanical and safety equipment needed to be on board and defines an identification mark to identify the country of origin of the vehicle. It was

[401] World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019, p. 5 and quoted reference.

prepared and opened during the United Nations Conference on Road and Motor Transport, held at Geneva between 23 August 1949 and 19 September 1949. The GC came into force on 26 March 1952. Initially, it had 20 signatories, this number having grown to reach 102 contracting parties currently[402].

310 The Geneva Convention replaces the "International Convention relative to Motor Traffic" signed by 40 States in Paris on 24 April 1926 that aimed to facilitate international tourism. The Geneva Convention has itself been replaced (and terminated between the contracting parties) by the Vienna Convention on Road Traffic of 8 November 1968 ("**Vienna Convention**" or "**VC**", see Art. 48 VC and Appendix A § 1.1.3 *infra*).

1.1.1.2 Overview

311 In a nutshell, the Geneva Convention fleshed out the principles enshrined in the earlier convention, in accordance with the developments of the car industry and revealed a growing concern for road traffic safety. While it did not stipulate the use of specific traffic signs (which came later along with the Vienna Convention), the Geneva Convention did require that contracting parties (i.e. states) adopt a homogeneous system of road signs and signals, and only use them where strictly necessary. The Geneva Convention did not lay down many driving rules or introduce much which was new, other than precautions to take when passing oncoming traffic, rules on priority and the use of traffic lights[403].

1.1.1.3 Art. 7 and 10 Geneva Convention

312 According to art. 7 GC, every driver, pedestrian or other road user shall conduct himself in such a way as not to endanger or obstruct traffic; he shall avoid all behaviour that might cause damage to persons, or public or private property.

313 Art. 10 GC states that the driver of a vehicle shall at all times have its speed under control and shall drive in a reasonable and prudent manner. He shall slow down or stop whenever circumstances so require, and particularly when visibility is not good.

314 Both these provisions are addressed towards a "driver", which poses interpretation questions for automated vehicles such as automated minibuses, as the driver of the vehicle *per se* is not a natural person anymore when the automated driving mode is activated, but an automated driving system performing the dynamic driving task, as discussed above (see § 2.3.1 *supra*).

1.1.1.4 Proposal of amendment and rejection

315 The Geneva Convention was supposed to be amended in 2016, similarly and in parallel to the Vienna Convention (see § 1.1.3.2 below), in order to admit systems that could affect the control of the vehicle (instead of a human driver), but the proposal has resulted in the rejection by contracting parties, due to procedural and administrative difficulties[404]. Therefore, it has not been amended since and automated vehicles might be considered to be non-compliant with these provisions.

---

[402] https://treaties.un.org/Pages/ViewDetailsV.aspx?src=TREATY&mtdsg_no=XI-B-1&chapter=11&Temp=mtdsg5&clang=_en (last consultation 31 August 2022).

[403] Opinion of the European Economic and Social Committee on "A European highway code and vehicle register", 2005/C 157/04, 28 June 2005, § 3.3 et seq.

[404] World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019, Efforts towards harmonization, p. 5 and the quoted reference.

1.1.2 UNECE Agreement of 20 March 1958 concerning the adoption of uniform technical prescriptions

1.1.2.1 Issuance of UN Regulations

316 One of the most important international treaties for vehicle registration matters is the "UNECE agreement dated 20 March 1958 concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts"[405] ("**Vehicle Parts Agreement**" or "**VPA**"), which has now been revised three times, the last time in 2017. The VPA was intended to facilitate the mutual recognition of vehicle approvals and to reduce supranational registration barriers. On the basis of the VPA, contracting parties issue regulations for vehicles, parts and equipment. These include, for example, brake systems, headlights and steering systems[406].

317 These regulations were initially called "UNECE Regulations" or, less formally, "ECE Regulations" in reference to the United Nations Economic Commission for Europe ("**UNECE**") where they were discussed and adopted. However, since many non-European states are now contracting parties to the VPA, the regulations are officially entitled "UN Regulations"[407], and often followed by their number.

318 A contracting party to the VPA may accept individual UN Regulations, but is not obliged to accept them. However, if a regulation is accepted, the contracting party is bound by it under international law and undertakes to register vehicles and parts approved by that regulation in its own country as well[408].

319 The VPA works on the principle of mutual recognition. Each contracting party designates a type-approval authority. Manufacturers submit their product to their chosen authority, to decide whether the product meets the terms of the UN Regulation. A product approved by one contracting party's authority under a UN Regulation must be accepted by all those contracting parties who have "applied the regulation". As Art. 3 para. 2 VPA states, this contracting party cannot require "any further testing, documentation, certification or marking concerning these type-approvals"[409].

320 The VPA was revised in 1995 to promote the participation of non-European states and became a global agreement. The VPA recognizes self-certification (see § 1.1.2.2 N 327 *infra*) as an alternative to type-approval and, therefore, does not preclude states whose rules and regulations are implemented through

---

[405] The full title being "Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations".

[406] BACH, Autonomes Fahren und gesetzliche Grundlagen, Universität Koblenz-Landau, Institut für Informatik, 21 July 2016, § 3.2.2 p. 8.

[407] https://www.drivingvisionnews.com/news/2011/08/29/the-end-of-the-ece-era/ (last consultation 31 August 2022).

[408] BACH, Autonomes Fahren und gesetzliche Grundlagen, Universität Koblenz-Landau, Institut für Informatik, 21 July 2016, § 3.2.2 p. 8.

[409] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.10 p. 88.

self-certification (such as the United States of America, see N 329 *supra*) from becoming contracting parties[410].

321 As of July 2022, the UN Regulations catalogue comprises more than 160 safety and environmentally relevant regulations for systems and parts. The latest UN Regulation, harmonising reverse warning sound of vehicles, was adopted in June 2022[411].

322 In the recent months, following UN Regulations related to automation of vehicles have been issued:

- UN Regulation 155 on Cyber Security and Cyber Security Management Systems ("**CSMS**", see below § 5.2.1.1);
- UN Regulation 156 on Software Updates and Software Update Management Systems ("**SUMS**" see below § 5.2.1.2);
- UN Regulation 157 on Automated Lane Keeping Systems ("**ALKS**")[412], which has been amended in June 2022 (extension of the ODD to 130 km/h and inclusion of lane changes)[413].

323 Other UN Regulations have also been updated, such as UN Regulation 79 which saw its 10 km/h limitation for autonomous systems removed in parallel with the 2016 amendment of the Vienna Convention.

324 On 21 February 2021, 64 states were contracting parties to the VPA. It now extends far beyond Europe as it includes the United Kingdom, Norway, Russia, Australia, Japan, the Republic of Korea and Switzerland, amongst others[414].

325 One of the most notable non-signatory to the VPA are the United States of America, which have their own Federal Motor Vehicle Safety Standards ("**FMVSS**") and do not recognise UN type-approvals[415]. Other significant non-signatory states are China and Singapore.

326 Nevertheless, most states, even if not formally participating in the VPA, recognize UN Regulations and either mirror the UN Regulations' content in their own national requirements, or authorize the import, registration, and use of UN type-approved vehicles, or both[416].

---

[410] The Revision 3 of the 1958 Agreement – questions and answers, Informal document WP.29-170-21, 170th WP.29, 15-18 November 2016, Agenda item 4.4.

[411] https://unece.org/sites/default/files/2022-04/ECE-TRANS-WP29-2022-88e.pdf (last consultation 31 August 2022).

[412] UN Regulation 157 initially applied for passenger cars and vans and has been extended to heavy vehicles including trucks, buses and coaches in November 2021.

[413] https://unece.org/sites/default/files/2022-05/ECE-TRANS-WP.29-2022-59r1e.pdf (last consultation 31 August 2022).

[414] https://unece.org/sites/default/files/2021-02/ECE-TRANS-WP.29-343-Rev.29.pdf (last consultation 31 August 2022).

[415] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations (last consultation 31 August 2022).

[416] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations (last consultation 31 August 2022).

1.1.2.2 Type-approval and self-certification

327 The VPA operates on the principles of type-approval. Any state that accedes to the VPA has authority to test and approve any manufacturer's design of a regulated product[417], regardless of the state in which that component was produced. Each individual design from each individual manufacturer is counted as one individual type. Once any acceding state grants a type-approval, every other acceding state is obliged to recognize that type-approval and regard that vehicle (or item of motor vehicle equipment) as legal for import, sale and use, according to the principle of mutual recognition (see N 319 *supra*).

328 Items type-approved according to a UN Regulation are marked with an *E* and a number, within a circle. The number indicates which state approved the item, and other surrounding letters and digits indicate the precise version of the regulation met and the type-approval number, respectively[418].

329 Other states are applying the so-called self-certification process, like the United States of America and Canada. The manufacturer or importer of a vehicle (or item of motor vehicle equipment) certifies — i.e. asserts and promises — that the vehicle or equipment complies with all applicable safety standards. The authorities neither approve motor vehicles or parts as complying with their standards, nor collect information from manufacturers as to the compliance[419].

330 For instance, in the United States of America, the law provides that "A manufacturer or distributor of a motor vehicle or motor vehicle equipment shall certify to the distributor or dealer at delivery that the vehicle or equipment complies with applicable motor vehicle safety standards prescribed under this chapter. Certification of a vehicle must be shown by a label or tag permanently fixed to the vehicle"[420].

331 This is generally considered as providing a more agile framework in favour of the car industry than the type-approval framework.

332 A few countries like Brazil are using a combination of self-certification and type-approval.

1.1.2.3 Non-compliance of automated vehicles with UN Regulations

333 Many of the UN Regulations stem from the conventional, "non-automated" era and are hardly adapted to automated vehicles, most of them being non-compliant because of their particular architecture and functionalities.

334 This being said, one of the latest UN Regulation 157 is dedicated to "highway traffic jam assistants" for private cars driving up to 60 km/h (and soon up to 130 km/h with lane changes), called Automated Lane Keeping Systems (considered to be equivalent of the SAE Level 3). In fact, it was the first UN Regulation related to automated vehicles (together with UN Regulations 155 and 156).

---

[417] Independent test institution may also be involved in the process, for instance by producing a report with the objective of confirming the validation of the requirements set out in the corresponding UN Regulation.

[418] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations (last consultation 31 August 2022).

[419] Congressional Research Service, U.S. and EU Motor Vehicle Standards: Issues for Transatlantic Trade Negotiations, CRS Report, 18 February 2014, p. 8.

[420] Congressional Research Service, U.S. and EU Motor Vehicle Standards: Issues for Transatlantic Trade Negotiations, CRS Report, 18 February 2014, p. 8 and quoted legal references.

335 UN Regulation 79 on Steering Equipment had to be updated during the issuance of UN Regulation 157 on ALKS. Initially, UN Regulation 79 was forbidding continuous system-based automated steering for speeds above 10 km/h, while ALKS are supposed to steer the vehicle until 60 km/h (respectively 130 km/h).

336 As UN Regulations define the conditions to be met by the various components of a vehicle in order for it to be homologated and for this homologation to be recognised internationally, in their absence, manufacturers of a new vehicle have to go through the whole homologation process with the authorities of the state in which they wish to deploy their vehicle.

337 This is what was happening until today with automated minibuses, which had to undergo a new approval process in all the countries where they are used. This implied specific requirements for each country, representing a considerable barrier to the growth of manufacturers of automated minibuses[421] and to their deployment as well. This issue shall now be (at least partially) solved through the newer legislation published recently in Germany, France and at European level in the summer 2022 (see Appendix A § 1.2.3 below).

338 Besides, UN Regulations are developed and issued within WP.1 and WP.29 (see § 1.1.5 et seq. *infra*). This has the advantage that UN Regulations can be adapted and updated to the latest technical developments more swiftly than through the heavy process of amending international treaties such as the Geneva and the Vienna Conventions.

1.1.2.4 Exemption approval

339 According to Art. 12 para. 6 VPA, a contracting party applying a UN Regulation may grant an exemption approval pursuant to a UN Regulation for a single type of wheeled vehicle, equipment or part which is based on a new technology, when this new technology is not covered by the existing UN Regulation, and is incompatible with one or more requirements of this UN Regulation.

340 The exemption approval procedure is precisely described in paragraphs 2 to 12 of Schedule 7 attached to the VPA[422] ("**Schedule 7**"). The "Administrative Committee" may authorise the exemption approval if it is satisfied that there is evidence of "at least an equivalent level of safety and environmental protection" to that provided by existing UN Regulations[423].

341 If contracting parties want to refuse, Paragraph 7 of Schedule 7 provides that they have the possibility to notify their disagreement or their intention not to accept the exemption approval immediately.

---

[421] PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, § 1.3 p. 27.

[422] See document E/ECE/TRANS/505/Rev.3, p. 39 et seq. https://unece.org/DAM/trans/main/wp29/wp29regs/2017/E-ECE-TRANS-505-Rev.3e.pdf (last consultation 31 August 2022).

[423] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.19 p. 90.

1.1.3 Vienna Convention on Road Traffic of 8 November 1968

1.1.3.1 Introduction

342 The Vienna Convention on Road Traffic, which should not be confused with the Vienna Convention on the Law of Treaties of 23 May 1969, is an international treaty designed to facilitate international road traffic and to enhance the safety on the roads through the adoption of standard road traffic rules amongst the contracting parties.

343 After its ratification, the Vienna Convention replaced the "International Convention relative to Motor Traffic" of 24 April 1926 and the Geneva Convention between the contracting parties (Art. 48 VC).

344 This Convention is the most comprehensive in terms of road traffic regulations, dedicating a whole chapter of thirty articles to the rules of the road and laying down rules on the main manoeuvres found in modern-day highway codes (see Chapter II, Art. 5 to 34 VC). The Vienna Convention went further than the previous — minimalist — conventions, which had just dealt with the passing of oncoming traffic and the associated signs and signals. It not only laid down the principles to be observed by drivers when performing the most dangerous manoeuvres (e.g. overtaking, change of direction, precautions to take vis-à-vis pedestrians etc.) but also regulated standing and parking, passengers boarding and alighting from vehicles, driving in tunnels — in short, the whole spectrum of typical situations that drivers face[424].

345 The Vienna Convention went also further than previous texts by requiring the contracting parties to bring the substance of their domestic legislation to comply with the driving rules laid down in it (Art. 3 VC). The advantage of this for drivers was that they would be familiar with the main driving rules when driving in other contracting parties (i.e. states)[425].

346 It should be noted that the Vienna Convention is not a self-executing treaty, meaning that its rules are not directly applicable and have to be transposed in the domestic legislation of the contracting parties (see Art. 3 VC)[426].

347 Therefore, the Vienna Convention contains legally binding provisions (not "principles") for the contracting parties (e.g. states), whilst road users have to comply with the domestic traffic laws[427] implementing the legally bindings provisions contained in the international conventions (e.g. road users do not have to comply with the provisions of the Vienna Convention directly).

---

[424] Opinion of the European Economic and Social Committee on "A European highway code and vehicle register", 2005/C 157/04, 28 June 2005, § 3.4.1.

[425] Opinion of the European Economic and Social Committee on "A European highway code and vehicle register", 2005/C 157/04, 28 June 2005, § 3.4.2.

[426] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 619.

[427] Informal document no 13 submitted by the secretariat, 10 March 2021, ECE-TRANS-WP.1-2021-Informal-No.13rev-e, p. 2 N 5 as well as p. 3 et seq.

348 States like the United States of America, China, Australia and Singapore have not signed the Vienna Convention, which has 86 contracting parties currently[428].

349 It should be noted that in contrast to UN conventions on vehicle safety, the European Union is (so far) not a contracting party to the conventions related to road traffic rules and only has observer status within UNECE, which could hamper its ability to coordinate Member State positions[429].

350 The Global Forum for Road Traffic Safety (WP.1) is in charge of amending the Vienna Convention (see N 371 below).

1.1.3.2 Amendments

351 In order to facilitate the introduction of automated vehicles, the definitions as well as Art. 8 para. 5 and 5[bis], 34 and 34[bis] (new) VC have been amended/created in 2016 and 2021.

352 The reasons for the 2016 amendment were to adapt the driver requirement[430] and the rule of the driver's control over the vehicle[431] contained in the Vienna Convention, which posed a hurdle to the approval of automated vehicles[432].

353 Art. 8 VC was amended with the introduction of para. 5[bis], amongst other things. According to this provision, the requirements of the driver's control of the vehicle are now deemed to be satisfied if the vehicle systems comply with international legal provisions on the approval of vehicles (sentence 1) or if the vehicle systems can (theoretically) be overridden or deactivated (sentence 2)[433].

354 In September 2020, WP.1 voted for a second amendment to the Vienna Convention, which shall facilitate the responsible use of automated driving systems. A new Art. 34[bis] provides that the driver requirement "is deemed to be satisfied" while the vehicle is using an automated driving systems which complies with (i) domestic technical regulations and any applicable international legal instrument concerning wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles, and (ii) domestic legislation on operation.

---

[428] https://treaties.un.org/Pages/ViewDetailsIII.aspx?chapter=11&mtdsg_no=XI-B-19&src=TREATY (last consultation 31 August 2022).

[429] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 617 p. 151.

[430] Art. 8 para. 1 VC states that "Every moving vehicle or combination of vehicles shall have a driver."

[431] According to Art. 8 para. 5 VC, "Every driver shall at all times be able to control his vehicle or to guide his animals" and to Art. 13 para. 1 VC, "Every driver of a vehicle shall in all circumstances have his vehicle under control so as to be able to exercise due and proper care and to be at all times in a position to perform all manoeuvres required of him. […]".

[432] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 619 and quoted references.

[433] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 619 and quoted references.

355 After its entry into force (depending on the contracting parties but beginning of July 2022 earliest[434]), contracting parties to the Vienna Convention will have to incorporate the amendment into their domestic legal road traffic framework[435]. The amendment does not provide any requirements as to who should be eligible to bring vehicles equipped with an automated driving system on public roads[436].

1.1.3.3 Compatibility with automated vehicles

356 It remains that several other provisions of the Vienna Convention are hardly compatible with automated vehicles and should be updated. Within UNECE in 2018, the Russian delegation has "stressed the need to amend the Vienna Convention to provide international and thus domestic legal basis for automated vehicles, as well as overcome the current legal difficulties, ensure international harmonisation, and define automated vehicles"[437].

357 For instance, various road traffic regulations call upon human intuition or interpretation of the driver, being implicitly a natural person (see also Recommendations under § 2.3 *supra*). According to Art. 6 para. 2 VC, road-users shall promptly obey all instructions given by authorized officials directing traffic. Art. 6 para. 3 VC provides the meaning of directions given by authorized officials, such as an arm raised upright (litt. a), arms outstretched horizontally (litt. b) and swinging red light (litt. c). Such signs are rather easily interpretable and comprehensive by a human being, and in the case of incomprehension, the "authorized official" can communicate with a human driver. But for automated driving systems, how to comply with this provision remains unclear and communication problems might arise between the "authorized official" and the automated driving system.

358 In a similar way, according to Art. 8 para. 6 VC, a "driver of a vehicle shall at all times minimize any activity other than driving. Domestic legislation should lay down rules on the use of phones by drivers of vehicles. In any case, legislation shall prohibit the use by a driver of a motor vehicle or moped of a hand-held phone while the vehicle is in motion". Yet, one of the purposes of automated driving at SAE Level 3 for instance is precisely to allow the human driver to perform activities other than driving when an automated driving system is in charge of the dynamic driving task. This issue has already been identified at UNECE level and amendments such as the creation of a new Art. 8 para. 6bis are under discussion[438].

359 Another example of these type of issues — although not directly generated by the Vienna Convention — are road traffic signals informing of potential hazards such as animals crossing the road, potential icy roads or flooding risks etc. Depending on the situation, this may involve swerving, a reduction in speed, to honk

[434] In Switzerland the amendment entered into force on 14 July 2021 (RO 2022 51), in France it was published in July 2022 through the "*Décret n° 2022-1034 du 21 juillet 2022 portant publication de l'amendement à la convention international sur la circulation routière de Vienne du 8 novembre 1968, adopté à Genève le 14 janvier 2022*" for instance.

[435] AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.

[436] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 3.2 p. 9.

[437] Report of the Global Forum for Road Traffic Safety on its seventy-seventh session, ECE/TRANS/WP.1/165, p. 5 N 16.

[438] Informal document no 13 submitted by the secretariat, 10 March 2021, ECE-TRANS-WP.1-2021-Informal-No.13rev-e, p. 2 N 2.

in order to warn other road users etc.[439]. Due to a lack of intuition, having the automated driving system assess which behaviour is appropriate and its consequences on the dynamic driving task might be complex.

360 Provisions that require a specific action that can only be carried out by a human person are also problematic. For instance, the provisions that require, in the case of a breakdown, to signal the location of a stopped vehicle on a lane with a warning triangle placed at a certain distance from the vehicle, with the purpose of warning other road users. It remains unclear how such obligation might be fulfilled by a driverless automated vehicle.

1.1.4 UNECE Agreement of 25 June 1998 concerning the establishment of global technical regulations

361 The Agreement concerning the establishing of global technical regulations ("**UN GTR Agreement**")[440] was issued in Geneva on 25 June 1998. The UN GTR Agreement was launched due to the fact that the United States of America and their self-certification regime were fundamentally barred from joining the VPA[441].

362 Following its mission to harmonise vehicle regulations, the UNECE solved the main issues, mostly administrative provisions regarding the type-approval and mutual recognition of type-approvals, that were preventing non-contracting parties to the VPA to fully participate to its activities[442].

363 The UN GTR Agreement has the aim to produce "meta"-regulations called "Global Technical Regulations" without administrative procedures for type-approval and the principle of mutual recognition. The UN GTR Agreement stipulates that contracting parties will establish, by consensual vote, United Nations Global Technical Regulations ("**UN GTRs**") in a global registry.

364 UN GTRs contain globally harmonised performance requirements and test procedures. Each UN GTR contains extensive notes on its development. The text includes a record of the technical rationale, the research sources used, cost and benefit considerations, and references to data consulted.

365 The contracting parties use their nationally established rulemaking processes when transposing UN GTRs into their national legislation. Similarly to the Vienna Convention (see N 346 above), manufacturers and suppliers cannot directly apply the UN GTRs, as these were intended to serve the contracting parties (e.g. states) and require transposition in national or regional law[443].

---

[439] Rödl & Partner, Innovationspapier zur automatisierten und fahrerlosen Personenbeförderung, erstellt im Auftrag des Verband Deutscher Verkehrsunternehmen e.V., Hamburg/Nürnberg, März 2021, p. 22.

[440] The full title being "Agreement concerning the Establishing of Global Technical Regulations for Wheeled Vehicles, Equipment and Parts which can be fitted and/or be used on Wheeled Vehicles".

[441] https://www.vda.de/vda/de/themen/automobilindustrie/standards-und-normung/harmonisierung-von-zulassungsvoraussetzungen (last consultation 31 August 2022).

[442] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations#1998_Agreement (last consultation 31 August 2022).

[443] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations#1998_Agreement (last consultation 31 August 2022).

366 As of August 2022, the UN GTR Agreement had 38 contracting parties, mostly European Member States in addition to Australia, Japan, India, the Republic of Korea, Russia, as well as self-certification states such as the United States of America and Canada. Switzerland is not a contracting party[444].

1.1.5 The UNECE, its working parties and subgroups

367 The UNECE was established after the second World War in 1947 to encourage economic integration and cooperation amongst its member states. It is one of the five United Nations regional commissions, administered by the Economic and Social Council ("**ECOSOC**"). The UNECE Sustainable Transport Division works to facilitate the international movement of persons and goods by inland transport modes. It aims to improve competitiveness, safety, energy efficiency and security in the transport sector[445].

368 The Inland Transport Committee ("**ITC**") is the highest policy-making body of the UNECE in the field of transport. Together with its subsidiary bodies, the ITC has provided a pan-European inter-governmental forum, where UNECE member countries come together to discuss tools for economic cooperation and negotiate and adopt international legal instruments on inland transport[446].

369 To deal with the transport issues, the ITC is assisted by a number of subsidiary bodies. Within UNECE, different working groups dedicated to specific topics were created. A few of the AV-relevant bodies will be presented briefly in the following sections. The current topics and ongoing works of these bodies during their yearly sessions can be found on the UNECE's website[447].

1.1.5.1 WP.1 — Global Forum for Road Traffic Safety

370 The UNECE pioneered road safety activities in the United Nations system with the establishment of an *Ad Hoc* Working Group on the prevention of road accidents in 1950. In 1988, the Working Party on Road Traffic Safety ("**WP.1**"), an intergovernmental body, was established. The Working Party changed its name to "Global Forum for Road Traffic Safety (WP.1)" in 2017[448].

371 Today, WP.1 remains the only permanent body in the United Nations system that focuses on improving road safety. Its primary function is to serve as guardian of the United Nations legal instruments aimed at harmonising road traffic rules, such as the Geneva and Vienna conventions, amongst others. Participation in WP.1 is open to all countries across the world[449].

---

[444] https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XI-B-32&chapter=11&clang=_en (last consultation 31 August 2022).

[445] https://www.connectedautomateddriving.eu/regulation-and-policies/world-wide-harmonization/ (last consultation 31 August 2022).

[446] https://www.connectedautomateddriving.eu/regulation-and-policies/world-wide-harmonization/ (last consultation 31 August 2022).

[447] https://unece.org/transport/road-traffic-safety (last consultation 31 August 2022).

[448] https://unece.org/about-us-15 (last consultation 31 August 2022).

[449] https://unece.org/about-us-15 (last consultation 31 August 2022).

372 Recently, WP1 has prepared and adopted a (non-binding) "Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic" on 20 September 2018. The purpose of this resolution is to guide contracting parties to the Geneva and Vienna Conventions as regards "the safe deployment of highly and fully automated vehicles in road traffic, in order to support the enhancement of road traffic safety, mobility and socio-economic progress"[450].

1.1.5.2 WP.29 — World Forum for Harmonization of Vehicle Regulations

373 In 1952, in addition to WP.1, another administrative committee was established, the "Working Party of experts on technical requirement of vehicles", known today as the "World Forum for Harmonization of Vehicle Regulations" or "Working Party 29" ("**WP.29**"), which is tasked with creating UN Regulations for vehicle components and systems[451]. While WP.1 is more focused on legal aspects, WP.29 is in charge of the technical aspects of road traffic regulations.

374 The European Union is a contracting party to the VPA and therefore a significant contributor to Working Party 29, as it may be considered to control a block of 25 out of the 54 votes *de facto*[452].

375 WP.29 is assisted in its work by specialized subsidiary (sub)groups known as Working Parties ("Groupe de Rapporteurs" in French, therefore abbreviated "GR") covering specific regulatory areas of vehicles. Their aim is to incorporate the technological innovations of vehicles to make them safer and more environmentally sound into the regulatory framework[453].

376 WP.29 should not be confused with the Article 29 Working Party, which was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018[454]. Since then, the Article 29 Working Party has now been replaced by the European Data Protection Board.

---

[450] Global Forum for Road Traffic Safety (WP.1), Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic, dated 20 September 2018 https://unece.org/DAM/trans/main/wp1/wp1doc/WP1_Resolution_Brochure_EN_web.pdf (last consultation 31 August 2022).

[451] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations (last consultation 31 August 2022).

[452] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.11 p. 89.

[453] https://www.connectedautomateddriving.eu/regulation-and-policies/world-wide-harmonization/ (last consultation 31 August 2022).

[454] https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en (last consultation 31 August 2022).

1.1.5.3 GRVA — Working Party on Automated/Autonomous and Connected Vehicles

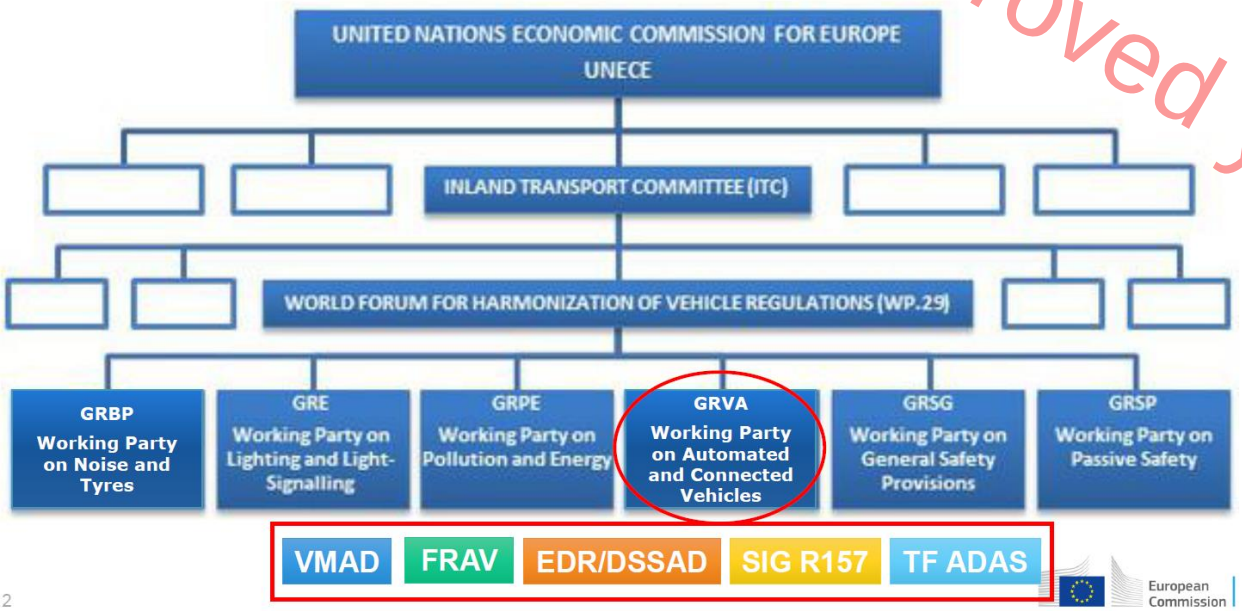

Figure 1: Overview of WP.29's Working Parties (source: Ms. Maria Cristina GALASSI[455])

377 The Working Party on Automated/Autonomous and Connected Vehicles ("Groupe de Rapporteurs pour les Véhicules Autonomes" in French, "**GRVA**") was created in February 2018, as the Inland Transport Committee acknowledged the importance of WP.29 activities related to automated, autonomous and connected vehicles. The existing Working Party on Brakes and Running Gear ("GRRF") was converted into the GRVA[456]. Since its creation, it has amongst others worked on the creation of UN Regulation 157 on ALKS.

378 As we will see below, diverse informal working groups are led by the GRVA. According to the UNECE's Framework Document on Automated Vehicles of 31 December 2019, the main themes of GRVA are the safety and security of automated driving systems and connected vehicles[457].

1.1.5.3.1 FRAV — Informal Working Group on Functional Requirements for Automated Vehicles

379 The Informal Working Group on Functional Requirements for Automated Vehicles ("**FRAV**") reports to GRVA and works closely with the Informal Working Group on Validation Methods for Automated Driving ("**VMAD**", see N 382 below).

380 FRAV focuses on safety requirements covering all automated driving systems' configurations (i.e. SAE levels 3 to 5). Its main objectives are that ADS drive safely and interact safely with their users,

[455] VMAD Informal Working Group and SG3, Seminar dedicated to "In service monitoring and reporting for automated driving safety", 16 May 2022, see https://aiforgood.itu.int/event/in-service-monitoring-and-reporting-for-automated-driving-safety/ (last consultation 31 August 2022).

[456] https://unece.org/introduction-4 (last consultation 31 August 2022).

[457] Revised Framework document on automated/autonomous vehicles, ECE/TRANS/WP.29/2019/34/Rev.2, https://undocs.org/ECE/TRANS/WP.29/2019/34/Rev.2 (last consultation 31 August 2022).

that ADS can manage safety-critical situations and failure modes, and that ADS maintain a safe operational state.

381 Its work items are, amongst others, the functional requirements for the combination of the different functions for driving: longitudinal control (acceleration, braking and road speed), lateral control (lane discipline), environment monitoring (headway, side, rear), minimum risk manoeuvre, transition demand, Human Machine Interface ("HMI") (internal and external) and driver monitoring[458].

1.1.5.3.2 VMAD — Informal Working Group on Validation Methods for Automated Driving

382 VMAD delivers new assessment and test methods of automated driving systems. It also reports to GRVA and has four subgroups, related to:

1. Scenarios;
2. Simulation;
3. Audit and Monitoring;
4. Track Test and Real-world tests.

383 VMAD develops assessment methods to validate the safety of automated systems, based on a multi pillar approach including auditing, simulation, virtual testing, test track testing, real world testing[459].

384 In particular, according to the Framework Document on Automated Vehicles of 31 December 2019, VMAD is dealing with the demonstration:

> "[…] of a robust design and validation process, based on a systems-engineering approach, with the goal of designing automated driving systems free of unreasonable safety risks and ensuring compliance with road traffic regulations and principles listed [in the framework document]. Design and validation methods should include a hazard analysis and safety risk assessment for automated driving systems, for the object and event detection and response , but also for the overall vehicle design into which it is being integrated and when applicable, for the broader transportation ecosystem. Design and validation methods should demonstrate the behavioural competencies an automated/autonomous vehicle would be expected to perform during a normal operation, the performance during crash avoidance situations and the performance of fallback strategies. Test approaches may include a combination of simulation, test track and on road testing"[460].

1.1.5.3.3 CS/OTA — Informal Working Group on Cyber security and software updates

385 The "Informal Working Group on Cyber Security and (Over-the-Air) Software Update issues" ("**CS/OTA**") addresses issues related to cybersecurity and over-the-air updates relevant for the automotive industry (e.g. for both conventional and automated vehicles), as well as data protection issues. CS/OTA also

[458] Revised Framework document on automated/autonomous vehicles, ECE/TRANS/WP.29/2019/34/Rev.2, https://undocs.org/ECE/TRANS/WP.29/2019/34/Rev.2 (last consultation 31 August 2022), Annex, Table 1, p. 5.

[459] https://www.connectedautomateddriving.eu/regulation-and-policies/world-wide-harmonization/ (last consultation 31 August 2022).

[460] Revised Framework document on automated/autonomous vehicles, ECE/TRANS/WP.29/2019/34/Rev.2, https://undocs.org/ECE/TRANS/WP.29/2019/34/Rev.2 (last consultation 31 August 2022), p. 3 N 9 litt. f.

develops relevant recommendations, regulations, provisions or documentation for both the UN GTR Agreement of 1998 and the VPA of 1958. It reports to GRVA[461].

386 The latest outcomes from CS/OTA are the recently adopted UN Regulation 155 on Cybersecurity and Cybersecurity Management Systems and UN Regulation 156 on Software Updates and Software Updates Management Systems.

1.1.5.3.4 EDR-DSSAD — Informal Working Group on Event Data Recorders / Data Storage Systems for Automated Driving

387 The Informal Working Group on Event Data Recorders/Data Storage Systems for Automated Driving ("**EDR-DSSAD**") reports to GRVA and to the Working Party on General Safety (GRSG). It has two subgroups on data storage and EDR's.

388 The EDR-DSSAD is dealing with "the function that collects and records the necessary data related to the system status, occurrence of malfunctions, degradations or failures in a way that can be used to establish the cause of any crash and to identify the status of the automated/autonomous driving system and the status of the driver"[462].

1.1.5.4 IGEAD — Informal Group of Experts on Automated Driving

389 During the seventy first session of the UNECE held in October 2015, WP.1 decided to establish an informal group of experts which will explore possibilities for WP.1 to work closer with WP.29 on the human factors issues (especially human machine interaction) in the context of technological advances[463], entitled the "Informal Group of Experts on Automated Driving" ("**IGEAD**").

390 IGEAD's recent work has focused on the driver/user roles and driver education in the context of technical progress and on "remote operations"[464].

1.1.5.5 GoE LIAV — Group of Experts on drafting a new legal instrument on the use of automated vehicles in traffic

391 The mandate of the Group of Experts on drafting a new legal instrument on the use of automated vehicles in traffic ("**GoE LIAV**") is to draft a new legal instrument, which is expected to complement the Geneva and Vienna Conventions. It will include a set of legal provisions for the safe deployment of automated

[461] https://www.connectedautomateddriving.eu/regulation-and-policies/world-wide-harmonization/ (last consultation 31 August 2022).

[462] Revised Framework document on automated/autonomous vehicles, ECE/TRANS/WP.29/2019/34/Rev. 2, https://undocs.org/ECE/TRANS/WP.29/2019/34/Rev.2 (last consultation 31 August 2022), p. 3 N 9 litt. i.

[463] Report of the Seventy–first session of the Working Party on Road Traffic Safety, ECE/TRANS/WP.1/151, https://unece.org/DAM/trans/doc/2015/wp1/ECE-TRANS-WP1-151e.pdf (last consultation 31 August 2022), p. 5 N 16.

[464] https://unece.org/sites/default/files/2022-06/ECE-TRANS-WP1-180e_0.pdf (last consultation 31 August 2022), p. 6 N 9.

vehicles in domestic and international traffic. These provisions will specifically aim to ensure road safety, in particular the safety of vulnerable road users[465].

392 The Group of Experts will have a two-year duration (with a possibility of extension) starting as of 1 July 2021. Upon the completion of its term, the Group of Experts will submit the complete draft new legal instrument to its supervising body (WP.1) for consideration and decision[466].

393 The GoE LIAV is not replacing existing informal groups working on AV-related matters. It has also been recommended that this body should integrate views and inputs from NGOs[467].

394 Some parties have already claimed that this new legal instrument should allow a worldwide harmonisation of the use of automated vehicles in traffic around 2025[468]. At the current stage, due to the technical, legal and even political complexity of the matter, the precise timing for the issuance of this instrument should be treated with particular caution.

395 As of March 2022, the programme of work of the GoE LIAV was the following:

- Conduct an assessment of road safety challenges posed by the use of automated vehicles in traffic that an international legal instrument could adequately address, which could later be used in an analysis of how the 1949 and 1968 Conventions on Road Traffic can be complemented (envisaged deadline: May 2022).
- Identify the recommended instrument type, the scope of issues by drafting a table of contents etc.) and legal implications (envisaged deadline: December 2022).
- Draft of an initial set of legal provisions for the safe deployment of automated vehicles in international traffic (envisaged deadline: May 2023)[469].

1.1.5.6 Others groups

396 WP.1 and WP.29 have also create numerous subgroups and informal working groups, such as:

- the Informal Group on Intelligent Transport Systems and Automated Driving ("ITS/AD"), which was a subgroup of WP.29 and held its last session in March 2018;
- The "Task Force on Advanced Driver Assistance Systems" ("**TF ADAS**") started its work on February 2021 and aims to resolve technical issues with automatically commanded steering functions provisions in UN Regulation 79 and to consider the development of a new UN Regulation to address advanced driving assistance systems (i.e. SAE Level 2 driving automation systems)[470].

---

465 https://unece.org/transport/road-traffic-safety/group-experts-drafting-new-legal-instrument-use-automated-vehicles (last consultation 31 August 2022).

466 *Ibid*.

467 Decisions on subsidiary bodies and on the structure of the Committee, Note by the secretariat, ECE/TRANS/2021/6 p. 2 N 6.

468 PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, § 1.2.4 p. 27.

469 Report of the Group of Experts on drafting a new legal instrument on the use of automated vehicles in traffic on its second session, 1 March 2022, https://unece.org/sites/default/files/2022-03/ECE-TRANS-WP1-GE3-2021-4e.pdf (last consultation 31 August 2022), Annex p. 7.

470 https://globalautoregs.com/groups/162-adas (last consultation 31 August 2022).

1.2 Legislation of the European Union

1.2.1 Competence

397 For the European Union to undertake legislative action, it needs not only to show that it has a legal basis to do so, but also to show that it complies with the principles of subsidiarity and proportionality[471].

1.2.1.1 Legal basis

398 The European Union is based on the principle of conferred powers, which means that it can only act in fields where the Member States have transferred powers to the European Institutions ("principle of conferral"). In practice, this means that the European Union may only legislate in areas for which there is a legal basis in the Treaty on the Functioning of the European Union ("**TFEU**")[472].

399 Art. 91 TFEU regulates the competence of the European Union to adopt legislation in the transport sector. Action under this provision should aim at setting common rules for international transport, to protect carriers from other Member States, to adopt measures with regards to transport safety, or any other "appropriate provision"[473].

400 The general internal market legal basis, Art. 114 TFEU, could also apply with regards to digital intermediaries, offering matchmaking in the field of transport, or with regard to a high level of protection for consumers and the environment[474].

401 Lastly, on setting the general principles for Services of General Economic Interest ("SGEIs") in the Member States, Art. 14 could also apply though with more limited scope, and could lead to "lower intensity" harmonisation because this legal basis is only about "setting principles and conditions"[475].

1.2.1.2 Subsidiarity

402 To resolve the issue of subsidiarity in European action of this nature, it is important to assess whether it would be better to regulate at European level rather than at the national level[476].

---

[471] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 53.

[472] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 53.

[473] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 53.

[474] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 53.

[475] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 53.

[476] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 53.

1.2.1.3 Proportionality

403 Next to the principle of conferral and subsidiarity, a future legislative proposal will have to comply with the principle of proportionality (Art. 5 TFEU). This means that the European Union will only take the action necessary to achieve the objective of the European Treaties and no more. Therefore, any harmonisation measure proposed by the European Commission should follow this principle[477].

404 Proportionality should not be assessed *ex ante* and *in abstracto*, but *in concreto* for each measure separately[478].

405 As a general guideline it may be said that any legal instrument providing, for instance, a "tool box", a set of criteria, general principles or basic rules to be used by national authorities – while allowing the Member States to adapt the procedures and tools to their needs – would likely satisfy this condition. The common agreement of "blacklisted" measures and practices, which by definition breach European law would also comply with the principle of proportionality[479].

1.2.2 Regulations 2018/858 and 2019/2144

1.2.2.1 Overview

406 In addition to the international agreements seen above, the European Union has set a comprehensive legal framework for the approval of motor vehicles and of their systems and components, established by the former Directive 2007/46.

407 This Directive was recently repealed by Regulation 2018/858[480] (Approval and Market Surveillance of Vehicles Regulation, in brief "**AMSVR**"), applicable since 1 September 2020. The core of the type-approval regulations are the technical requirements for motor vehicles concentrated in the AMSVR's Annex II. It should be noted that the AMSVR has been amended by Regulation 2019/2144 dated 27 November 2019 ("revised General Safety Regulation" or "**GSR**"), which applies since 6 July 2022[481].

1.2.2.2 Approval and Market Surveillance of Vehicles Regulation ("AMSVR")

408 The AMSVR lays down an administrative type-approval procedure for manufacturers willing to market a vehicle, system, component or separate technical unit in the entire European territory. The manufacturer has to demonstrate that each candidate vehicle type, system, component or separate technical unit

[477] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 54.

[478] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 54.

[479] HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021, § 5.1 p. 54.

[480] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.

[481] Art. 19 Regulation 2019/2144.

comply with technical regulatory requirements contained in its Annex II. They refer to many UN Regulations such as, for instance, directional equipment, lamps, heating systems etc.[482].

409 European type-approval certificates are issued by national approval authorities and allow a manufacturer to market vehicles EU-wide without any additional requirements. European type-approvals are issued after verification of the compliance with the relevant requirements. Compliance checks are carried out by technical services designated by approval authorities. During the certification process, manufacturers must establish an information folder and can be required to grant access to any software or algorithm but also, if needed, to provide information or documentation necessary to understand this software or algorithms. Thus, approval authorities and technical services can request information that is necessary to understand software and algorithms underlying the functioning of automated vehicles[483].

410 As mentioned, the AMSVR incorporates and refers to UN Regulations and it also completes them in two main ways:

- In some areas, most notably on emissions, the European Union has established its own standards for vehicles placed on the European market.
- The European Union also has a system for Whole Vehicle Type-Approval ("**WVTA**").

411 In addition, the manufacturer must also satisfy the approval authority that there will be "conformity of production" — that the production models will be manufactured according to the approved specifications. The procedures with regard to conformity of production are intended to ensure that each vehicle, system and component that is manufactured, and also each separate technical unit, corresponds to the approved type[484].

412 Depending on the Member States, the type-approval procedure may also be carried out by an independent, third party assessor[485].

1.2.2.3 Whole Vehicle Type Approval certificate

413 If the requirements are satisfied, the approval authority issues a Whole Vehicle Type Approval certificate. The manufacturer then provides a "certificate of conformity" for each production vehicle, with the purpose to confirm that it meets the specifications of the WVTA certificate. The certificate of conformity certifies that the vehicle can be sold, registered and used in the European Union[486].

---

[482] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 61.

[483] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 61.

[484] https://www.tuev-nord.de/en/news/areas-of-application/cop-conformity-of-production/ (last consultation 31 August 2022).

[485] Such as the "*Technischer Überwachungsverein*" ("TÜV") in Germany.

[486] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.13 et seq. p. 89.

1.2.2.4 Access to ODB and RMI

414 Besides, the AMSVR also ensures that manufacturers grant an unlimited, standardised and non-discriminatory access to vehicles' on-board diagnostics ("ODB") and repair and maintenance information ("RMI", including security features of the vehicle)[487] to third parties.

1.2.2.5 Provisions applying during the lifecycle of the product

415 The AMSVR also contains several provisions that apply during the use of products.

416 First, each Member State must designate authorities for market surveillance to carry checks verifying the compliance of vehicles, systems, components and separate technical units with the requirements of the AMSVR (Art. 6 para. 1 et seq. AMSVR). National authorities can request any information, including access to software and algorithms (Art. 8 para. 8 AMSVR). National authorities have the power to investigate the compliance of AI-based AV products with the safety requirements of European law. The AMSVR also empowers the European Commission to carry out checks of compliance with the regulation of the European market approvals granted to vehicles, systems, components, and separate technical units[488].

417 When national authorities grant market approval for any vehicles, systems, components and separate technical units, they must carry out checks to verify that manufacturers produce products that comply with their initial authorisations. These checks are based on products obtained from the manufacturers' facilities and the authority can request access to software, algorithms and any information necessary to understand their functioning. The authorities responsible for type-approval must monitor compliance of products with this market approval[489].

418 When, based on its checks or notification from type-approval authorities, a market surveillance authority discovers that a vehicle, systems, components and separate technical units present high risks or do not comply with the AMSVR, it must assess the item in question. If the manufacturer fails to remedy the non-compliance or if the risk requires swift measures, national authorities can withdraw or recall the product[490].

1.2.2.6 Exemption approval regime for new technologies

419 There is a long-standing procedure in European law to cater for new technology which is incompatible with existing UN Regulations. Art. 39 AMSVR applies where a system, component or unit "incorporates new technologies or new concepts that are incompatible with one or more regulatory acts". If the system nevertheless meets the test of ensuring "at least an equivalent level of safety and environmental

[487] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 62.

[488] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 3.3.1 p. 31.

[489] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 3.3.1 p. 31.

[490] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 3.3.1 p. 32.

protection", an approval authority may grant provisional approval[491]. UN Regulations are one example of "regulatory acts" concerned by Art. 39 AMSVR.

420 Initially, that approval is only valid in the territory of that type-approval authority, though authorities in other Member States may accept it, if they wish to do so[492]. The approval authority must then inform the European Commission, which decides whether to accept or refuse approval. If the European Commission accepts the approval, it "adopts implementing acts". This has the effect that all Member States must accept the technology[493], to the contrary of the exemption approval for UN Regulations (according to Schedule 7 of the VPA, see § 1.1.2.4 *supra*).

421 Based on this legal basis, the European Commission has created guidelines on the exemption procedure for the European approval of automated vehicles. The aim of these guidelines is to harmonise the practice of Member States for the national *ad-hoc* assessment of automated vehicles and to streamline the mutual recognition of such assessment, as well as to ensure fair competition and transparency[494].

422 Despite this legislative derogatory framework, manufacturers of automated vehicles, components or units have not taken advantage of this provision. As of 22 March 2021, no request for exemption had been filed for vehicles of SAE Level 3 or 4[495].

1.2.2.7 Provisions dedicated to "automated vehicles" and "fully automated vehicles"

423 The revised General Safety Regulation ("GSR"), applicable since 6 July 2022, was the first European legal instrument defining "automated vehicles" and "fully automated vehicles", at Art. 3 GSR:

- "automated vehicle" means a motor vehicle designed and constructed to move autonomously for certain periods of time without continuous driver supervision but in respect of which driver intervention is still expected or required[496];
- "fully automated vehicle" means a motor vehicle that has been designed and constructed to move autonomously without any driver supervision[497].

424 Art. 11 para. 1 GSR lists six fields where the European Commission "shall by means of implementing acts adopt provisions concerning uniform procedures and technical specifications" for automated vehicles and

[491] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.16 p. 89; See Art. 39 para. 1 and 2 AMSVR and former Art. 20 Directive 2007/46 (repealed).

[492] Art. 39 para. 5 AMSVR.

[493] Art. 39 para. 5 AMSVR; Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.17 p. 90.

[494] European Commission, Guidelines on the exemption procedure for the EU approval of automated vehicles, Version 4.1 supported by the Technical Committee on Motor Vehicles of 12 February 2019, p. 2.

[495] LAGRANGE, The importance of UNECE Regulations for the EU legislation on Automated driving, Future Networked Car Symposium, Session 1: Regulatory advances in highly automated driving, 22 March 2021, slide 8.

[496] Art. 3 (21) Regulation 2019/2144 of 27 November 2019.

[497] Art. 3 (22) Regulation 2019/2144 of 27 November 2019.

fully automated vehicles, as defined at Art. 3 para. 21 and 22 GSR. It concerns amongst others systems to replace the driver's control of the vehicle (litt. a), to provide the vehicle with real-time information on the state of the vehicle and the surrounding area (litt. b), driver availability monitoring systems (litt. c); event data recorders (litt. d) and systems to provide safety information to other road users (litt. f). The European Commission shall also enact provisions regarding the type-approval of those systems under the same provision[498].

425 In addition to the specific provisions related to automated vehicles, the GSR deals with following issues that have potential implications for AVs:

- First, at Art. 3 GSR, it defines new advanced safety systems such as intelligent speed assistance (para. 3), advanced driver distraction warning (para. 6), advanced emergency braking system (para. 10) and emergency lane-keeping system (para. 11);
- Second, it imposes on manufacturers the obligations to ensure that all vehicles, systems, technical units and components comply with technical regulatory requirements concerning, inter alia, protection against unauthorised use and cyberattacks and remote access to in-vehicle data or software modification that endanger vehicle passengers and other road users (Art. 4 para. 5 GSR);
- Third, Art. 6 para. 1 GSR also requires event data recorder (litt. g), intelligent speed assistance (litt. a) and advanced driver distraction warning (litt. d) for all motor vehicles; the GSR further requires braking and lane-keeping systems for cars and light commercial vehicles as well as special systems to detect and avoid vulnerable road users for buses and trucks; and provides high-level technical requirements for those safety systems, including with regard to the processing of personal data[499].

426 According to the report of the Law Commission of England and Wales and the Scottish Law Commission, the term "automated vehicle" in the GSR appears to cover SAE Level 3 systems, but there are differences in terminology compared with the SAE taxonomy contained in ISO/SAE DPAS 22736.

427 The GSR defines automated vehicles as being able to move without "continuous supervision", while fully automated vehicles are defined as being able to "move autonomously" without "any driver supervision" at all. This is in contrast to ISO/SAE DPAS 22736, which expressly envisages that no driver supervision is required for SAE Level 3 (or higher) level systems. It is not clear what the GSR expects by way of "non-continuous supervision" or how far this is similar to "receptivity" in the SAE taxonomy sense[500].

428 Besides, it should be noted that the European legislation lacks a legal definition of important concepts such as the "driver" and "driving"[501], although "driver" as a concept appears in the third driving permit Directive[502].

---

[498] Art. 11 para. 2 Regulation 2019/2144.

[499] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 60.

[500] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 4.53 p. 46 and quoted references.

[501] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 4 and quoted references.

[502] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences.

1.2.3 Delegated Regulation as regards the technical requirements for fully automated vehicles produced in small series

429 Since beginning of 2021 latest, the European Commission has been working on a draft Delegated regulation on […] fully automated vehicles produced in small series […] and annexes to this Delegated Regulation. This Regulation was initially scheduled to enter into force on 6 July 2022, i.e. the same day than the GSR, but it has been finally adopted by the European Commission on 20 June 2022 and will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union[503].

430 The complete name of the adopted act is "Commission delegated regulation of 20 June 2022 amending Annexes I, II, IV and V to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the technical requirements for vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update, C(2022) 3823 final". It is enclosed with four Annexes.

431 Amongst others, this Delegated regulation aims to set out the technical requirements to be applied for the European type-approval of fully automated vehicles produced in small series[504].

432 In order to allow for a progressive but quick introduction of automated driving technologies as first stage, this Delegated regulation harmonises requirements for the European whole vehicle type-approval of fully automated vehicles produced in small series. As a next stage, the European Commission intends to continue its work to further develop and adopt the necessary requirements for the whole vehicle type approval of fully automated vehicles produced in unlimited series, with a target date set to July 2024[505].

433 Subject to the requirements of Art. 42 and 45 AMSVR[506], Member States' authorities may continue to apply alternative approval schemes (national small series and individual vehicle approvals)[507].

---

[503] Art. 3 Commission delegated regulation of 20 June 2022 amending Annexes I, II, IV and V to Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the technical requirements for vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update, C(2022) 3823 final, and its four Annexes. To the knowledge of the author in August 2022, the publication did not happen in the meantime.

[504] Commission delegated regulation as regards the technical requirements for fully automated vehicles produced in small series, Explanatory memorandum, § 1 p. 1.

[505] Commission delegated regulation as regards the technical requirements for fully automated vehicles produced in small series, Explanatory memorandum, § 1 p. 1.

[506] Regulation (EU) 2018/858.

[507] Commission delegated regulation as regards the technical requirements for fully automated vehicles produced in small series, Explanatory memorandum, § 1 p. 1.

434 Annex IV Delegated regulation updates the annual production limits for the European small series scheme to set limits of 1'500 vehicles per annum for fully automated (mini)buses (categories M_2, M_3, N_2 and N_3). This limit has been controversial[508].

1.2.4 Implementing Regulation laying down rules for the type-approval of motor vehicle with regard to their automated driving system

435 In parallel to the drafting of the Delegated regulation as regards the technical requirements for fully automated vehicles produced in small series, the European Commission has also worked on an Implementing regulation as regards the type-approval of automated driving systems ("ADS") of fully automated vehicles[509]. This act has been adopted on 5 August 2022, a few weeks after the Delegated regulation and the entry into force of the revised GSR.

436 This Implementing regulation has two main parts: ADS performance requirements (see Annex II) and ADS compliance assessment (see Annex III). The ADS performance requirements specify what capabilities an automated vehicle must have to receive a type–approval. The ADS compliance assessment specifies how an automated vehicle will be evaluated, audited, and tested before it will get type–approval[510].

437 In a nutshell, the Implementing regulation for the type approval of ADS contains four articles:

- Art. 1 defines the scope of the regulation;
- Art. 2 provides for definitions of concepts used in the Regulation such as automated driving system, dynamic driving task, minimal risk manoeuvre and condition, object and event detection and response, on-board operator, remote intervention operator, functional and operational safety, time to collision, transport service operator etc.
- Art. 3 contains "administrative provisions and technical specifications", which are materially contained in the Annexes to which Art. 2 refers;
- Art. 4 sets the entry into force and provides that this Regulation shall be binding in its entirety and directly applicable in all Member States.

438 Annex I provides a model of an "Information document for European type-approval of fully automated vehicles with regard to their automated driving system".

439 Annex II contains the performance requirements that should be fulfilled by the ADS, namely:

- Dynamic driving task:

[508] See for instance European Automobile Manufacturers' Association's (ACEA) Feedback – Public Consultation on EU Automated cars – Technical Specification (ADS Implementing Act) of 4 May 2022, § 1 p. 2, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12152-Automated-cars-technical-specifications/F3255486_en (last consultation 31 August 2022).

[509] Commission implementing regulation of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles, C(2022) 5402 final, and its four Annexes.

[510] https://www.eetimes.com/eu-releases-ads-legislation-draft/ (last consultation 31 August 2022).

i) under nominal traffic scenarios;
ii) under critical traffic scenarios (emergency operation);
iii) at operation design domain boundaries;
iv) under failure scenarios;

- Minimal risk manoeuvre and Minimal risk condition;
- Human machine interaction;
- Functional and operational safety;
- Cybersecurity and software updates;
- Automated driving system's data requirements and specific data elements for the event data recorder of fully automated vehicles;
- Manual driving mode;
- Operating manual; and
- Provisions for periodic roadworthiness tests.

440 Annex III relates to the compliance assessment, divided in five parts, based on:

- The traffic scenarios to consider (Part. 1);
- The assessment of the ADS' safety concept and the audit of the manufacturer safety management system (Part. 2);
- The tests for the most relevant traffic scenarios (Part. 3);
- The principles to be used for the credibility assessment for using virtual toolchain to ADS validation (Part. 4);
- The system established by the vehicle manufacturer to ensure in-service reporting (Part. 5).

441 Annex IV is a model of the European type-approval certificate for the vehicle system.

1.2.5 Intelligent Transport Systems

1.2.5.1 Intelligent Transport Systems Directive

442 The more than 10 years old Intelligent Transport Systems ("**ITS**") Directive[511] establishes a framework for deployment and use of Intelligent Transport Systems, application and services in the field of road transport in the European Union. An ITS is defined as a "system in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport" (Art. 4 para. 1 ITS Directive).

443 Art. 2 ITS Directive identifies four priority areas for development of ITS:

- use of road, traffic and travel data;
- continuity of traffic and freight management services;
- road safety and security and
- communication between vehicles.

[511] Directive 2010/40/EU of the European Parliament and of 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.

444 Besides, the ITS Directive also identifies six priority actions within those areas at Art. 3 ITS Directive, amongst others:

- the provision of European-wide multimodal travel information services (litt. a);
- the provision of European -wide real-time traffic information services (litt. b);
- data and procedures for the provision, where possible, of road safety related minimum universal traffic information free of charge to users (litt. c).

445 To enable the deployment of ITS application and services within these priority areas, the ITS Directive empowers the European Commission to adopt technical, functional, organisational and service specifications through delegated acts. Member States are required to take the necessary steps to implement these specifications when deploying ITS services and applications. These specifications must be implemented in accordance with a set of principles detailed in Annex II of the ITS Directive (e.g. being cost-efficient, proportionate, delivering interoperability, facilitating intermodality). Hence, the ITS Directive establishes a framework identifying priority areas for applications and services that may be used in support of or in combination with AV products and services[512].

446 Travel and traffic information services aspects of the ITS Directive will be presented further in details below (see § 3.5.2 N 751 ss below). Accessibility aspects are outlined in the dedicated section (see § 2.2.7 *infra*).

447 The European Commission is currently revising the ITS Directive and a proposal[513] as well as an impact assessment[514] have been published end of 2021.

1.2.6 Resolution on a European strategy on Cooperative Intelligent Transport Systems

448 In March 2018, the European Parliament adopted a resolution on a European strategy on Cooperative Intelligent Transport Systems. This document sets high ambitions for legislative measures in the field and stressed a number of key areas that should be of focus, including:

- adopting rules to enable European wide cross-border interoperability;
- defining a framework for liability in the field of connected transport;
- ensuring a level playing field and security when it comes to storing and accessing in-vehicle data;
- granting third parties access to in-vehicle data and promoting competition in the market, as well as

[512] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 65.

[513] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/40/EU of the European Parliament and of 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, COM(2021) 813 final, 14 December 2021.

[514] Commission Staff Working Document, Impact Assessment Report, SWD(2021) 474 final, 14 December 2021.

- protecting consumer rights[515].

1.3 National legislation

1.3.1 Regulation of automated vehicles at national level

449 Member States have limited rights to permit vehicles to be used on their own roads without European type-approval because of the existing European framework. National approval is only available for vehicles produced in limited numbers (or "small series")[516]. The limits are low. Under the Directive 2007/46, for example, cars were only considered to be a small series where annual production did not exceed 100 vehicles. Under Regulation 2018/858 ("AMSVR"), this figure has been increased to 250 per Member State[517]. There is also a scheme for "individual vehicle approval"[518] which allows people to manufacture or import single vehicles or a few vehicles at a time[519].

450 It follows that vehicle type-approval and road worthiness tests are harmonised at European level and there is little to no room for regulations in these fields at national level. In the same time, until recently with the entry into force of the AMSVR and the revised GSR (Regulation 2019/2144), the legal framework at European level did not contain provisions on automated and/or autonomous motor vehicles.

451 In 2021, the German Ministry of Transport and Digital Infrastructure considered that depending on their stage of development, automated minibuses (often called "People-Mover" in Germany) are rather likely to enter into the category of an *aliud* (e.g. a robot) [520] rather than into the category of a motor vehicle under the AMSVR.

452 Therefore, according to this interpretation, a non-harmonised sector would exist, allowing for national law-making and national approval, with a validity limited to the national jurisdiction[521]. The French

[515] IACOB/CAMPMAS/SIMONELLI (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Annex IV Recommendations to the EU and national policy makers and an action plan for the creation of shared EU-wide in-vehicle data platforms, EASME/COSME/2018/004, 20 April 2021, p. 211.

[516] Art. 41 to 43 AMSVR.

[517] AMSVR, Annex V (2).

[518] Art. 44 to 47 AMSVR.

[519] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020, § 6.21 et seq. p. 90.

[520] Bundesministerium für Verkehr und digitale Infrastruktur (Germany), *Entwurf einer Verordnung zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, A. Begründung, II. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, Bearbeitungsstand 10. Juni 2021,* p. 67.

[521] Bundesministerium für Verkehr und digitale Infrastruktur (Germany), *Entwurf einer Verordnung zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, A. Begründung, II. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, Bearbeitungsstand 10. Juni 2021*, p. 67.

Government also enacted various ordinances and decrees on automated vehicles and minibuses (called "navettes urbaines" or "navurb") and therefore seems to have followed a similar approach in 2021.

453 As mentioned previously, the European Commission Delegated regulation as regards the technical requirements for fully automated vehicles produced in small series adopted in June 2022 provides that "Member States' authorities may continue to apply alternative approval schemes (national small series and individual vehicle approvals) subject to the requirements under Art. 42 and 45 of Regulation (EU) 2018/858". Besides, Member States may also "regulate the safety of operation of fully automated vehicles in traffic and the safety of operation of those vehicles in local transport services. To all aspects not covered by the harmonised requirements, national or local rules of the Member States apply"[522].

454 The influence of the Vienna Convention on the national lawmaking dedicated to automated and autonomous vehicles has also been discussed in Sweden.

455 According to the 2018 Swedish report's discussion related to the Vienna Convention (see § 1.3.8.1 below), the Vienna Convention makes it "inappropriate to introduce national driver-specific rules". The report, however, also analyses the VC in relation to sanctions: "It can be noted that the Vienna Convention lacks sanctions against the parties to the agreement. If country A nationally interprets the convention in a way and country B interprets the convention in another, there is no international body that can decide which country is right or wrong about the interpretation, even if the UNECE Secretariat that manages the Vienna Convention has some views about the interpretation" of the matter[523].

456 Hence, the report concludes that there would be no sanctions if Sweden were to read the Vienna Convention in a different way than it was written. The report also states that "it is possible to make an extensive national interpretation of the Vienna Convention to enable experiments and a careful introduction of fully automated driving"[524].

457 The question of the legal soundness of this approach may remain open to the benefit of general interest and innovation, as it has allowed to establish the first sets of legal basis' in Europe, which were strongly requested by many stakeholders. Nonetheless, this might pose further questions in the future, depending on the legal developments at international and European level.

1.3.2 Countries with AVENUE trials

458 The legal context in the four countries where AVENUE trials took place (namely Denmark, France, Luxembourg and Switzerland) where already presented in AVENUE's Deliverables 2.10 (p. 28 et seq.) and 2.11 (Appendixes 1 to 4, p. 27 et seq.), i.e. the First and Second report on regulatory requirements and compliance plan[525]. They will not be presented and discussed in substance in this deliverable, unless for

[522] Commission delegated regulation as regards the technical requirements for fully automated vehicles produced in small series, Explanatory memorandum, § 1 p. 1 et seq.

[523] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[524] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[525] D2.10 can be downloaded under following link, and D2.11 under following link.

new relevant provisions that have been published in the meantime (such as France, see § 1.3.3) or for particular topics.

1.3.3 France

459 The French "Loi d'orientation des mobilités" (Law on the orientation of mobility, in short "**LOM**") no 2019-1428 dated 24 December 2019[526] has set milestones regarding the deployment of automated vehicles in France.

460 Previously, other relevant provisions were enacted[527]:

- Art. 37-IX of Law no 2015-992 dated 17 August 2015 on energy transition, which empowers the French government to introduce by ordinance any measure to allow the circulation of autonomous vehicles on the public roads for experimental purposes;
- Ordinance no 2016-1057 dated 3 August 2016 on the experimentation of self-driving vehicles on public roads[528];
- Decree no 2018-211 dated 28 March 2018 on the experimentation of vehicles with "delegated driving functions" on public roads[529];
- Order dated 17 April 2018 on the experimentation of vehicles with "delegated driving functions" on public roads[530];
- Decree no 2018-1045 dated 28 November 2018 on vehicles dedicated to urban transport of persons[531];
- Art. 125 of Law no 2019-486 dated 22 May 2019 ("Loi Pacte") which followed to objectives, namely to broaden the scope of the experimentations and to better identify issues, particularly in terms of liability;

461 In particular, Art. 12 LOM empowers the French government to establish by ordinance the framework for the deployment of autonomous vehicles, which aims amongst others to define the conditions for authorising the operation of public or private collective road transport systems with "delegated driving functions" (i.e. automated driving systems). In addition to the prior approval of the vehicles, this involves a prior verification of the safety of the routes for the concerned vehicles[532].

462 Based on this legal basis, a series of governmental ordinances, decrees and orders were enacted, such as:

- Ordinance no 2021-442 dated 14 April 2021 on access to vehicle data[533] (see § 5.3.1.1 below);

[526] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039666574 (last consultation 31 August 2022).
[527] For further details, see PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021, § 1.6.1 p. 37 et seq.
[528] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032966695/ (last consultation 31 August 2022).
[529] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036750342 (last consultation 31 August 2022).
[530] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036868691 (last consultation 31 August 2022).
[531] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037662059 (last consultation 31 August 2022).
[532] Ministère de la transition écologique, Un an d'actions publiques pour le développement des véhicules autonomes Mai 2018 - Avril 2019, Avril 2019, p. 14.
[533] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043370884 (last consultation 31 August 2022).

- Ordinance no 2021-443 dated 14 April 2021 on the criminal liability in case of use of a vehicle with "delegated driving functions" and its conditions of use[534];
- Decree n° 2021-873 dated 29 June 2021 implementing Ordinance no 2021-443 dated 14 April 2021[535];
- Order dated 2 August 2022 as regards authorization of remote supervisors for automated road transport systems[536].

1.3.3.1 Decree no 2021-873 dated 29 June 2021

463 The French Decree no 2021-873 dated 29 June 2021[537] sets conditions for automated vehicles and automated road transport systems to be deployed on French roads. It covers automation levels up to fully automated systems, provided that these are under supervision of a person in charge of remote intervention and are deployed on pre-defined paths or zones[538].

464 The decree sets definitions and general safety provisions for these systems, as well as requirements for the driver or the person in charge of remote intervention[539]. These requirements are specified in a detailed order published in August 2022 that contains provisions as regards the qualifications, mandatory training and certification of the person in charge of remote intervention[540].

465 The decree also sets conditions under which fully automated systems (encompassing vehicles, roadside or remote equipment and operation procedures), can be commissioned, following a specific safety demonstration process[541].

466 The provisions of decree no 2021-873 dated 29 June 2021 will come into force on 1 September 2022, allowing the deployment of automated passenger transport services, beyond an experimental framework[542].

---

[534] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043370894 (last consultation 31 August 2022).

[535] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043729532 (last consultation 31 August 2022).

[536] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046151685 (last consultation 31 August 2022).

[537] Décret no 2021-873 du 29 juin 2021 portant application de l'ordonnance no 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation.

[538] Informal document GRVA-11-23, dated 1 July 2021 and submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, https://unece.org/sites/default/files/2021-09/GRVA-11-23e.pdf (last consultation 31 August 2022), p. 1.

[539] Informal document GRVA-11-23, dated 1 July 2021 and submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, https://unece.org/sites/default/files/2021-09/GRVA-11-23e.pdf (last consultation 31 August 2022), p. 1.

[540] See Titles II to V of the Order dated 2 August 2022 as regards authorization of remote supervisors for automated road transport systems, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046151685 (last consultation 31 August 2022).

[541] Informal document GRVA-11-23, dated 1 July 2021 and submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, https://unece.org/sites/default/files/2021-09/GRVA-11-23e.pdf (last consultation 31 August 2022), p. 1.

[542] Informal document GRVA-11-23, dated 1 July 2021 and submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, https://unece.org/sites/default/files/2021-09/GRVA-11-23e.pdf (last consultation 31 August 2022).

467 The decree introduces the concept of automated road transport systems ("*Système de transport routier automatisé*", "**ARTS**") which are described as a set of highly or fully automated vehicles, and technical installations allowing remote intervention or participating in safety deployed on predefined routes or areas, and supplemented with operating, upkeep and maintenance rules, for the purpose of providing a road transport passenger service[543].

468 With regard to the safety demonstration for allowing ARTS operation on public roads, the French legislator did not follow the traditional approval concept and is taking an open approach to the respective system levels and parties involved therein. There is the role of a "manufacturer" of the vehicle ("*constructeur de véhicules à moteur*", which itself still requires prior approval), the "designer of the technical system" ("*Concepteur du système technique*"), the "service organizer" ("*Organisateur du service*") and the "operator" ("*Exploitant*"). This can, except in some cases, be the same entity, but it does not have to be[544].

469 The designer of the technical system (i.e. vehicle plus equipment plus control center) is responsible for the overall design of the technical system and in particular for defining its functionalities and their conditions of use (amongst others, the operational design domain of vehicles and the system itself, conditions for minimum risk or emergency manoeuvres). Following evaluation and safety demonstration, the commissioning and operation of ARTS is subject to the decision of the service organizer[545].

470 The French approach allows for much flexibility and takes into account the interests and responsibilities, in particular for cases in which different entities and especially several manufacturers as well as mobility service providers are involved[546].

1.3.3.2 First driverless approval

471 According to various press clippings, the first approval for a driverless automated minibus circulating on a specific public road has been granted end of 2021.

1.3.4 Germany

1.3.4.1 2017 First AV-related amendment to the German Road Traffic Act

472 On 21 June 2017, an amendment of the Road Traffic Act dedicated to "automated driving" ("*Gesetz zum automatisierten Fahren*"[547]) came into force. It allowed automated driving systems (SAE Level 3) to take

[543] Informal document GRVA-11-23, dated 1 July 2021 and submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, https://unece.org/sites/default/files/2021-09/GRVA-11-23e.pdf (last consultation 31 August 2022) p. 2.

[544] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 3.2 p. 13.

[545] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 3.2 p. 13.

[546] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 3.2 p. 13.

[547] A non-official English translation of the most important provisions of the German Road Traffic Act can be found in the annex of EBERS, Civil Liability for Autonomous Vehicles in Germany, available at SSRN: https://ssrn.com/abstract=4027594 or http://dx.doi.org/10.2139/ssrn.4027594, 31 August 2022, p. 30.

over the dynamic driving task under certain conditions. A driver was still mandatory, however, he was allowed to turn away from traffic and vehicle control when the vehicle was in automated mode[548].

1.3.4.2 2021 Second AV-related amendment to the Road Traffic Act

1.3.4.2.1 Overview

473 A second more detailed amendment dedicated to "autonomous driving" ("*Gesetz zum autonomen Fahren*") entered into force on 21 July 2021[549]. It should be mentioned that despite using the wording of "autonomous driving", which might imply that this amendment regulates SAE Level 5 vehicles, it actually regulates vehicles of SAE Level 4 and below, but not above.

474 This second amendment creates the legal framework for "autonomous" vehicles to be able to drive in regular operation in defined operating areas on public roads, nationwide within Germany. It follows these purposes:

- Increasing road traffic safety;
- Enabling new mobility concepts;
- Increasing transport efficiency;
- Reducing of emissions;
- Strengthening Germany as location for innovation;
- Easier experimentation possibilities;
- Better participation for mobility-impaired persons[550].

475 Flexibility is at the forefront of this second amendment: the operation of driverless vehicles is made possible for a large number of deployment scenarios. The various use cases are not exhaustively regulated *ex ante* in advance and are only locally limited to a defined area of operation. Individual approvals, exceptions and conditions, such as the presence of a safety operator who is always ready to intervene, are therefore unnecessary[551].

476 The deployment scenarios are the following (amongst others):

- Shuttle transport from point A to B;
- "People movers" (automated minibuses travelling on a fixed route);
- Hub to hub automated transport (e.g. between two distribution centres);
- Demand-oriented transportation offers at off-peak times;
- Transport of passengers and/or goods on the first or last mile;

[548] https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html (last consultation 31 August 2022).

[549] https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html (last consultation 31 August 2022).

[550] Informal document GRVA-11-19, submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, slide 2 https://unece.org/sites/default/files/2021-09/GRVA-11-19e_0.pdf (last consultation 31 August 2022).

[551] https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html (last consultation 31 August 2022).

- "Dual Mode Vehicles" such as vehicles with automated valet parking feature[552].

477 The second amendment (newly) regulates the following matters, amongst others:

- Technical requirements for the construction, characteristics and equipment of vehicles with autonomous driving functions;
- Approval and inspection procedure for the granting of an operating licence for vehicles with autonomous driving functions by the competent central (federal) authority ("*Kraftfahrt-Bundesamt*");
- Regulating obligations of persons engaged in the operation of vehicles with autonomous driving functions, with the creation of the "*technische Aufsicht*";
- Regulations on the processing of data during the operation of vehicles with autonomous driving functions;
- Enabling the (subsequent) activation of automated and autonomous driving functions of already type-approved motor vehicles (so called "sleeping functions");
- Adaptation and creation of uniform and harmonised regulations to enable the testing of automated and autonomous motor vehicles[553].

478 Instead of a driver, the second amendment creates a new role of a "technical supervisor" or "technical supervision" ("*technische Aufsicht*"), e.g. a person responsible to ensure compliance with the road traffic laws. For this purpose, the "*technische Aufsicht*" has a variety of obligations, such as assessing transmitted vehicle data in order to be able to activate alternative driving manoeuvres or switch off the automated driving system as well as communicating with passengers[554] (see also N 52 above as regards the qualifications of the "*technische Aufsicht*").

479 The approval of automated vehicles takes places in three steps[555]:

- Approval
  Operation of an automated vehicles requires that the vehicle manufacturer obtains an operating permit from the "*Kraftfahrt-Bundesamt*" (which is also responsible for market surveillance). The Ordinance sets out the procedural framework for the permit, including the technical requirements which are detailed in its Annex I. The application of the vehicle manufacturer requires detailed documentation, such as a declaration concerning compliance with the technical requirements and the provision of a safety concept concerning functional safety, information technology and general road traffic safety. The manufacturer further needs to document test scenarios in a catalogue covering test parameters and environmental influences on the vehicle that may arise during operation.

---

552 https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html (last consultation 31 August 2022).

553 https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html (last consultation 31 August 2022).

554 AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.

555 https://www.engage.hoganlovells.com/knowledgeservices/news/german-federal-council-clears-the-way-for-autonomous-driving (last consultation 31 August 2022); see also Informal document GRVA-11-19, submitted during 11th GRVA session, 27 September 2021 – 1 October 2021, Provisional agenda item 11, https://unece.org/sites/default/files/2021-09/GRVA-11-19e_0.pdf (last consultation 31 August 2022).

- A second approval regarding the specific operational design domain (ODD)
  The owner (which may also be the vehicle manufacturer) of the automated vehicle needs to define its operating area which has to be limited geographically to a defined environment, e.g. A to B (routes or particular parts of highways for instance) or even A^2 (area). The ODD needs to be approved by the competent authority for the specific operating area (which may be a federal or regional/local authority). The application requires a detailed description by the owner, including an illustration of a cartographically delimited area, the purpose of the operation and the associated operating conditions. The competent authority then verifies the suitability of the specific operating area. In the course of the operation, the owner must then ensure that, based on the repair and maintenance information provided by the vehicle manufacturer, the vehicle systems for the active and passive safety of the automated vehicle are regularly checked and an extended departure check ("*erweiterte Abfahrkontrolle*") is completed.

- Registration
  Based on the two first approvals, and similar to conventional vehicles, the registration of the SAE Level 4 vehicles can take place and the individualised automated vehicle receives license plates.

480 In addition, the second amendment will extend existing experimentation opportunities for autonomous driving functions and there will be the possibility to approve vehicles with so-called "sleeping" autonomous driving functions (i.e. the functions cannot influence the vehicle when deactivated) which can be activated at a later stage by way a subsequent approval[556].

1.3.4.2.2 Ordinance

481 The details of the provisions of the second amendment are implemented in an Ordinance of the German Ministry of Transport and Digital Infrastructure, called "Autonomous Vehicle Approval and Operation Ordinance" ("*Autonome Fahrzeug-Genehmigungs- und Betriebsverordnung*" — "**AFGBV**"). The AFGBV has been published on 30 June 2022[557] and entered into force on 1 July 2022.

482 The AFGBV regulates, amongst others:

- the granting of operating licences and approvals for vehicles equipped with automated and autonomous driving functions;
- the approval of the specific operating areas of these vehicles;
- the admission of vehicles equipped with autonomous driving functions to road traffic;
- their market surveillance;
- the requirements and obligations of the vehicle manufacturer, the owner/keeper and the technical supervision.

1.3.4.2.3 Data privacy

483 The AFGBV also contains data privacy provisions that will be review in the dedicated part below (see Appendix A § 5.3.2 *infra*).

[556] AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.
[557] Bundesgesetzblatt Jahrgang 2022 Teil I Nr. 22, S. 986 et seq.

1.3.4.2.4 Further obligations, liability and ethics

484 In addition to the new role of the "*technische Aufsicht*" and responsibilities, other involved stakeholders will need to fulfil additional obligations. The manufacturer of a vehicle with autonomous driving functions is, for example, responsible for aspects of cybersecurity (e.g. provision of proof that the electrical and electronic architecture of the vehicles is protected against attacks), risk assessments and trainings for the persons engaged in the operation and deployment. Vehicle owners have also to bear an enhanced duty of care[558].

485 The vehicle manufacturer must also provide a comprehensive training to the persons involved in the operations and deployment, in particular with regard to the driving functions and the performance of the tasks of the "*technische Aufsicht*" (§ 1f para. 3 (5)).

486 The liability of the vehicle owner under the current road traffic regime will generally not change. However, should the vehicle owner decide to delegate the tasks of the "*technische Aufsicht*", he/she will be responsible for any fault of the person entrusted with those tasks. Existing statutory provisions dealing with driver liability will not be applicable[559].

487 Ethical aspects are also taken into account. According to § 1e para. 2 no. 2 StVG, the vehicle must be equipped with a "system of accident avoidance" ("*System der Unfallvermeidung*") in order to solve dilemma situations in an ethically justifiable manner. How such a balancing of legal interests has to take place in practice remains unclear[560]. The German Ministry for Transport and Digital Infrastructure previously published a report of an *ad hoc* ethics commission on automated and connected driving in June 2017[561], which might serve as a guideline.

1.3.4.2.5 First approval

488 End of 2021, the first approval under the new legislation was granted to a German manufacturer for two of its private car models (equipped with SAE Level 3 ALKS technology)[562]. They are deployed on the German highways since May 2022.

489 Besides, in the city of Monheim, the public transport operator has been granted the first nationwide route concession for their vehicle operation until 2026. This means that the automated minibus' service fleet is fully integrated into the public transport offer of the city of Monheim, i.e. with operating and transport obligations[563].

---

[558] AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.

[559] AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.

[560] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 624 and quoted references.

[561] Ethik-Kommission (eingesetzt durch den Bundesminister für Verkehr und digitale Infrastruktur), Automatisiertes und Vernetztes Fahren – Bericht, June 2017.

[562] https://www.kba.de/DE/Presse/Pressemitteilungen/Allgemein/2021/pm49_2021_erste_Genehmigung_automatisiertes_Fahren.html?snn=3662144 (last consultation 31 August 2022).

[563] https://www.vdv-akademie.de/blog/eine-busfahrt-ohne-fahrerin/ (last consultation 31 August 2022).

1.3.5 Spain

490 A new framework regulation which entered into force on 21 March 2022[564] introduced a series of modifications to the current regulation of vehicles and contains, amongst others, provisions dedicated to automated vehicles.

491 For the most part, these provisions leave the future detailed regulatory framework in the hands of the General State Administration, through administrative regulations that have not yet been issued[565].

492 Experimentations of SAE Levels 3 to 5 automated vehicles is permitted only where specific prior authorisation (exemption) has been obtained from the government ("*Dirección General de Tráfico*")[566].

493 The "Instruction 15/V-113"[567] aims at regulating the granting of special authorizations for testing and research tests conducted automated vehicles on roads open to traffic. The Instruction 15/V-113 sets a number of requirements for the vehicle, the driver and the applicant that must be fulfilled before an exemption is granted[568].

1.3.6 Italy

494 Under the Decree published on 28 February 2018 by the Ministry of Infrastructures and Transport[569], significant restrictions apply to automated vehicles in Italy. The current regulatory regime is principally aimed at experimentation of SAE Level 3 and 4 automated vehicles on public roads[570].

495 Although the testing of automated vehicles is permitted with the appropriate authorization on certain roads, there must be a safety operator ("*Supervisore*") present inside the vehicle to be able to take manual control at any given time[571].

496 Art. 10 of the Decree contains a number of obligations to be fulfilled by the "*Supervisore*", in particular:

- holding a driving permit for minimum five years;

---

564 "Ley 18/2021 de 20 de diciembre 2021, por la que se modifica el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial […] en materia del permiso y licencia de conducción por puntos", https://www.boe.es/eli/es/l/2021/12/20/18/con (last consultation 31 August 2022).

565 WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022, p. 17 et seq (as of March 2022).

566 https://cms.law/en/int/expert-guides/cms-expert-guide-to-autonomous-vehicles-avs/spain (last consultation 31 August 2022).

567 https://www.dgt.es/export/sites/web-DGT/.galleries/downloads/muevete-con-seguridad/normas-de-trafico/VEH-vehiculos/15.V-113-Vehiculos-Conduccion-automatizada.pdf (last consultation 31 August 2022).

568 https://www.connectedautomateddriving.eu/regulation-and-policies/national-level/eu/spain/ (last consultation 31 August 2022).

569 Decreto 28 febbraio 2018 Modalita' attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Road e di guida connessa e automatica, GU Serie Generale n. 90 del 18 Aprile 2018, p. 4 et seq.

570 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

571 Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D5.4, IoT Policy Framework for autonomous vehicles applications, 26 December 2018, Version 1.0, § 2.3.1 p. 19.

- having successfully passed a safe driving course or a specific course for automated vehicles testing at an accredited body in one of the countries of the European Union;
- having conducted tests on automated vehicles in a protected site or on a public road; and
- possess the necessary knowledge, adequately documented, to take part in the tests as safety operator[572].

1.3.7 Netherlands

497 On 24 February 2017, the law on testing autonomous vehicles ("*Experimenteerwet zelfrijdende auto*") came into force in the Netherlands.

498 This law allows the authorities to deviate from individual provisions of the Dutch national road traffic act ("StVO"), as well as from other laws – in each case exclusively for experimental purposes. The purpose of the law on testing autonomous vehicles is to enable the testing of driverless (self-driving) vehicles on Dutch roads in the future, subject to compliance with specific provisions[573]. The Dutch Vehicle Authority ("RDW") is the competent authority that grants a discretionary exemption for the testing of driverless vehicles on public roads. Companies can apply for an exemption after which the application goes through an approval process with the RDW[574].

499 After the introduction of the new law in 2017, there is currently no longer a requirement for a driver to be located inside the vehicle, but a driver must still be in control of the vehicle – if necessary by remote control. In the Netherlands, it is therefore possible for the driver to be either inside or outside the vehicle, as long as the test driver is in control of the vehicle at all times. If the driver is outside the vehicle, he/she must not be more than six metres away from the vehicle and the vehicle speed is limited to a maximum of 10 km/h[575].

500 Regarding the proceedings for trials, the RDW decides where and under what circumstances the testing can be carried out. First, the RDW will analyse the application, the testing plan and the test results that are available at that time. If this analysis is satisfactory, all functionalities that the applicant wants to test on public roads will be tested on an enclosed test track. The exemption will only be granted if these tests are passed as well. The conditions of the exemption will be decided upon by the RDW. Possible conditions are the type of road and the weather conditions under which testing is allowed, but additionally, it could also require obtaining additional insurance[576].

---

[572] WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022, § 2 p. 6 and § 4 p. 14.

[573] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 11.

[574] Sohjoa Baltic, The Legal Framework, The Roadmap to Automated Electric Shuttles in Public Transport, IKEM — Institut für Klimaschutz, Energie und Mobilität e.V., May 2020, p. 57.

[575] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 11.

[576] VELLINGA, Legal aspects of Automated driving, On drivers, producers and public authorities, University of Groningen, Groningen, 2020, § 2.5.3 p. 54.

501 On 1 July 2019, the Netherlands introduced a testing regime ("Method admittance procedure") for "connected automated vehicles"[577]. It enables companies to seek approvals regardless of any manufacturing status.

1.3.8 Sweden

1.3.8.1 Report on self-driving vehicles

502 In 2015, the Swedish government authorised a special investigator to analyse what regulatory changes were needed in order to introduce driver-supporting technology and fully or partly self-driving vehicles on the road. The assignment included considering and submitting legislative proposals with the aim of creating better legal conditions for: a) trials of self-driving vehicles on public roads and b) the introduction of such vehicles on public roads. This work resulted in the publication of two reports of more than 1'400 pages, published in 2018[578].

503 According to these researches, multi-stage development of regulations was required to deal with developments in the field of automated mobility so that this development could take place in a safe, sustainable manner. The researchers recommended an adaptation of the regulations so that these do not impede the development of new solutions for enhanced attainment of transport policy targets. The researchers proposed that in the short term (over the next five years), Swedish regulations should be adapted to prepare for automated driving and facilitate the introduction of highly or fully automated vehicles (essentially corresponding to SAE levels 4–5). During this time, focus should be on facilitating the market introduction of certain self-driving vehicles and facilitating trials of advanced automated functions for driving in convoy (platooning), freight transport and passenger transport. To this end, the researchers proposed a new act on automated driving, consisting of three sections; one relating to the driver, one relating to penalties and one relating to data storage[579].

504 The Swedish government concluded that the existing legal framework already made it possible to carry out trials at all levels of automation on Swedish roads, as the Swedish Transport Administration has the legal authority to grant exemptions to existing legal regulations (technical building regulations, road traffic regulations) in individual cases[580].

---

[577] https://www.rdw.nl/over-rdw/information-in-english/about-rdw/connected-automated-vehicle/method-admittance-procedure-its (last consultation 31 August 2022).

[578] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[579] AXHAMN, Look out – Self-driving vehicles are around the corner!, in P. Wahlgren (Ed.), 50 years of law and IT: the Swedish Law and Informatics Research Institute: 1968-2018, Scandinavian Studies in Law; Vol. 65, Stockholm 2018, § 3.1 p. 372.

[580] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 17.

505 On 20 April 2017, the Swedish government passed an ordinance that allowed experiments with self-driving vehicles, with permission for such experiments to be granted by the Swedish Transport Agency. In September 2018, it also began to allow experiments with self-driving vehicles on public roads[581].

506 Since then, a memo (Ds 2021:28) addressing certain responsibility questions in relation to automated vehicles was published by the government, but no additional legislative developments took place[582]. It seems that the Swedish government was waiting for regulations to be adopted at European level before proceeding to amendments at national level[583].

507 The memo Ds 2021:28 also concluded to the need for new rules in order to promote the use of so-called geofencing for automated vehicles[584].

1.3.8.2 Ordinance 2017:309 on the performance of trials with self-driving vehicles on public roads

508 With the introduction of the new ordinance[585], concrete legal framework conditions for the performance of trials on public roads in Sweden were created.

509 The ordinance specifically stipulates that the transport authority ("*Transportstyrelsen*") can issue temporary exemption certificates to carry out test drives by means of automated vehicles on public roads. However, the authority must first clarify with the applicants that the planned implementation of the tests will not endanger road safety or significantly disturb the environment. The authority has to evaluate the test applications on the basis of the information provided and determine whether the legal requirements can be met. Should no endangerment and nuisance be assumed in the performance of the test, the authority may issue a temporary exemption[586]. This individual exemption certificate is issued with regard to the requested route, the requested vehicle and the specific system[587].

510 Such an exemption may be withdrawn by the authority at any time if there are subsequent changes or if, contrary to expectations, conditions imposed by the authority are not met or implemented (Art. 8 Ordinance). In addition, the authority also has the right to set further framework conditions for the test

[581] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[582] https://www.wistrand.se/en/germany-and-france-at-the-forefront-regarding-legislation-on-automated-vehicles-will-sweden-be-left-behind/ (last consultation 31 August 2022).

[583] WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022, p. 24.

[584] WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022, p. 29.

[585] Ordinance (2017:309) on autonomous vehicle tests.

[586] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 17.

[587] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 18.

drives at any time (Art. 4 Ordinance). The exemption is only granted for a limited period of time, but it can be extended (Art. 4 Ordinance)[588].

511 According to Art. 7 Ordinance, similarly to the Netherlands, there must be a driver inside or outside the vehicle at all times, who can check the vehicle at any time[589].

1.3.9 Austria

512 On 19 December 2016, the Ordinance on automated driving ("AutomatFahrV") came into force in Austria. According to the newly introduced § 102 para. 3a KFG, the driver may transfer certain driving tasks to assistance systems or automated and connected driving systems present in the vehicle through the authorisation (test certificate), if these systems have been approved (in particular, if they comply with UN Regulations) or if these systems comply with the requirements for test purposes set out in the ordinance[590].

513 The ordinance currently allows the following use cases to be tested on Austria's roads:

- Highway pilot with lane change assistant;
- Automated minibuses;
- Self-driving army vehicles[591].

514 Further use cases could be included in the Ordinance by the "*Bundesministerium Verkehr, Innovation und Technologie*" by means of an amendment, if required, and after a thorough evaluation of their road safety. Such systems must all be designed in such a way that compliance with the provisions of the Austrian Road Traffic Act remain nevertheless possible[592].

515 According to § 8 AutomatFahrV, automated minibuses are currently allowed to drive at a maximum of 20 km/h and can theoretically be tested on all roads. Before the systems are approved for test purposes on roads with public traffic, they must have already covered at least 1'000 kilometers on a private test field, virtually or on the test bench[593].

516 On 11 March 2019, the first amendment to the AutomatFahrV came into force. A new third section of this ordinance now regulates automated driving of vehicles produced in series and defines the two use cases of parking aid (§ 10) and the automatic lane keeping systems (§ 11). The use cases could already be used

[588] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 17.
[589] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 17.
[590] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 7.
[591] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 7.
[592] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 8.
[593] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 7.

(legally) before, but the driver is now temporarily relieved of certain duties[594]. Both use cases (defined as SAE Level 2) may now be approved under an ordinary regime (and not under a trial framework).

517 On 1 April 2022, a second amendment to the AutomatFahrV was released[595], allowing new use cases for testing and amongst others:

- Automated vehicles for passenger transport such as automated minibuses (§ 7 and § 7a);
- Automated vehicles for the transport of goods (§ 7b);
- Automatic lane keeping system with automated entering and exiting of highways (not allowed previously, § 8 and § 8a);
- Automated valet parking (§ 9a).

518 Like Switzerland and other countries, Austria relies on a delegation of the exact formulation of AV-regulations at ordinance level[596] (e.g. a material law emitted by the executive body which is more agile and flexible than a formal law enacted by the legislative body).

519 In contrast to other countries, which regulate automated driving systems as such, Austria has focused on two particular use cases. With this approach, regulation can be "precisely tailored", but it will have to be readjusted more often[597].

1.3.10 Finland

520 As of March 2022, Finland has launched a national project to implement the amendments of the Vienna convention, and the work will proceed in phases[598].

1.3.11 Norway

521 On 6 January 2016, the Norwegian government authorised the Norwegian Public Roads Administration to investigate and prepare possibilities for regulations that would allow for experiments with self-driving vehicles on public roads[599].

522 On 15 December 2017, the Norwegian Parliament passed new legislation that allowed experiments with self-driving vehicles on public roads. This law permitted the responsible authority to make exceptions to existing laws that had previously prevented the testing of self-driving vehicles. When designing this

[594] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 626 and quoted references.

[595] Verordnung des Bundesministers für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie über Rahmenbedingungen für automatisiertes Fahren (Automatisiertes Fahren Verordnung – AutomatFahrV), BGBl. II Nr. 402/2016.

[596] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 626 and quoted references.

[597] LOHMANN, Mobilität von Morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 627 and quoted references.

[598] https://unece.org/sites/default/files/2022-03/ECE-TRANS-WP1-Informal-8e.pdf (last consultation 31 August 2022).

[599] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

legislation, the government relied heavily on the Swedish report on self-driving vehicles[600] (see above § 1.3.8.1).

523 Norway, however, went further than Sweden in terms of the role of the driver, since the Norwegian legislation did not impose the requirements of having a driver physically in or outside the vehicle[601].

1.3.12 Switzerland

524 Trials of automated vehicles are currently possible and approved according to Art. 106 para. 5 of the Swiss road traffic law, which states that "in the event of the occurrence of new technical developments in the field of road traffic […], the Federal Council may take such provisional measures as may prove necessary pending the adoption of legislation".

525 The Swiss Federal Roads Office ("**FEDRO**") has launched various studies as regards automated driving and smart mobility. Amongst others, two important group of studies on the "Effects of automated driving" and "Mobility of the future" were published recently[602].

526 In 2022, the Federal Council (Swiss federal government) submitted to the Parliament an amendment to the Swiss road traffic law, with provisions dedicated to "Vehicles with automation systems" ("*Fahrzeuge mit einem Automatisierungssystem*", Art. 25a – 25d SVG).

527 According to this draft amendment, the Swiss government should be able to determine the extent to which drivers are relieved of their duties and the extent to which driverless vehicles with automated driving systems can be approved if they operate on defined routes and under supervision.

528 The framework conditions will be laid down in the provisions of a formal law, the Swiss road traffic law, but the technical details will be regulated in a dedicated ordinance to be issued by the Federal Council, allowing to keep an agile approach to the upcoming technological evolutions.

529 The FEDRO should also be given the possibility to approve and financially support tests with automated vehicles.

1.3.13 Great Britain

530 In Great Britain, the Law Commission for England and Wales and the Scottish Law Commission ("**Law Commissions**") were in charge of examining together options for regulating AV's. The Law Commissions

[600] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[601] HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020, § 5.1 p. 5 and quoted references.

[602] Forschungspakete "*Auswirkungen des automatisierten Fahrens*" und "*Verkehr der Zukunft*", see https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet/studien-und-berichte.html (last consultation 31 August 2022).

published various interesting and comprehensive reports and consultation papers between November 2018 and January 2022[603].

531 Amongst others, the Law Commissions have recommended the creation of an Automated Vehicles Act, under which a clear distinction would be made between vehicles which allow for assisted driving and those which have "self-driving" features[604].

532 The Law Commissions also introduced the concept of an "Automated Driving System Entity" ("**ADSE**") which is the entity that puts the automated driving system forward for approval and is legally responsible for how the automated driving system performs the dynamic driving task. The scope of ADSE appears to be broad, which may also serve as a good example for other regulators. It is stated that the vehicle manufacturer or software designer or a joint venture may, for example, be the ADSE, taking into account the development and future of the industry landscape, in order to remain flexible. Another proposal is that developers should be able to submit an automated driving system they have created for national approval, even if they are not responsible for manufacturing the whole vehicle[605].

533 In August 2022, the government of the United Kingdom accepted the recommendations issued by the Law Commissions and announced large investments[606] as well as the development of proposals for legislation within a forthcoming Transport Bill to be submitted to the Parliament. The government's proposals and "Theory of Change" supposed to take place until 2025 is distilled into tree pillars of activity:

- Ensuring safety and security of connected and automated vehicles;
- Securing the industrial and economic benefits of CAVs and
- Delivering the societal benefits of CAVs through greater research and engagement with the public, as well as commitment to promote and align connected and automated vehicles with wider future transport strategies[607].

534 Previously, the United Kingdom had published an "Automated and Electric Vehicles Act" on 19 July 2018. In a nutshell, this Act clarifies the liability scheme for automated vehicles as follows:

- Where the vehicle is insured and an injury results from an accident, the insurer shall be liable for damages;
- Where the vehicle is not insured, the owner shall be liable;
- Where a person allows the vehicle to drive itself when it is inappropriate to do so and causes an accident, neither the insurer nor the owner of the vehicle shall be liable[608].

---

[603] https://www.lawcom.gov.uk/project/automated-vehicles/ (last consultation 31 August 2022).

[604] WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022, p. 30.

[605] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 3.2 p. 16.

[606] The government announced GBP 100 million investments (including the GBP 40 million previously announced in 2022) to kickstart commercial deployments.

[607] https://www.lexology.com/library/detail.aspx?g=9785d88b-acd0-445b-9cec-4956007344af (last consultation 31 August 2022); see also Report under https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1099173/cam-2025-realising-benefits-self-driving-vehicles.pdf (last consultation 31 August 2022).

[608] https://www.mondaq.com/canada/rail-road-cycling/1119282/autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

1.3.14 United States of America

1.3.14.1 Overview

535 In the United States, regulatory responsibility for motor vehicles is divided between the federal level and the individual states. At federal level, regulations regarding vehicle registration are issued in the Federal Motor Safety Vehicle Standards ("**FMVSS**"), similar to the UNECE Regulations for vehicle registration in the European Union. The obligations of drivers, amongstother things, are defined at the individual state level[609].

536 Due to the different legislative powers, the regulations in the individual states on automated driving often differ consequently from each other, and can vary from a ban to a broad release[610].

1.3.14.2 National Highway and Transportation Safety Administration ("NHTSA")

537 An important federal agency in the field of automated driving is the National Highway and Transportation Safety Administration ("**NHTSA**"), which is part of the United States Department of Transportation. The NHTSA develops uniform safety standards for motor vehicles in the USA, finances road safety programmes and conducts research activities in the field of transport[611].

538 Since most highly or fully automated vehicles are currently not compatible with the FMVSS, NHTSA often grants exemptions for a maximum period of two years. However, NHTSA may not and cannot issue exemptions from the driver obligations for testing purposes, as this is the competence of the local authorities in the individual states[612].

539 NHTSA has drafted strategies for vehicle automation[613]. Part of these strategies are concrete recommendations to the individual states on how they should implement automated driving in their legal systems. These are only recommendations, as NHTSA does not have the authority to enact uniform rules, laws or regulations in the area of driver responsibilities for all states[614].

540 NHTSA considers the automated driving system to be an item of motor vehicle equipment and has set about to build a regulatory framework specifically for the ADS. The focus lies on the safety of the ADS,

---

[609] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 24.

[610] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 24.

[611] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 24.

[612] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 24.

[613] The latest report "Ensuring American leadership in automated vehicle technologies, Automated Vehicles 4.0" has been published in January 2020.

[614] Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018, p. 24.

which, as NHTSA recognizes, can be the responsibility of several types of entities: "*Entities involved in the development and deployment of automation technology have an important role in their responsibilities for safety assurance of ADS-equipped vehicles and in providing transparency about their systems are achieving safety*". The ADS developer can be understood in a broad manner, and may include traditional vehicle manufacturers as well as new entrants (e.g. tech companies)[615].

541 Until recently, federal input on the rapid emergence of automated vehicles has been absent. For example, the federal "Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act" or the "Self Drive Act", which had been dormant since 2017, was reintroduced again in June 2021. The re-introduced "Self Drive Act" seeks to advance safety by prioritizing the protection of consumers, reaffirm the role and responsibilities of federal and state governments, update the FMVSS to account for advances in technology and the evolution of highly automated vehicles and maximize research and development opportunities for autonomous vehicles in the United States[616].

542 This proposed legislation requires the manufacturers of automated vehicles to have a cybersecurity plan, including having a written cybersecurity policy and appointing an officer for the management of cybersecurity. However, the "Self Drive Act" does not provide in depth requirements regarding how vehicle manufacturers should ensure that their self-driving vehicles go through software updates. Additionally, the "Self Drive Act" does not address liability and damages for accidents involving autonomous vehicles[617].

1.3.14.3 California

543 California is one of the federal states at the forefront of AV deployment and related legal developments. Since 2014, California has had legislation in place to accommodate for the experimentation of so-called self-driving vehicles. Division 16.6, Section 38750 of the California Vehicle Code is devoted to autonomous vehicles. This section entails definitions, requirements for insurance and the operator and how to act in case of a failure etc.[618].

544 As follows from the California Code of Regulations, a so-called Manufacturer's Testing Permit is needed for experimenting self-driving vehicles on public roads. A Testing Permit will only be issued when all of the requirements laid down in the California Code of Regulations and California Vehicle Code are met, and all of the necessary testing required to satisfy the Department for Motor Vehicles that the vehicles are safe to operate on public roads has been completed[619].

---

[615] Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021, § 3.2 p. 16.

[616] https://www.mondaq.com/canada/rail-road-cycling/1119282/autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

[617] https://www.mondaq.com/canada/rail-road-cycling/1119282/autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

[618] VELLINGA, Legal aspects of Automated driving, On drivers, producers and public authorities, University of Groningen, Groningen, 2020, § 2.5.1 p. 49 and quoted references.

[619] VELLINGA, Legal aspects of Automated driving, On drivers, producers and public authorities, University of Groningen, Groningen, 2020, § 2.5.1 p. 49 and quoted references.

545 More than fifty approvals for experimentations on public roads have been granted by this state. As of July 2022, a vehicle manufacturer is deploying driverless robotaxis in the city of San Francisco for commercial services during night hours.

1.3.15 Canada

546 At the federal level in Canada, the Motor Vehicle Safety Act regulates the manufacture and importation of motor vehicles. Provinces and territories in Canada have developed and/or are developing their own regulatory regimes as to the testing and deployment of automated vehicles on public roads[620].

547 In August 2021, Transport Canada released Guidelines for testing automated driving systems which replaced an earlier edition published in 2018. They seek to clarify the different roles and responsibilities of federal, provincial, territorial and municipal governments in approving and facilitating testing of automated vehicles as well as explaining the process for organizations to obtain approvals from different levels of government prior to conducting testing[621].

548 Ontario began a ten-year pilot program in 2016 to allow the testing of automated vehicles on Ontario's roads under strict conditions. Under a regulation published in Ontario[622], SAE Level 3 automated vehicles can be driven on Ontario public roads with authorization. Québec also has a similar legal regime[623].

549 A new regulation[624] in Ontario (amending the previous one) now allows driverless automated vehicles as well as cooperative truck platoons, both under certain conditions[625].

1.3.16 Japan

1.3.16.1 SAE Level 3

550 In Japan, the government amended the Road Transportation Vehicle Act ("RTVA") and the Road Traffic Act ("RTA") in April 2020, which generally allows SAE Level 3 automated vehicles to be used on public roads[626].

---

620 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

621 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

622 O. Reg. 517/18: PILOT PROJECT - AUTOMATED VEHICLES filed December 20, 2018 under Highway Traffic Act, R.S.O. 1990, c. H.8 https://www.ontario.ca/laws/regulation/r18517 (last consultation 31 August 2022).

623 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

624 O. Reg. 306/15: PILOT PROJECT - AUTOMATED VEHICLES under Highway Traffic Act, R.S.O. 1990, c. H.8 https://www.ontario.ca/laws/regulation/150306 (last consultation 31 August 2022).

625 https://www.ontario.ca/page/automated-vehicle-pilot-program (last consultation 31 August 2022).

626 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

551 "Autonomous driving systems" are defined by the RTVA as "a set of sensors and artificial intelligence that replace all driver capabilities with a recording device"[627].

552 The RTVA outlines technical specifications that ADS systems must comply with. Additionally, manufacturers and importers of ADS-equipped vehicles must provide model-specific ADS specifications to users[628].

553 The RTVA permits the Minister of Land, Infrastructure, Transport and Tourism to set conditions on the usage of each automatic operating device. The conditions can include, amongst other conditions:

- Road conditions: general road, motorway, specialized road, highway, etc.; and
- Geographic conditions: urban areas, mountainous areas and other specialized areas[629].

554 Under the RTA, the driver of a SAE Level 3 ADS-equipped vehicle cannot use the ADS technology unless the usage conditions have been met. If the driving environment conditions no longer meet the requirements, the driver must take over the dynamic driving task. Therefore, the driver must be in a position to facilitate a prompt take-over[630].

555 Significantly, under the RTA, the driver of an ADS-equipped vehicle must use a vehicle recording device. The police may request disclosure of the applicable recording from the driver. If the police considers that the provided records are insufficient, they may issue penalties against the driver, including a driving prohibition[631].

1.3.16.2 SAE Level 4

556 The RTA limits the use of SAE Level 4 automated vehicles to authorized public road experimentations[632].

557 On September 2021, the Ministry of Land, Infrastructure, Transport and Tourism and the Ministry of Economy, Trade and Industry announced that they would carry out a new project named "Road to the L4". In this project, the Japanese government aims to increase and implement the use of SAE Level 4 automated vehicles. The goal is to deploy the use of SAE Level 4 vehicles in more than 40 locations by 2025[633].

---

627 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

628 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

629 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

630 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

631 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

632 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

633 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives and https://unece.org/sites/default/files/2022-03/ECE-TRANS-WP1-Informal-8e.pdf (last consultation 31 August 2022).

1.3.17 China

1.3.17.1 Overview

558 On 24 March 2021, the Ministry of Public Security of China issued "Draft Proposed Amendments of the Chinese Road Traffic Safety Law" (the "**MPS Proposed Amendments**"). The MPS Proposed Amendments clarify the requirements related to the experimentation of automated vehicles, as well as a brief allocation of liability[634] by simply indicating that the responsibility of the driver and the automated driving system developer shall be determined in accordance with the law[635].

559 The MPS Proposed Amendments require that vehicle manufacturers conduct road experimentation for automated vehicles in closed roads before they can apply for a temporary license to conduct further road experimentations in public roads. Road experimentations on public roads can only be conducted at designated times, areas and routes in accordance with the law. During experimentations, a driver must be sitting in the driver's seat and be able to take over when needed[636].

560 This was an important milestone, as it was the first time that China proposed specific legislation for automated vehicles at the level of the Road Traffic Safety Act[637]. On July 2021, the draft was promulgated into law[638].

561 In August 2022, a Chinese service provider was granted the approval for the commercial deployment of driverless robotaxis in the cities of Chongqing and Wuhan[639].

1.3.17.2 Shenzen

562 In parallel, the Standing Committee of the Shenzhen Municipal People's Congress released a Draft for Comments of the Regulations of Shenzhen Special Economic Zone on the Administration of Intelligent and Connected Vehicles (the "**Shenzhen Draft Regulations**") on its website for public comment on 23 March 2021[640].

563 Generally, vehicle manufacturers may sell motor vehicles in China only upon meeting the standards published by the Ministry of Industry and Information Technology of China. However, the Shenzhen Draft

---

634 https://www.chinalawinsight.com/2021/04/articles/corporate-ma/chinas-legislation-on-autonomous-cars-rolls-out/ and the quoted references (last consultation 31 August 2022).

635 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

636 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

637 https://www.chinalawinsight.com/2021/04/articles/corporate-ma/chinas-legislation-on-autonomous-cars-rolls-out/ and the quoted references (last consultation 31 August 2022).

638 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

639 https://www.reuters.com/business/autos-transportation/baidu-bags-chinas-first-fully-driverless-robotaxi-licenses-2022-08-08/ (last consultation 31 August 2022).

640 https://www.chinalawinsight.com/2021/04/articles/corporate-ma/chinas-legislation-on-autonomous-cars-rolls-out/ and the quoted references (last consultation 31 August 2022).

Regulations allow manufacturers to sell autonomous vehicles within Shenzhen upon meeting a special set of local standards[641].

564 Automated vehicles can be operated on the roads of Shenzhen once they are registered with Public Security Traffic Administrative Bureau and the applicable certificates of registration, plates and licenses are issued. The Shenzhen Draft Regulations also regulate cybersecurity, including requirements for companies to establish a cybersecurity evaluation and management system[642].

565 The Shenzhen Draft Regulations also contain provisions for determining liability for traffic violations and accidents of autonomous vehicles:

- With a driver present, the driver shall be liable in case of an accident; however, if the accident is caused by a defect in the automated driving system, the driver can sue the manufacturer or distributor of the vehicle to recover damages paid to the victim.
- Without a driver present, the controller or owner of the vehicle shall be liable in case of an accident. Similar to automated cars with a driver, if the accident is caused by a defect in the automated driving system, the controller or owner can sue the vehicle manufacturer or distributor of the vehicle to recover damages paid to the victim[643].

566 Shenzhen is clearly vying to be the first location in China where automated vehicles may realize commercialization[644].

1.3.18 Further countries

567 For further information regarding regulations and policies of European Member States and other States, it may be referred to the CCAM website[645] which contains sections compiled in the framework of the CARTRE project[646] between 2016 and 2018, as well as to AUTOPILOT's Deliverable 5.4 "IoT Policy Framework for autonomous vehicles applications"[647].

* * *

641 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

642 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

643 https://www.blg.com/en/insights/2021/10/the-sensor-autonomous-vehicles-cross-jurisdictional-regulatory-perspectives (last consultation 31 August 2022).

644 https://www.chinalawinsight.com/2021/04/articles/corporate-ma/chinas-legislation-on-autonomous-cars-rolls-out/ and the quoted references (last consultation 31 August 2022).

645 https://www.connectedautomateddriving.eu/regulation-and-policies/ (last consultation 31 August 2022).

646 CARTRE Coordination of Automated Road Transport Deployment for Europe, Deliverable D3.8 "Guidance on National Testing Regulations – Final edition", 30 September 2018.

647 Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D5.4, IoT Policy Framework for autonomous vehicles applications, 26 December 2018, Version 1.0, § 2 p. 14 et seq.

1.4 Intermediary remarks

568 Transitioning from the "driver centric" approach in the international and national framework is an important paradigm shift and the adaptation of the approval framework to automated vehicles will require numerous legislative changes. The efforts that have already been initiated at international and national levels to revise the existing framework should be acknowledged.

569 Nevertheless, the inertia involved by such legislative changes might result in undesirable legal gaps in the approval of automated minibuses and vehicles. The fact that amendments brought in international law (such as the Vienna Convention) need to be adapted in domestic law increases the delays. Regarding the regulation of these new technologies, efforts should be made at all levels, as they evolve from a technological point of view in a quicker way than international and national legislations.

570 Some states (pushed by their industry) have anticipated this situation and followed a dynamic pioneering legal approach. Other states follow a more conservative approach and are waiting for the international, European and national regulations. But by waiting today, these states might in fact already fall behind, as these new technologies requires specific skills, knowledge and expertise from the authorities that should be developed as soon as possible.

571 A legislative trend encountered in different jurisdiction is to enact principles related to automated vehicles in formal laws and to regulate the details by "material" (such as ordinances, decrees, orders etc.) laws, published and adopted by the governments or related entities. This approach allows to keep the legal framework flexible and agile, in order to evolve with the technologies, which seems to be a smart approach.

572 At international level, the different legal regimes of type approval and self-certification do not help coordination and harmonisation. As self-certification allows for more flexibility, some voices consider that it might form a comparative advantage for manufacturers experimenting and deploying their vehicles in these jurisdictions.

* * *

2 Overview of the legal framework as regards accessibility to persons with reduced mobility

573 At international level, the right for everyone to be able to enjoy seamless travel independently is addressed by the European treaties that guarantee the right to free movement for all citizens, as well as Art. 21 and 26 of the Charter of Fundamental Rights of the European Union and Art. 9 of the United Nations Convention on the Rights of Persons with Disabilities[648], that will briefly be detailed below.

2.1 UN Convention on the Rights of Persons with Disabilities

574 The Convention on the Rights of Persons with Disabilities[649] ("**CRPD**") was adopted by the United Nations General Assembly on 13 December 2006. The European Union and all Member States are parties to the CRPD. Norway ratified it on 3 June 2013[650], Switzerland on 15 April 2014[651] and the United Kingdom in July 2009[652].

575 The CRPD guarantees all human rights for people with disabilities and ensures that they can participate in public, economic and social life. It does not contain any special rights, but defines universal human rights from the perspective of persons with disabilities. The aim is to promote equal opportunities for persons with disabilities and to prevent discrimination against them in society[653].

576 The Convention guarantees persons with disabilities *inter alia* the right to:

---

[648] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 12.

[649] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities (last consultation 31 August .2022).

[650] https://www.bufdir.no/en/English_start_page/Disabilities_in_Norway/#:~:text=Norway%20and%20international%20treaties&text=The%20UN%20General%20Assembly%20adopted,disability%20is%20the%20CRPD%27s%20goal (last consultation 31 August 2022).

[651] https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/un-human-rights-treaties/convention-on-rights-of-persons-with-disabilities.html (last consultation 31 August 2022).

[652] https://www.gov.uk/government/publications/2010-to-2015-government-policy-equality/2010-to-2015-government-policy-equality#appendix-10-united-nations-convention-on-the-rights-of-disabled-people (last consultation 31 August 2022).

[653] https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/un-human-rights-treaties/convention-on-rights-of-persons-with-disabilities.html (last consultation 31 August 2022).

- an independent and autonomous life;
- his or her own family;
- employment;
- an adequate living standard and social protection;
- access to education;
- participate in public and cultural life and
- protection against multiple discrimination, violence, exploitation and abuse[654].

577 Amongst others, Art. 20 CRPD provides that contracting parties shall take effective measures to ensure personal mobility with the greatest possible independence for persons with disabilities, including by facilitating the personal mobility of persons with disabilities in the manner and at the time of their choice, and at affordable cost (litt. a).

578 The CRPD requires contracting parties to take appropriate measures to ensure that persons with disabilities have access, on an equal basis with others, to the physical environment, to transportation, to information and communications and to other facilities and services open or provided to the public, both in urban and in rural areas[655].

579 These measures include the identification and elimination of obstacles and barriers to accessibility *inter alia* in buildings, road and transportation[656].

580 Contracting parties are obliged to create "focal points" that supervise the implementation of their commitments under the Convention. They must also develop a national programme to implement and promote the Convention[657].

581 Moreover, contracting parties are to take appropriate measures to develop, promulgate and monitor the implementation of minimum standards and guidelines for the accessibility, to ensure that private entities offering facilities and services which are open or provided to the public take into account all aspects of accessibility for persons with disabilities, to provide training for stakeholders and forms of live assistance and intermediaries and to promote other appropriate forms of assistance and support to persons with disabilities to ensure their access to information[658].

---

[654] https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/un-human-rights-treaties/convention-on-rights-of-persons-with-disabilities.html (last consultation 31 August 2022).

[655] Recital 13 Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

[656] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 248 p. 62.

[657] https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/un-human-rights-treaties/convention-on-rights-of-persons-with-disabilities.html (last consultation 31 August 2022).

[658] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 248 p. 62.

2.2 Initiatives and legislation of the European Union

582 The European Union is applying its international obligations (such as those of the CRPD) by the legislation listed in the table § 2.2.10.1 and respective European accessibility standards listed in table § 2.2.10.2 below. The European regulation on accessibility has to be transposed to the national legislation in all Member States.

2.2.1 European communication on passenger rights in all transport modes

583 Published in 2011[659], this communication sets out the vision for the definition and realisation of basic European passenger rights, such as the right to non-discrimination in access to transport and the right to compensation, amongst others.

584 The European Commission recognised that the different rules applying to the different modes of transport make seamless travel difficult, while it also clearly mentioned that the adoption of the proposal for a European Accessibility Act would be an opportunity for developing a general set of standards for the accessibility of transport infrastructure and services[660].

2.2.2 European strategy for the rights of persons with disabilities (2021-2030)

585 In March 2021, the European Commission adopted the Strategy for the rights of persons with disabilities 2021-2030[661]. The Strategy builds on the results of the previous European Disability Strategy 2010-2020, which paved the way to a barrier-free Europe and to empower persons with disabilities so they could enjoy their rights and participate fully in society and economy[662].

586 Similarly to the CRPD, the objective of this Strategy is to progress towards ensuring that all persons with disabilities in Europe, regardless of their sex, racial or ethnic origin, religion or belief, age or sexual orientation:

- enjoy their human rights;
- have equal opportunities, equal access to participate in society and economy;
- are able to decide where, how and with whom they live;
- move freely in the European Union regardless of their support needs and

[659] Communication from the Commission to the European Parliament and the Council: A European vision for Passengers: Communication on Passenger Rights in all transport modes, COM/2011/0898 final.

[660] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 13.

[661] European Commission, Directorate-General for Employment, Social Affairs and Inclusion, Union of equality: strategy for the rights of persons with disabilities 2021-2030, COM(2021) 101 final, Publications Office, March 2021, https://data.europa.eu/doi/10.2767/31633 (last consultation 31 August 2022).

[662] https://ec.europa.eu/social/main.jsp?catId=1484 (last consultation 31 August 2022).

- no longer experience discrimination[663].

2.2.3 European sustainable and smart mobility strategy

587 The sector-specific European Sustainable and Smart Mobility Strategy published in December 2020 acknowledges in its section "Flagship 9 – Making mobility fair and just for all" that mobility remains not sufficiently accessible for people with disabilities or reduced mobility[664].

588 The European Commission wants to ensure that the new mobility possibilities are affordable and accessible in all regions and for all passengers, including those with disabilities and reduced mobility[665].

589 According to the Staff Working Document related to the Strategy, persons with disabilities and reduced mobility still consider that they do not enjoy equal access to public transport: they demand more accessibility and the elimination of the pre-notification requirement necessary to give assistance to them in case they cannot use independently public transport (or at least to shorten such periods which they consider extremely long at the moment)[666].

2.2.4 Regulation 1300/2014 "TSI PRM"

590 The Regulation "TSI PRM"[667] improved access to rail travel for persons with disabilities since its entry into force in 2007. It has been revised in 2014, 2016 and 2019[668].

591 Amongst others, the TSI PRM obliges manufacturers and public authorities to equip new and refurbished trains with wheelchair accessible toilets, opening and closing audio signals of the train doors, hearing loops at ticket desks, tactile markings on platforms and many other accessibility features that were previously not mandatory[669].

[663] https://ec.europa.eu/social/main.jsp?catId=1484 (last consultation 31 August 2022).

[664] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 88 p. 20.

[665] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 89 p. 20.

[666] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 934 p. 213.

[667] Commission Regulation (EU) No 1300/2014 of 18 November 2014 on the technical specifications for interoperability relating to accessibility of the Union's rail system for persons with disabilities and persons with reduced mobility.

[668] European Disability Forum (EDF), EDF recommendations on the revision of the TSI-PRM 2019, Brussels, October 2019, p. 4.

[669] European Disability Forum (EDF), EDF recommendations on the revision of the TSI-PRM 2019, Brussels, October 2019, p. 3.

2.2.5 Regulation 1371/2007 on rail passengers' rights

592 The Regulation on Rail Passengers' Rights ("Rail PRR")[670] establishes rules for the provision of assistance at rail stations, transport of and liability for mobility equipment, as well as passengers' rights in cases of delay or cancellation.

593 According to Art. 24 litt. a Rail PRR, a maximum notice period is required to book assistance for persons with reduced mobility, which is defined at 48 hours. This actually prohibits spontaneous travel of persons with reduced mobility. This is why in some European countries, shorter notice periods have been regulated[671].

2.2.6 Regulation 181/2011 concerning the rights of passengers in bus and coach transport

594 The material scope of the Regulation is restricted to bus travels in distances over 250 kms (Art. 2 para. 1).

595 According to Art. 3 litt. j Regulation 181/2011, a "disabled person" or "person with reduced mobility" means any person whose mobility when using transport is reduced as a result of any physical disability (sensory or locomotory, permanent or temporary), intellectual disability or impairment, or any other cause of disability, or as a result of age, and whose situation needs appropriate attention and adaptation to his particular needs of the services made available to all passengers. This definition is broader than the one provided by the CRPD and does not hinder the inclusivity of the endless array of disabilities and mobility issues that exist[672].

596 Any person experiencing reduced mobility (directly or indirectly, permanent or temporary) when travelling by bus becomes a beneficiary of the rights enshrined in Regulation 181/2011: persons in a wheelchair and those who broke a leg, persons with visual or mental impairment, aged persons, all of them are included. A varying array of rights is then acknowledged to the beneficiaries in Chapter III, including obligations for bus services providers to provide adequate information, accept them on board, provide assistance at terminals and on board etc.[673].

597 Regulation 181/2011 requires that carriers must provide disability awareness training to their personnel, including the drivers. Additionally, as defined under Art. 12, the Member States have to provide the

[670] Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations.

[671] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 14.

[672] Arrillaga/Sanchez Barrueco (et al.), Contribution to the Public Consultation on the evaluation of the European Disability Strategy 2010-20, Performance Review of the implementation of Regulation 181/2011/EU, 13 November 2019, Deusto Law School, p. 75.

[673] Arrillaga/Sanchez Barrueco (et al.), Contribution to the Public Consultation on the evaluation of the European Disability Strategy 2010-20, Performance Review of the implementation of Regulation 181/2011/EU, 13 November 2019, Deusto Law School, p. 3.

European Commission with a list of designated terminals that are accessible for persons with disabilities and reduced mobility[674].

2.2.7 Intelligent Transport Systems Directive

598 According to the Intelligent Transport Systems Directive[675] (see above § 1.2.5.1 N 442 et seq.), multimodal travel information and planning services need to be accessible both in terms of the format in which the information is presented (i.e. compatibility with assistive devices, adhering to web accessibility guidelines, etc.), as well as covering specific information on accessibility of the journey, relevant to persons with reduced mobility (i.e. transfer times that are realistic and take into account the specific persons with reduced mobility abilities, etc.). The provision of information through accessible web and mobile services needs to be of specific quality[676][677].

2.2.8 European Accessibility Act

599 The Directive 2019/882 dated 17 April 2019 ("**European Accessibility Act**")[678] pays attention to accessibility of transport service information for persons with disabilities and as a complement of the sectorial passenger rights legislation, which covers also the assistance to be provided to passengers with disabilities and reduced mobility when travelling by air, rail, waterborne or bus and coach transport.

600 According to Art. 2 para. 2 European Accessibility Act, it applies to following services provided to consumers after 28 June 2025: […] elements of air, bus, rail and waterborne passenger transport services, except for urban, suburban and regional transport services for which only the last bullet point apply:

- websites;
- mobile device-based services including mobile applications;
- electronic tickets and electronic ticketing services;
- delivery of transport service information, including real-time travel information; this shall, with regard to information screens, be limited to interactive screens located within the territory of the Union; and
- interactive self-service terminals located within the territory of the Union, except those installed as integrated parts of vehicles, aircrafts, ships and rolling stock used in the provision of any part of such passenger transport services; […].

[674] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 14.

[675] Directive 2010/40/EU of the European Parliament and of 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.

[676] Web Content Accessibility Guidelines ("WCAG") 2.1 of level A, or even AA.

[677] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 15.

[678] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance), OJ L 151, 7.6.2019.

2.2.9 Trans-European Transport Network

601 The Regulation 1315/2013 as regards Union Guidelines for the development of the trans-European Transport Network ("**TEN-T**") aims to support the functioning of the internal market and to foster territorial, economic and social cohesion by reducing regional disparities. It combines and integrates transport infrastructure development and relevant transport policy aspects (such as rail interoperability, road safety or intelligent infrastructure components) enabling efficient, inclusive and sustainable transport solutions[679].

602 The TEN-T has been an important European legislation for improving accessibility of transport infrastructure for persons with disabilities, persons with reduced mobility and older persons.

603 A proposal for a revision of the TEN-T has been published by the European Commission on 14 December 2021[680] and amended in July 2022 due to Russia's war of aggression in Ukraine[681].

2.2.10 Overview tables

604 In the two following sub-sections, a table describing selected legislation and standards with their status, abbreviation, date, title, classification and comments can be found as reference to the elements discussed in the recommendations under § 3 N 0 et seq.

[679] European Commission, Revision of Regulation on Union Guidelines for the development of the trans-European transport network (TEN-T), Inception Impact Assessment, Ares(2020)6977996, 20 November 2020, p. 1.

[680] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A812%3AFIN (last consultation 31 August 2022).

[681] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13512-Development-of-trans-European-transport-TEN-T-network-in-light-of-war-in-Ukraine-amended-proposal-for-guidelines_en (last consultation 31 August 2022).

2.2.10.1 Accessibility legislation

Status	Abbreviation	Year	Title	Web link	Comments
active	PBefG		Passenger Transportation Act	https://www.gesetze-im-internet.de/pbefg/	
active	181/2011	2011	Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport and amending Regulation (EC) No 2006/2004	https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32011R0181&qid=1655896020039	
active	2019/882 (EAA)	2019	Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services	http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM%3A2015%3A615%3AFIN	for public transport see Art. 2 (2) c EAA
active	2016/2102/EU (WAD)	2016	Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies = Web Accessibility Directive	https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L2102	
active, proposal for repeal	1315/2013	2013	Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU Text with EEA relevance	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1315&qid=1656586484027	
Proposal	amendment of 2021/1153 and 913/2010, repeal of 1315/2013		Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Union guidelines for the development of the trans-European transport network, amending Regulation (EU) 2021/1153 and Regulation (EU) No 913/2010 and repealing Regulation (EU) 1315/2013	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:812:FIN	
active	661/2009	2009	Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (Text with EEA relevance)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009R0661&qid=1659610448061	

active	181/2011	2011	REGULATION (EU) No 181/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 February 2011 concerning the rights of passengers in bus and coach transport and amending Regulation (EC) No 2006/2004	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011R0181&qid=1659611067077	
active	1107/2006	2006	Regulation (EC) No 1107/2006 of the European Parliament and of the Council of 5 July 2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1107&from=EN	
active	1371/2007	2007	Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R1371&from=EN	
active	1177/2010	2010	Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010R1177&from=EN	
active	2008/57/EC	2008	Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0057&from=EN	

2.2.10.2 Accessibility standards

Status	Standard abbreviation	Year	Title	Classification	Comments
active	DIN 13278	2022	Smart mobility for persons with reduced mobility - Functional approaches	public transport	English version expected September 2022
active	DIN EN 301549 V3.2.1	2021	Accessibility requirements for ICT products and services	ICT	-
active, new proposal	DIN EN 16584-1	2017	Railway applications – Design for PRM use – General requirements – Part 1: Contrast	public transport	Draft published May 2022
active, new proposal	DIN EN 16584-2	2017	Railway applications – Design for PRM use – General requirements – Part 2: Information	public transport	Draft published May 2022
active, new proposal	DIN EN 16584-3	2017	Railway applications – Design for PRM use – General requirements – Part 3: Optical and friction characteristics	public transport	Draft published May 2022
active, new proposal	DIN EN 16585-2	2017	Railway applications – Design for PRM use - Equipment and components onboard rolling stock - Part 2: Elements for sitting, standing and moving	public transport	Draft published May 2022
active, new proposal	DIN EN 16585-3	2017	Railway applications – Design for PRM use - Equipment and components onboard rolling stock - Part 3: Clearways and internal doors	public transport	Draft published May 2022
active, new proposal	DIN EN 16586-1	2017	Railway applications – Design for PRM use - Accessibility of persons with reduced mobility to rolling stock — Part 1: Steps for access and egress	public transport	Draft published May 2022
active, new proposal	DIN EN 16586-2	2017	Railway applications – Design for PRM use - Accessibility of persons with reduced mobility to rolling stock — Part 2: Boarding aids	public transport	Draft published May 2022

active	DIN EN 16683	2016	Railway applications - Call for aid and communication device - Requirements	public transport	-
active	Guide TSI PRM	2015	Guide for the application of the PRM TSI	public transport	-
active, new proposal	TSI PRM - 1300/2014	2014	COMMISSION REGULATION (EU) No 1300/2014 of 18 November 2014 on the technical specifications for interoperability relating to accessibility of the Union's rail system for persons with disabilities and persons with reduced mobility	public transport	Draft published December 2021
active	ISO 19029	2016	Accessible design — Auditory guiding signals in public facilities	public transport	-
active	DIN EN 17285	2020	Railway applications - Acoustics - Measuring of door audible warnings	public transport	-
active	DIN EN 17478	2022	Transport Services — Customer communications for passenger transport services — A Universal Design approach	public transport	NA 023-00-02 GA N 2583
active, new proposal	DIN EN 16587	2017	Railway applications - Design for PRM Use - Requirements on obstacle free routes for infrastructure	public transport	-
active	DIN 32984	2020	Tactile walking surface indicators in public areas	Accessibility	-
active	DIN 32981	2018	Tactile and acoustic devices for blind and partially sighted persons on traffic signals - Requirements	public transport	-
active	DIN EN ISO 9241-171	2008	Ergonomics of human-system interaction - Part 171: Guidance on software accessibility	ICT	-
active	DIN 32974	2000	Acoustic signals in public traffic areas - Requirements	public transport	-
active	ISO 7731	2003	Ergonomics - Danger signals for public and work areas - Auditory danger signals	public transport	Warning signals for public areas with requirements for hearing function. Public transport is not affected.
active	ISO/TS 9241-126	2019	Ergonomics of human-system interaction — Part 126: Guidance on the presentation of auditory information	Accessibility	This document focuses on guidelines for presentation of information in the auditory modality.

active	ISO 9241-303	2011	Ergonomics of human-system interaction - Part 303: Requirements for electronic visual displays	ICT	Requirements for electronic displays. Does not handle accessibility for disabilities but to some extent visual impairment related to, for example, the elderly.
active	ISO 17049	2013	Accessible design - Application of braille on signage, equipment and appliances	Accessibility	Requirements for braille on signs, equipment and devices.
active	ISO TR 22411	2021	Ergonomics data for use in the application of ISO/IEC Guide 71:2014	Accessibility	This Technical Report presents ergonomics data and guidelines for applying ISO/IEC Guide 71 in addressing the needs of older persons and persons with disabilities in standards development. It provides: - ergonomics data and knowledge about human abilities - sensory, physical, cognitive abilities and allergies; - guidance on the accessible design of products, services and environments.
active	ISO 24505	2016	Ergonomics - Accessible design - Method for creating colour combinations taking account of age-related changes in human colour vision	Accessibility	Requirements for color combination in signs and displays adapted for all ages.
active	ISO 24508	2019	Ergonomics - Accessible design - Guidelines for designing tactile symbols and characters	Accessibility	The use of tactile information in a design requires proper

					consideration to best support human tactile senses so that the information is easily and correctly understandable. Guidelines for designing tactile symbols and characters based on ergonomic knowledge of human tactile abilities are therefore necessary for such design.
active	ISO 24509	2019	Ergonomics - Accessible design - A method for estimating minimum legible font size for people at any age	Accessibility	This document provides a method for estimating minimum legible font size for single characters, but not for words or sentences, in self-luminous or reflected mode, used in documents, products labels, signs, and displays for people at any age and in any viewing condition in which viewing distance, luminance and contrast are varied. This document applies designing and evaluating legibility of single characters for people at any age who have no pathological disorders in their eyes, but not for people with visual impairments such as low vision. The application is

					specifically directed to, but not limited to, the cases of printed materials where fixed font size is used. Applicability of the method to other languages is given in Annex F.
active	ISO/IEC Guide 71	2014	Guide for addressing accessibility in standards	Accessibility	Guide for standard developers with requirements and recommendations for accessibility related to products, services and the built environment.

2.2.11 National laws related to accessibility

605 National laws and regulations related to accessibility differ amongst European countries. Some Member States have widely integrated accessibility into their legislation and enforcement practices, while others need to make further progress in order to be fully aligned with international and European legislation[682].

606 For more details about national legislation on transport issues, it can be referred to the European Commission's Disability Online Tool[683] or to the European study "Mapping and Performance Check of the Supply of Accessible Tourism Services"[684].

607 In addition to European regulations, many Member States also have national technical standards and norms in place, but they are usually inconsistent. In response to these rules, as well as on their own initiative, actors in the transport sector (not only operators, also infrastructure owners for example) have implemented a diverse set of practices to accommodate the wishes and needs of PRMs[685].

* * *

[682] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 15.

[683] https://www.disability-europe.net/dotcom (last consultation 31 August 2022).

[684] European Commission, Mapping and performance check of the supply of accessible tourism services: final report, Publications Office, 2015, https://data.europa.eu/doi/10.2873/584417 (last consultation 31 August 2022).

[685] European Commission (Breemersch et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018, p. 20.

3 Overview of the legal framework as regards data and vehicle communications

3.1 Introduction

608 From an economical point of view, data is a non-rival good, in the same way than street lights or a scenic view: many people can access them at the same time, and it can be "consumed" over and over again, without impacting their quality or running the risk that supply will be depleted. Many figures demonstrating that the volume of data is constantly growing exists. For instance, according to studies, a growth from 33 zettabytes[686] generated in 2018 to 175 zettabytes is expected in 2025. It is an untapped potential, as 80% of industrial data is actually never used[687]. Data is often described as the "new oil of the 21st century".

609 Automated vehicles and minibuses can be considered, in most of their use cases, as connected vehicles, as they are able to communicate with various infrastructures. In the following sections, it will be assumed as a working hypothesis that automated vehicles are also connected vehicles.

610 At international level within UNECE, in the discussion about access to data from (automated) vehicle operations, two levels have been distinguished and will be regulated differently: the interface including data security, which should be the subject of regulation under WP.29, and the use of vehicle data including (personal) data protection, which is to be regulated at regional/national level (European Union, United States of America, China etc.).

611 The European legal framework related to data is structured at the same time by :

- Cross-sectoral (or horizontal) acts, which apply across various sectors and industries: the General Data Protection Regulation ("**GDPR**"), the Data Governance Act ("**DGA**"), the (draft) Data Act ("**DA**"), the Digital Markets Act ("**DMA**") etc.;
- Sectoral acts, dedicated to the transport sector, such as the Intelligent Transport Systems Directive and type-approval related acts (such as the revised General Safety Regulation, the Delegated Regulation on road safety-related minimum universal traffic data etc.) that also contains provisions related to the processing, recording etc. of data.

[686] One zettabyte is equal to a trillion gigabytes.

[687] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (last consultation 31 August 2022).

3.2 European data strategy and related acts

3.2.1 European Data Strategy

3.2.1.1 Overview

612 The European Commission has published its data strategy in February 2020. It constitutes an important milestone for the posterior data oriented regulations. The European strategy for data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty[688].

613 According to the European Commission, the European Data Strategy rests on four main pillars:

- a cross-sectoral governance framework for boosting data access and use;
- significant investments in European federated cloud infrastructures and interoperability;
- empowering individuals and SMEs in the European Union with digital skills and data literacy;
- the creation of common European Data Spaces in crucial sectors and public interest domains, through data governance and practical arrangements[689].

3.2.1.2 Importance of data for connected and automated vehicles

614 The European Commission considers that transport and mobility are at the forefront of the debate on data sharing. This concerns the automotive sector, where connected cars critically depend on data. Digitalisation and data in all modes of transport and in logistics will be an essential component of further work on the "European Transport System". The European Commission plans to take actions for cross-modal data sharing logistics and passengers ecosystems[690].

615 The European Commission intends to take use of modern vehicles that can generate up to 25 gigabytes of data every hour, which can be used for innovative mobility-related services and for repair and maintenance services[691].

616 In the same time, the European Commission highlights that there is currently not enough private sector data available for use by the public sector to improve evidence-driven policy-making and public services, such as mobility management[692].

---

[688] https://digital-strategy.ec.europa.eu/en/policies/strategy-data (last consultation 31 August 2022).

[689] https://fpf.org/blog/itpi-event-recap-the-eu-data-strategy-and-the-draft-data-governance-act/ (last consultation 31 August 2022).

[690] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions – a European strategy for data, COM(2020) 66 final, dated 19 February 2020, p. 27.

[691] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions – a European strategy for data, COM(2020) 66 final, dated 19 February 2020, p. 27.

[692] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions – a European strategy for data, COM(2020) 66 final, dated 19 February 2020, p. 7.

3.2.1.1 European mobility data space

617 The sector of mobility is one of nine strategic areas (besides health, energy and industrial manufacturing etc.) where the European Union intends to create a shared European data space. The aim of these common European data spaces is to ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control[693].

618 The mobility and transport sector has an important acquis of existing European frameworks (some of which are regulated) that organise data sharing for both passengers and freight in the domains of business-to-business ("B2B"), business-to-government ("B2G"), government-to-business ("G2B") and government-to-government ("G2G") data sharing. Most of these frameworks have their own governance, architecture, platforms, etc. and they already include some important achievements as regards the harmonisation of data-sharing conditions. This will be duly taken into account in the approach to the European mobility data space[694].

619 In addition, various digital initiatives at European level, driven by Member States or by private actors, seek to provide the data governance, technical infrastructure and economic models to create a data economy in the mobility sector[695].

620 The common European mobility data space will build upon existing European and Member States' legislation and infrastructures related to transport data. It should focus on promoting interoperability by contributing tools to support convergence on governance and infrastructure. Particular attention should be paid to enabling data sharing with linked sectors such as buildings, energy, environment or health, for example to fully leverage the benefits of e-mobility[696].

621 The legal framework of relevance for this data space is in constant evolution. The Sustainable and Smart Mobility Strategy announced future legislative initiatives related to the sharing of mobility data as well as the adaptation of existing frameworks in the area of mobility. These legislative initiatives would also contribute to the development of the mobility data space[697].

622 In the automotive sector, as mentioned above (see Appendix A § 1.2.2.4 *supra*), the type-approval legislation provides for conditions of access of third party service providers to repair and maintenance information. This legislation is currently under review (as of July 2022)[698] and will presented in further details below (see § 3.2.5 below).

---

[693] https://digital-strategy.ec.europa.eu/en/policies/strategy-data (last consultation 31 August 2022).

[694] European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23 February 2022, § 6.3 p. 18.

[695] European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23 February 2022, § 6.3 p. 18.

[696] European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23 February 2022, § 6.3 p. 18.

[697] European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23 February 2022, § 6.3 p. 18.

[698] European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23 February 2022, § 6.3 p. 18.

623 As regards the timeline, the European Commission presented a roadmap in December 2021[699] and it intends to present a concept and strategy to establish the mobility data space in 2022 and follow-up actions will be adopted between 2022 and 2024.

3.2.2 The Data Governance Act

624 The Data Governance Act[700] ("**DGA**") is a cross-sectoral act published on 30 May 2022. It will enter into force on 24 September 2023[701]. It is based on Art. 114 TFEU and will be directly applicable within European Member States.

3.2.2.1 Overview

625 The overarching principle underlying the DGA is that data should be Findeable, Accessible, Interoperable and Re-usable (so-called "FAIR data principles"[702]).

626 The DGA intends to address following situations:

- Making public sector data available for re-use, where data is subject to rights of others (e.g. privacy rights, intellectual property rights and trade secrets);
- Sharing of data amongst businesses, against remuneration in any form;
- Use of personal data with the help of a "personal data-sharing intermediary"; designed to help individuals exercise their rights under the GDPR (through data rooms or data wallets);
- Allowing data use on altruistic grounds[703].

3.2.2.2 Re-use of protected data held by public sector bodies

627 Chapter II of the DGA (Art. 3 to 8 DGA) creates a mechanism for re-using certain categories of protected data held by public sector bodies, which is conditional on the respect of the rights of others (notably on grounds of protection of personal data, but also protection of intellectual property rights and commercial confidentiality).

628 This mechanism is without prejudice to sector-specific European legislation on access to and the re-use of this data. The re-use of such data falls outside the scope of the Directive 2019/1024 (Open Data Directive, see § 3.4.1 below)[704].

---

[699] https://digital-strategy.ec.europa.eu/en/events/workshop-common-european-mobility-data-space (last consultation 31 August 2022).

[700] Regulation 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation 2018/1724.

[701] Art. 38 DGA.

[702] See Recital 2 of the DGA.

[703] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25 November 2020, p. 1.

[704] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25 November 2020, p. 7.

629 The DGA does not create a right to re-use such data, but provides for a set of harmonised basic conditions under which the re-use of such data may be allowed (e.g. the requirement of non-exclusivity[705]).

630 Public sector bodies allowing this type of re-use would need to be technically equipped to ensure that data protection, privacy and confidentiality are fully preserved. Therefore, Member States will have to set up a single contact point supporting researchers and innovative business in identifying suitable data[706]. They are also required to put structures in place to support public sector bodies with technical means and legal assistance (see Art. 7 DGA)[707].

631 Public sector bodies which allow re-use of data may charge fees for allowing the re-use of such data. These fees shall be non-discriminatory, proportionate and objectively justified and shall not restrict competition (Art. 6 para. 2 DGA).

3.2.2.3 Data intermediation

632 Data intermediation services (Chapter III, Art. 10 to 15 DGA) are a business model covered by the DGA which aims to enable companies and individuals to share data. These services can take the form of digital platforms that allow companies and individuals to freely share or control their data and exercise their rights[708].

633 Many companies currently fear that sharing their data would imply a loss of competitive advantage and represent a risk of misuse. The DGA therefore defines a set of rules for providers of data intermediation services (so-called data intermediaries, such as data marketplaces) to ensure that they will function as trustworthy organisers of data sharing or pooling within the common European data spaces. In order to increase trust in data sharing, this new approach proposes a model based on the neutrality and transparency of data intermediaries[709].

634 The approach of the DGA is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services (Art. 13 and 14 DGA)[710].

635 According to Art. 10 and 11 DGA, data intermediation services providers are required to submit a notification to the competent authority. It is not an approval but a mechanism to determine the conditions

[705] Art. 4 DGA "Prohibition of exclusive arrangements".

[706] Art. 8 DGA "Single information point".

[707] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25 November 2020, p. 7.

[708] https://www.cnil.fr/en/european-strategy-data-cnil-and-its-counterparts-comment-data-governance-act-and-data-act (last consultation 24 August 2022).

[709] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#ecl-inpage-l4ihlqt9 (last consultation 24 August 2022).

[710] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25 November 2020, p. 7.

for the data intermediary services and establish supervisory control for the compliance with the conditions.

636 The DGA lays down a number of requirements for providers who engage in this activity, such as:

- The data intermediation services provider may not itself use the data for which it acts as an intermediary (Art. 12 litt. a DGA). It only facilitates the exchange of data in the format in which it receives them and converts them only to improve interoperability or at the user's request (Art. 12 litt. c DGA);
- It may offer additional services to facilitate data exchange (temporary storage, anonymisation and pseudonymisation etc., see Art. 12 litt. e DGA);
- The data intermediation services provider may not make its commercial conditions dependent on the use of other services it provides (Art. 12 litt. b DGA);
- It must have procedures in place to prevent fraudulent or abusive access to data via its services (Art. 12 litt. g DGA);
- If the data intermediation services provider becomes insolvent, it should ensure reasonable continuity of its services to enable data subjects and data holders to access, transfer or retrieve their data (Art. 12 litt. h DGA);
- It must ensure the security of data in its storage, processing and transmission (Art. 12 litt. l DGA);
- The data intermediation services provider shall act in the best interests of data subjects when facilitating the exercise of their rights, by informing and advising them in a concise, transparent, comprehensible and easily accessible manner about the use of their data (Art. 12 litt. m DGA);
- It shall keep a log of the data intermediation activity (Art. 12 litt. o DGA).

3.2.2.4 European Data Innovation Board

637 The DGA also sets out conditions for the creation of a new European Data Innovation Board ("**EDIB**", see Chapter VI), an expert group including representatives from all Member State competent authorities, the European Data Protection Board, the European Data Protection Supervisor and ENISA (amongst others, see Art. 29 para. 1 DGA).

638 The tasks of the EDIB are largely advisory, helping to set up consistent practices and procedures and advising the Commission in a number of areas, including cybersecurity, cross-border data sharing, interoperability and cross-sector standards and guidance[711].

3.2.2.5 Influence on automated vehicles

639 Although its concrete impact and application (both in general and in the field of automated vehicles) is currently unclear, the DGA's mechanism of re-using certain categories of protected data is interesting for the sector of automated vehicles. As mentioned previously, sharing mobility data is very important (as presented in the AVENUE vision) and controllers of mobility data might invoke data protection on various grounds (intellectual property rights, trade secrets, personal privacy, contractual clauses etc.) in order to avoid the sharing of their mobility data. Therefore, any mechanism that would allow to overcome this hurdle is welcome.

[711] https://www.taylorwessing.com/fr/insights-and-events/insights/2022/06/radar---ec-data-governance-act-will-apply-from-24-september-2023 (last consultation 31 August 2022).

640 The same applies to the data intermediation services, as this business model aims to enable companies and individuals to share data. Similar structures might be applied and applicable in the field of automated vehicles.

641 The DGA's European Data Innovation Board is an institution that is similar to cooperation platforms between authorities that ought to be created at European level in the field of automated vehicles.

3.2.3 The Digital Markets Act

642 The Digital Markets Act[712] ("**DMA**") aims to ensure that no large online platform, that acts as a "gatekeeper" for a large number of users, abuses its position to the detriment of companies wishing to access such users[713].

643 The European Parliament has adopted the text of the Digital Market Act early July 2022[714] and it has been approved by the European Council on 18 July 2022[715]. It will enter into force on the twentieth day following this publication and will apply six months after its entry into force (Art. 54 DMA), which is expected to happen in February 2023[716].

644 The DMA forms a "package" of digital legislation together with the Digital Services Act. The latter will not be studied in this deliverable, as it intends to improve content moderation on social media platforms.

3.2.3.1 Designation of gatekeepers

645 The DMA's threshold is very high and, apart from exceptional cases, does not concern SMEs. According to Art. 3 para. 1 DMA, an undertaking shall be designated as a gatekeeper if, amongst others:

- it has a significant impact on the internal market;
- it provides a core platform service which is an important gateway for business users to reach end users; and
- it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

646 If a platform has good arguments against its designation as a gatekeeper, it can challenge the designation by means of a specific procedure that enables the European Commission to check the validity of those arguments[717] (Art. 3 para. 5 DMA).

---

[712] Regulation 2022/… of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 2020/0374(COD) as of 24 August 2022.

[713] https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/ (last consultation 31 August 2022).

[714] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4313 (last consultation 31 August 2022).

[715] https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/dma-council-gives-final-approval-to-new-rules-for-fair-competition-online/ (last consultation 31 August 2022).

[716] https://www.simmons-simmons.com/en/publications/cl5qyuy0o1h0y0a59y4osbiqx/the-digital-markets-act-is-adopted-by-the-council (last consultation 31 August 2022).

[717] https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/ (last consultation 31 August 2022).

3.2.3.2 Obligations for gatekeepers

647 Amongst others, Art. 5 para. 2 DMA prohibits gatekeepers from:

- processing, for the purpose of providing online advertising services, personal data of end users using services of third-parties that make use of core platform services of the gatekeeper;
- combining personal data from the relevant core platform service with personal data from other core platform services or from any other services provided by the gatekeeper or with personal data from third-party services;
- cross-using personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice-versa; and
- signing in end users to other services of the gatekeeper in order to combine personal data,

3.2.3.3 Open APIs

648 Gatekeepers must allow business users and providers of ancillary services with access to and interoperability of with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services[718], free of charge (see Art. 6 para. 7 DMA and Recital 57).

3.2.3.4 Enforcement and fines

649 To ensure a high degree of harmonisation in the internal market, the European Commission will be the sole enforcer of the DMA (Recital 91 and Art. 20 et seq. DMA). The Commission can decide to engage in regulatory dialogue to make sure gatekeepers have a clear understanding of the rules they have to abide by and to specify their application where necessary (Recital 65)[719].

650 An advisory committee (Art. 50 DMA) and a high-level group (Art. 40 DMA) will be set up to assist and facilitate the work of the European Commission. Member states will be able to empower national competition authorities to start investigations into possible infringements and transmit their findings to the Commission (Recital 91)[720].

651 To make sure that gatekeepers do not undermine the rules set out in the DMA, the regulation also enforces anti-circumvention provisions (Art. 13 DMA)[721].

652 If a gatekeeper violates the rules laid down in the legislation, it risks a fine of up to 10% of its total worldwide turnover (Art. 30 para. 1 DMA). For a repeated offence, a fine of up to 20% of its worldwide turnover may be imposed (Art. 30 para. 2 DMA)[722].

---

[718] https://www.pwc.ch/en/insights/regulation/dma-implication.html#sectionx (last consultation 31 August 2022).

[719] https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/ (last consultation 31 August 2022).

[720] https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/ (last consultation 31 August 2022).

[721] https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/ (last consultation 31 August 2022).

[722] https://www.consilium.europa.eu/en/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/ (last consultation 31 August 2022).

3.2.3.5 Influence on automated vehicles

653 With the current definition, it does not seem that stakeholders from the automated vehicles industry would qualify as gatekeepers in the short term.

654 Nevertheless, a recent study highlighted various parallels between gatekeepers under the DMA and manufacturers of connected and automated vehicles:

- vehicle manufacturers, like large online platforms, benefits from access to and control of vast amounts of data collected from connected and automated vehicles;
- vehicle manufacturers became *de facto* intermediaries between vehicle users and third-parties (independent service providers), as it happens with regard to very large online platforms and business users leveraging the platform to connect with end-users (see also § 3.2.5 below);
- when providing data driven services to vehicle users, independent service providers need to access data held by vehicle manufacturers. As a result, vehicle manufacturers (similarly to online platforms), have the ability to connect independent service providers with end-users. Under these circumstances, vehicle manufacturers can leverage their central position and access to data to prioritize the portfolio of their services, as they play a dual role as platform operator and service provider[723].

3.2.4 The Data Act

655 The Data Act proposal ("**DA**") has been published on 23 February 2022 by the European Commission. After the Data Governance Act and the Digital Market Act, the Data Act is the last horizontal building block of the European Commission's data strategy.

656 Similarly to the DGA, the Data Act aims to address the problem of insufficient availability of data for use within the European economy. This insufficient availability is caused mainly by the lack of clarity on data rights, imbalances in negotiating power, limited access to fair and trustworthy cloud services and a lack of cross-sector data interoperability in the European Union[724].

657 Therefore, the goal of the Data Act is to "maximize the value of data in the economy and society by ensuring that a wider range of stakeholders gain control over their data and that more data is available for use, while maintaining incentives to invest in data generation"[725].

658 The Data Act proposal is often described as the private sector's equivalent of the Open Data Directive (see § 3.4.1 below).

3.2.4.1 Overview

659 The draft of the Data Act pursues both ambitious and challenging goals.

---

[723] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 103.

[724] Commission Staff Working Document, Executive Summary of the Impact Assessment Report, SWD(2022) 35 final, Brussels, 23 February 2022, p. 1.

[725] Commission Staff Working Document, Executive Summary of the Impact Assessment Report, SWD(2022) 35 final, Brussels, 23 February 2022, p. 1.

660 First, it seeks to encourage business-to-business data-sharing transactions, especially in the context of future (and yet largely undefined) data spaces (including the mobility data space) and industrial value chains. It does so by seeking to provide enhanced legal certainty and introducing provisions that prevent larger incumbents from exploiting their bargaining power by restricting data flows, or appropriating the lion's share of the contractual surplus[726].

661 Second, the draft of the Data Act seeks to reduce so-called "vendor lock-in" problems, by giving smaller companies and individuals portability rights on their data, in an attempt that echoes a similar measure introduced by the GDPR. The draft also introduces a general obligation to keep devices and data separate, allowing end users to switch to alternative cloud/edge services providers for the data generated by their devices, without depending on the integrated device vendor[727].

662 Third, the draft of the Data Act goes further by providing that when a user wishes to transfer data services to competing providers, the data holder should ensure that data are shared in fair, reasonable and non-discriminatory conditions. This provision seems to generalise the approach adopted by the European Union in sector-specific legislation, such as the Second Payment Services Directive ("**PSD2**"), where banks were obliged to transfer data to third party providers through an Open Application Programming Interface, with the consent of the customer (see § 3.4.4 below). In addition, service providers are requested to take action to ensure that outgoing customers maintain "functional equivalence" after they have switched to another provider[728].

663 Fourth, the draft of the Data Act ventures into the content of contracts for the sharing of data between businesses, in an attempt to promote fairness and avoid contractual agreements built on imbalances in negotiating power between the contractual parties. Following a consolidated tradition in European law, dating back at least to Directive 93/13 on unfair terms in consumer contracts, the proposed "unfairness test" includes both a general provision and a list of clauses that are either always unfair ("black list") or presumed to be unfair ("grey list'"). Unfairness, when found, impedes the use of data by both contractual parties[729].

664 Fifth, the draft of the Data Act introduces interoperability provisions by empowering the European Commission, with the support of standardisation bodies, to intervene with common specifications to promote the interoperability of data processing services, to facilitate the pooling of data (e.g. in data spaces or data provision "for good") and promote easier switching across data providers. These provisions will apply in particular to smart contracts for data spaces, as already announced in the Commission's annual strategy on standardisation for 2022[730].

3.2.4.2 Application to automated vehicles

665 According to Art. 1 para. 2 DA, the Data Act will apply to, amongst others :

[726] https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/ (last consultation 31 August 2022).
[727] https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/ (last consultation 31 August 2022).
[728] https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/ (last consultation 31 August 2022).
[729] https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/ (last consultation 31 August 2022).
[730] https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/ (last consultation 31 August 2022).

- manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services (litt. a);
- to data holders that make data available to data recipients in the European Union (litt. b);
- to data recipients in the European Union to whom data are made available (litt. c).

666 Products are defined as a tangible, movable item that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data (Art. 2 para. 2 DA).

667 Therefore, it seems likely that the Data Act will apply in the field of automated vehicles, for instance to manufacturers of automated vehicles according to Art. 1 para. 2 litt. a DA as manufacturers of products that collect data concerning their use and their environment, for instance.

During its consultation period, the proposal of the Data Act triggered many reactions from stakeholders of the automotive industry, with often opposing points of view:

- Some stakeholders (mostly vehicle manufacturers) requested restrictions of the scope of data and the possibilities of third parties to commercialize it. They also pleaded for more protection of vehicle data and functions under trade secrets and asked for additional legal grounds for their own data processing activities[731];
- Others stakeholders (mostly independent service providers) called for a broader scope of data to be included and recommended the expansion of the favourable provisions for SMEs regarding compensation and protection against unfair terms to all stakeholders. They are concerned that the vehicle manufacturers could abuse trade secret protection strategically to impede data sharing obligations[732].

668 Various voices have considered that the Data Act will not be able to ensure a level playing field between vehicle manufacturers and independent service providers with respect to access to in-vehicle data and resources[733].

669 This point of view has been shared by the European Commission, which acknowledges that the Data Act will have a major impact on the mobility ecosystem, boosting innovation and competition in aftermarkets, other automotive or electric vehicles related services, but that it might need to be complemented by more specific provisions for the automotive sector[734]. The European Commission has therefore launched in Spring 2022 the public consultation as regards a proposal for a regulation on access to vehicle data, functions and resources[735].

---

[731] GILL, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 16 May 2022, p. 7.

[732] GILL, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 16 May 2022, p. 7.

[733] GILL, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 16 May 2022, p. 1; FIGIEFA, European Commission's proposal for Data Act welcomed, but robust automotive-specific legislation urgently required, Brussels, 23 February 2022.

[734] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 1.

[735] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en (last consultation 31 August 2022).

3.2.5 Proposal for a regulation on access to vehicle data, functions and resources

670 The European Commission has opened a public consultation as regards a regulation on access to vehicle data, functions and resources between 29 March and 2 August 2022 and schedules the adoption of this act for the fourth quarter of 2022[736].

3.2.5.1 Goal

671 This initiative of the European Commission aims to set the conditions for accessing and using in-vehicle data generated by modern vehicles. It aims to enable clear and competition-friendly European rules for services that are based on access to car data, for instance:

- repair and maintenance;
- car sharing;
- mobility as a service;
- insurance[737].

3.2.5.2 Overview and issues to be solved

672 Access to data, functions and resources is crucial for the development of innovative data-driven mobility services. Public authorities also need access to data, functions and resources to perform their tasks, such as CO^2 monitoring, ensuring compliance with pollutant emissions regulations or doing roadworthiness controls[738].

673 However, today, although vehicles generate huge amounts of data, the access to these data is limited and not standardised. At the same time, it is essential that access to vehicle data, functions and resources do not create new risks for cybersecurity, road safety, intellectual property or data protection[739].

674 As mentioned above, the proposal for the Data Act will empower users by giving them the right to have access to vehicle data and the right to share the data with third parties. However, the Data Act provisions may not go into sufficient details of access to functions and resources, crucial for the provision of data-dependent services in the automotive sector[740].

---

[736] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources/feedback?p_id=29298097 (last consultation 31 August 2022).

[737] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en (last consultation 31 August 2022).

[738] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

[739] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

[740] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

675 Furthermore, problems with the disparity of available data and access modes across vehicle brands, as well as the interplay between access to data and relevant cybersecurity and safety measures, are so closely linked to the nature of connected products (in this case, vehicles) that they can not be addressed with cross-sectoral legislation[741].

676 This means that, to ensure the Data Act is properly implemented in the automotive/mobility ecosystem, its principles could be complemented by measures to standardise the data sets concerned and to ensure access not only to data, but also vehicle functions and resources, as well as by rules ensuring effective, non-discriminatory, safe and secure access allowing for fair competition, notably for aftermarket and mobility services[742].

677 According to a recent study[743], better use of car data, resources and functions by all stakeholders could result in higher quality and cheaper data-based services for consumers. It could also lead to the high take-up of such services, to the benefit of consumer welfare and innovation[744].

3.2.5.3 Proposed options

678 The European Commission proposes four different possibilities, in a nutshell:

- No sectorial intervention at European level. The existing legislation would apply (access to vehicle repair data according to the AMSVR, Data Act and cross-sectoral competition rules, amongst others);
- The creation of equal and non-discriminatory access rights and transparency measures;
- The same than above, with an additional minimum list of data, functions and resources to be made available;
- The same than above, with additional governance provisions on access to this data[745].

679 For the reasons described in different chapters of this deliverable and in the AVENUE vision and in accordance with other studies[746], the last scenario seems to be largely desirable from a societal point of view.

[741] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

[742] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

[743] MARTENS/MUELLER-LANGER, Access to Digital Car Data and Competition in Aftermarket Maintenance Services, Journal of Competition Law and Economics, ISSN 1744-6414, 16 (1), 2020, JRC119621, p. 116-141.

[744] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

[745] European Commission, Access to vehicle data, functions and resources, Call for evidence for an Impact Assessment, Ares(2022)2302201, 29 March 2022, p. 2.

[746] See also Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 3.

3.2.6 Artificial Intelligence Act

3.2.6.1 Introduction

680 As part of its digital agenda, the European Commission has published a "Proposal for a regulation laying down harmonised rules on artificial intelligence (AI)"[747] ("**AI Act**") in April 2021. The European Commission emphasised that its approach is shaped by European values and risk-based, ensuring both safety and fundamental rights protection[748]. This proposal has led to many discussions and reactions from different stakeholders.

681 The AI Act is the world's first attempt to get a legislative grip on the phenomenon of Artificial Intelligence ("AI"). The proposal follows a risk-based approach and imposes regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety[749].

682 With its proposal for an AI Regulation, the European Commission is pursuing a horizontal approach that, unlike other European product safety legislation, is not sector-specific but relates to the use of AI in general. In this way, the European Commission hopes that the regulation will be "comprehensive and future-proof" with "flexible mechanisms that enable it to be dynamically adapted as the technology evolves and new concerning situations emerge"[750].

683 AI systems are defined by the AI Act proposal as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" (Art. 3 para. 1 Draft AI Act).

684 It should be noted that the AI Act does not directly apply to motor vehicles, but empowers the European Commission to amend the type-approval legislation to implement the principles of the AI regulation[751].

---

[747] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021)206 final, 21 April 2021.

[748] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 1.

[749] EBERS, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022, § 6 p. 22.

[750] EBERS, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022, § 4.1 p. 13 and the quoted reference.

[751] Meeting minutes of the 12th meeting of the subgroup of the motor vehicles working group on "Automated and connected vehicles", Brussels, 24 March 2022, https://circabc.europa.eu/sd/a/fb8f9b2d-e81e-440e-83ff-99fdd3696d3f/ACV%2018-02-22%20minutes%20rev%202.pdf, § 4 p. 2 (last consultation 31 August 2022).

3.2.6.2 Banned unacceptable AI practices

685 In its AI Act Proposal, the European Commission proposes to completely prohibit particular types of unacceptable AI systems, such as AI systems that manipulates persons or exploit the fragility of vulnerable persons, that may serve for social scoring by governments, exploitation of vulnerabilities of specific groups of persons such as children, that use subliminal techniques etc. (see Art. 5 Draft AI Act).

3.2.6.3 Regulation of high-risk AI systems

686 High-risk AI systems should be permitted on the European market; however, they are subject to compliance with mandatory requirements and an *ex ante* conformity assessment before they can be put on the market (Art. 8 et seq. AIA)[752].

687 Providers of high-risk AI systems are therefore subject to various obligations and must maintain sound risk management systems. They must feed the AI system with training, validation and testing data that meets specific quality requirements and are handled through appropriate data governance and management practices. Users must comply with the instructions and report to the provider/distributor any serious incident or malfunctioning, which could lead to a breach of fundamental rights[753].

688 If the high-risk AI system is part of a product which is subject to a third-party conformity assessment under the European product safety framework, compliance will be addressed in the context of that conformity assessment[754].

689 Automated vehicles are likely to be classified as high risk AI systems[755].

3.2.6.4 Market surveillance and penalties

690 Providers of high-risk AI systems must establish and document an appropriate post-market monitoring system to continuously check compliance with regulatory requirements ("*ex post* market surveillance"). They must report serious incidents and malfunctioning to the market surveillance authority of the Member State where the incident or the associated breach of fundamental rights occurred[756].

---

[752] EBERS, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022, § 4.1 p. 14.

[753] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 1.

[754] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 2.

[755] https://www.lexisnexis.co.uk/legal/guidance/automated-vehicles-key-legal-issues-in-the-eu (last consultation 31 August 2022)

[756] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 2.

691 Market surveillance authorities must require the relevant operators to take appropriate measures or even to withdraw the AI system when the AI system is in breach of the regulation or when the AI system, while in line with the regulation, presents a risk for health, safety, human rights or a public interest[757].

692 Fines for non-compliance can be very high, up to EUR 30 million or, if the offender is a company, up to 6% of its total worldwide annual turnover for the preceding financial year[758].

693 National competent authorities must be appointed for the "application and implementation" of the AI Act. A national supervisory authority is to be designated amongst them to act as market surveillance authority. The consistent application of the AI Act is to be ensured by a European Artificial Intelligence Board, chaired by the Commission and composed of the European Data Protection Supervisor and representatives of the national supervisory authorities. The European Artificial Intelligence Board collects and shares best practices and takes a position on emerging issues for the implementation and enforcement of the regulation[759].

3.2.6.5 No national regulations

694 The AI Act in the proposal's form does not allow Member States to regulate this technology at national level, as the European Commission has explicitly chosen the instrument of a regulation based on the internal market clause (Art. 114 TFEU) to prevent fragmentation of the internal market. This is particularly relevant considering how wide a concept of "AI system" the regulation embraces[760].

695 The new rules would apply directly to both public and private actors inside and outside the European Union as long as the AI system is placed on the Union market or its use affects people located in the European Union (Art. 2 para. 1 Draft AI Act), similarly to the GDPR.

3.2.6.6 Regulatory sandboxes

696 An interesting novelty introduced by the AI Act proposal is the creation of AI "regulatory sandboxes" (Art. 53 et seq. Draft AI Act).

3.2.6.6.1 Concept

697 The term "regulatory sandbox" can be traced back to financial technologies, where regulatory sandboxes have existed since 2014, mainly in the United Kingdom[761].

698 A regulatory sandbox is a tool allowing businesses to explore and experiment with new and innovative products, services or businesses under a regulator's supervision. It provides innovators with incentives to

[757] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 2.

[758] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 2.

[759] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 2.

[760] ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021, p. 2.

[761] POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021, p. 1 and the quoted reference.

test their innovations in a controlled environment, allows regulators to better understand the technology and fosters consumer choice in the long run. However, regulatory sandboxes also come with a risk of being misused or abused and need the appropriate legal framework to succeed[762].

699 The Draft AI Act does not provide a definition, but Art. 54 states that AI regulatory sandboxes "shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time". In order to understand the concept of AI regulatory sandboxes, one has to explore how it fits within the broader notion of experimental lawmaking[763], which will now be briefly described.

3.2.6.6.2 Characteristics of experimental legal regimes

700 An experimental legal regime (or experimental approach to legislation) encourages actors to test new technologies or services in a real-life environment. Three main features characterise an experimental legal regime:

- a temporary nature (limited duration);
- a trial-and-error approach to regulation and
- the collaborative involvement of the stakeholders and competent authorities in the process[764].

701 In practice, an experimental legal regime (or an AI regulatory sandbox) requires the applicant to present a proposal that would explain the objectives, process and expected results to the competent authority, as well as details such as sample size and experimental period length[765].

702 Legal experimentation can be divided into two key types: experimenting by derogation and experimentation by devolution:

- Experimenting by derogation implies that certain rules or regulations are put aside to complete the experiment. It requires the legislator to include an experimental clause in a legislative basis to enable the experiment to derogate from a specific law.
- Experimentation by devolution requires a national or supranational government to empower the local government to establish a regulation or law in a particular area relevant to the experiment. It allows policy differentiation between government levels, so that decisions can be taken at a local level taking into account local preferences and needs. Thus, devolution potentially creates a policy laboratory and stimulates innovation[766].

703 Regulatory sandboxes make it possible to test new technologies transparently and contribute to evidence-based lawmaking. From a market actor perspective, one of the main benefits is the additional flexibility in terms of the regulatory burden. In addition, the controlled environment of regulatory sandboxes is

[762] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733544 (last consultation 31 August 2022).

[763] POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021, p. 1.

[764] POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021, p. 2.

[765] POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021, p. 2.

[766] POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021, p. 2 and the quoted reference.

particularly accommodating to products and services that do not easily fit in the traditional regulatory framework[767], such as it is the case for automated vehicles.

704 Nonetheless, some concerns have been raised amongst others regarding the interplay between Art. 54 Draft AI Act and the GDPR. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have recommended (i) to clarify the scope and objectives of the regulatory sandboxes and (ii) that the Proposal should also clearly state that the legal basis of the regulatory sandboxes should comply with the requirements established in the existing data protection framework[768].

705 In addition, for automated vehicles, the question of creating regulatory sandboxes (that are very desirable in this field) should be carefully assessed in order to avoid a trade-off that might lower safety and create unacceptable risks.

3.3 Intermediary remarks

706 In conclusion, interesting and promising acts have been adopted and/or are currently in the process of being published, but their interplay with the existing framework (and in particular the GDPR) seems to be the source of questions and uncertainty. The mobility sector and automated vehicles in particular might need a specific piece of legislation dedicated to data, as the acts seen above are mostly horizontal/cross-sectoral (with the exception of the proposal for a regulation on access to vehicle data) and their application and effects on automated vehicles and minibuses is unclear yet.

[767] POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021, p. 2 and the quoted reference.

[768] European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, p. 3 and p. 17.

3.4 "Non-personal" data and open data

707 Before presenting the framework for personal data, we will provide an overview of the framework as regards non-personal data and open data, as the frameworks applying to this type of data are less stringent than for personal data.

3.4.1 Open Data Directive

708 Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information ("**PSI Directive**" or "**Open Data Directive**") entered into force on 16 July 2019 and replaces Directive 2003/98/EC as of 17 July 2021, which was amended by Directive 2013/37/EU.

709 Member States had until 17 July 2021 to transpose the Open Data Directive into their national law (Art. 17 para. 1 Open Data Directive).

3.4.1.1 Principles

710 The Open Data Directive is based on the general principle that public-sector information held by public-sector bodies or public undertakings, and publicly funded research data, should be reusable for commercial and non-commercial purposes, free of charge or at marginal costs. Public sector bodies are furthermore required to make dynamic data[769] available for re-use immediately after collection, via suitable Application Programming Interfaces ("**APIs**") and where relevant, as a bulk download[770].

711 The Open Data Directive applies in principle to all accessible public-sector information such as geographical, land registry, statistical or legal information held by public-sector bodies and some public undertakings and to accessible publicly funded research data[771].

712 The Open Data Directive covers all types of documents containing such information, including written texts, databases, audio files and film fragments[772].

713 However, a few situations are exempted from its scope (Art. 1 para. 2 Open Data Directive). Amongst others, the Open Data Directive does not apply to:

a. documents for which third parties hold intellectual property rights;
b. documents whose access is excluded or restricted on the virtue of a national access regime or on the grounds of sensitive critical infrastructure protection;
c. documents whose supply falls outside the scope of the public task of a public-sector body or outside the scope of provision of services in the general interest of a public undertaking;

[769] According to Art. 2 para. 8 PSI Directive, dynamic data means "documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data".

[770] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.2 p. 43.

[771] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.4 p. 44.

[772] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.4 p. 44.

d. documents related to the activities of a public undertaking directly exposed to competition and therefore not subject to procurement rules under Art. 34 of Directive 2014/25/EU[773].

714 The Open Data Directive modernises the existing public sector information framework in many ways, including most notably by expanding the stakeholders and the data covered, by introducing a specific focus on high-value datasets, and by including dynamic data and APIs within its scope[774].

715 One could argue that if private businesses profit from data provided by the government, the general public should in return obtain some benefits from the data that businesses generate through the use of government data, or that at least government agencies obtain access to such data at marginal costs. In order to prevent public sector information being locked in by private companies that work for the government, the European Union will establish safeguards that will reinforce transparency and limit the conclusion of agreements which could lead to exclusive reuse of public sector data by private partners[775].

3.4.1.2 Dynamic data

716 The concept of dynamic data was newly introduced by this Directive and is defined as "documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data" (Art. 2 para. 8 Open Data Directive)[776].

717 In the transport sector, dynamic data can relate to real-time information on disruption and delays, dynamic fares and seat availability etc. as opposed to static data which refers to schedules and basic fares for transport modes, for instance.

718 This shows that, for public sector information too, there is a shift towards "data as a service", rather than merely as static downloads[777].

3.4.1.3 High-value datasets

719 Moreover, the Open Data Directive also introduces the concept of "high-value datasets", defined as documents the re-use of which is associated with important benefits for the society and economy. These are subject to a separate set of rules, ensuring their availability free of charge and in machine readable

[773] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.4 p. 44.
[774] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.4 p. 44.
[775] THOUVENIN/TAMÒ-LARRIEUX, Data Ownership and Data Access Rights – Meaningful Tools for Promoting the European Digital Single Market?, Big Data and Global Trade Law, Cambridge University Press, July 2021, p. 316 et seq., p. 334 and quoted references.
[776] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.2 p. 43.
[777] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.2 p. 43.

formats, provided via APIs and, where relevant, as bulk download. The sharing of such datasets is highly stimulated by the Open Data Directive[778].

720 Annex I of the Open Data Directive defines the following categories of high-value datasets:

(a) geospatial datasets;
(b) datasets consisting of information regarding earth observation and environment;
(c) meteorological datasets;
(d) statistical datasets;
(e) datasets consisting of information regarding companies and company ownership and
(f) datasets consisting of information regarding mobility[779].

721 As a consequence, the Open Data Directive aims at boosting the socio-economic potential of public-sector information and makes this information more easily available for companies by increasing the supply of dynamic data and of datasets with a particularly high economic impact, while at the same time promoting competition and transparency in the information market[780].

722 An implementing act on high-value datasets is expected to be published any time soon.

3.4.1.4 Open data versus other interests

723 It should be noted that an inherent tension exists between the Open Data Directive's aim to make public data more accessible and to encourage the re-use of this information, and the aim of the NIS Directive (see § 5.2.2 et seq. below) to ensure security and continuity of essential services. A certain amount of data gathered and generated through the provision of essential services will necessarily be of a sensitive nature. Making this sensitive data accessible to the public can inherently entail risks for the security and continuity of the service. This clearly shows that, while open data policies are for the most part beneficial to society, these policies should not be pursued thoughtlessly[781].

3.4.2 Free Flow Regulation

724 The Regulation 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data ("**Free Flow Regulation**") became applicable on 28 May 2019.

[778] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.2 p. 43.
[779] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.4 p. 44.
[780] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.1.2 p. 43.
[781] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.8.6 p. 195.

3.4.2.1 Purpose

725 The Free Flow Regulation aims to remove some barriers to the free flow of non-personal data in the internal market and to ensure that every organisation can store or otherwise process data anywhere in the European Union, while ensuring that national supervisors retain appropriate regulatory controls[782].

3.4.2.2 Data localisation requirements

726 In the past, the free flow of (personal and non-personal) data has been hindered by the presence of so-called "data localisation requirements"[783].

727 A "data localisation requirement" is any obligation or prohibition provided for in the law of a Member State which imposes the processing of data in its own territory or hinders the processing of data in any other Member State (see Art. 3 para. 5 Free Flow Regulation). Much of the Free Flow Regulation focuses on eliminating data localisation requirements wherever possible, in order amongst others to increase competition.

728 Data localisation requirements are often prompted by the perception that data are more secure when stored within a country's border. Data security however depends on the security measures that are implemented, rather than on the location where the data is stored[784].

729 Recently, due to various factors and political events, the emergence of questions around the concept of (national) data sovereignty might create a trend towards imposing data localisation requirements again and/or at least within the European borders and democracies.

3.4.2.3 Data porting and self-regulatory codes of conduct

730 Art. 6 Free Flow Regulation introduces the concept of "data porting" and provides that the European Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ("codes of conduct"), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards.

731 The "data sharing" aspect allows notably professional users[785] of such services to request their data back, or to move it to competing service providers. While the sharing of data is limited to these parties – providers of data processing services and their professional users – porting is thus turned into an instrument that facilitates data flows and avoids lock-in effects[786].

---

[782] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.1.4.1 p. 25.

[783] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.1.4.1 p. 25.

[784] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.6.5 p. 133 and quoted reference.

[785] Defined as "any natural or legal person including a public authority or a body governed by public law, using or requesting a data processing service for purposes related to its trade, business, craft, profession or task" (Art. 3 para. 8 Free Flow Regulation).

[786] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.1.4.3 p. 26.

732 Furthermore, these "codes of conduct" must also ensure that professional users have access to information on the conditions for switching and facilitate the ability for professional users to compare different service offers. Therefore, such "codes of conduct" could aid the development of AI products and services for automated vehicles through facilitating the movement of non-personal data retained by stakeholders[787].

3.4.2.4 Issues related to the delimitation of personal data

733 The scope of the Free Flow Regulation is limited to electronic data other than personal data as defined by Art. 4 para. 1 GDPR. In the case of a mixed dataset composed of both personal and non-personal data, the Free Flow Regulation applies to the non-personal data part of the dataset. Where personal and non-personal data in a dataset are inextricably linked, the Free Flow Regulation shall not prejudice the application of the GDPR (Art. 2 para. 2 Free Flow Regulation). Mixed datasets occurring often within the context of automated (and connected) vehicles, an uncertainty results from the interplay between these two regulations.

734 As we will see below (see § 4.2.4), the definition of personal data extends very broadly. Therefore situations of data (re-)combination and re-identification (that would render de-personalised data personal again) may happen. This gives also rise to some uncertainty as to what data actually falls within the scope of the Free Flow Regulation in the field of automated vehicles.

3.4.3 Other regulations

735 Various regulations, often related to intellectual property rights and/or trade secrets, might apply and/or influence the deployment of automated vehicles and the free flow of data that is suggested by the AVENUE vision, amongst others:

- The Database Directive[788];
- The InfoSoc Directive[789];
- The Directive on copyright in the digital single market[790];
- The Computer Programs Directive[791];
- Etc.

[787] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 74.

[788] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[789] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

[790] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market.

[791] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.

736 For an extensive review these acts, it can be referred to the 2018 report published in another Horizon 2020 project called "LeMO" ("Leveraging big data for managing transport operations")[792].

3.4.4 Payment Service Directive

737 The Directive 2015/2366 of 25 November 2015 on payment services in the internal market ("**PSD2**"), might serve as an example/inspiration of legal framework for automated vehicles as regards data management.

738 The PSD2 is the successor to PSD1, introduces enhanced security measures to be implemented by all payment service providers. Furthermore, it introduces new categories of service providers[793] who are able under certain conditions to obtain access to certain account information from payment service providers (i.e. a form of data sharing which is mandatory once the customer has authorised it)[794].

739 The PSD2 establishes rules to provide more flexibility and freedom to customers regarding their payment data. They are able to make their data available to third party service providers – who must also meet supervisory and security requirements – while maintaining the confidentiality of these data[795].

740 Customers decide for themselves whether they want to give these third parties access to their payment accounts and they can refuse any request for permission from a third party if they wish to do so. This means that, in terms of data sharing, customers retain complete control. Data may only be shared on their request. Inversely, payment institutions or other targeted institutions may not refuse to share data with these third parties once the transfer has been authorised by the customers. PSD2 also reinforces the obligation to keep customers' financial data confidential. The PSD2 concentrates heavily on strong customer authentication. Banks must implement appropriate security measures to ensure the confidentiality of their data. Here again, the position of the customer is key[796].

741 Due to PSD2, bank customers – including both individual customers and businesses – can exercise control over the transmission of their financial transaction data and may conduct their finances through third-party providers[797]. The Directive sets out rules on the transmission and use of financial (transaction) data[798].

---

[792] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, Chapter 3.7 p. 135 et seq.

[793] Account servicing payment service providers, payment initiation service providers, and account information service providers.

[794] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.1 p. 46.

[795] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.2 p. 46.

[796] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.2 p. 46.

[797] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.4 p. 46.

[798] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.3 p. 46.

742 The Directive aims to increased competition in the financial sector and more protection of customers' accounts. To achieve this goal, PSD2 establishes rules that will ensure transparency towards customers. Banks are forced to share their customers' financial transaction data on their request. The banks' monopoly on their customers' data is therefore eliminated, or at least significantly reduced. Third party providers may initiate payments for the customers directly from their bank account, as banks are forced to open access to their customers' accounts to third-party providers via application programme interfaces (APIs). In addition, banks must implement appropriate security measures to keep customers' data confidential. This means that banks must convince their customers to use two-stage identity verification[799].

743 The European Bank Agency drafted technical standards covering various technical issues, particularly the issue of strong customer authentication ("SCA"). SCA is an authentication based on the use of two or more elements categorised as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data[800].

3.5 Sector specific strategy and legislation

3.5.1 Sustainable and Smart Mobility Strategy

744 The European Commission's Sustainable and Smart Mobility Strategy was published on 9 December 2020, e.g. after the European Data Strategy that was published earlier in February 2020.

745 As regards smart mobility, the Sustainable and Smart Mobility Strategy sets two milestones to be reached by 2030:

- Automated mobility will be deployed on large scale and
- Seamless multimodal passenger transport will be facilitated by integrated electronic ticketing and freight transport will be paperless.

746 According to the Sustainable and Smart Mobility Strategy, data is at the heart of the digital transformation. Exchanging data is a prerequisite for a seamless passenger experience across modes, allowing integrated planning, ticketing, and purchase. Furthermore, exchanging data enables operators to optimise their operational and maintenance processes. In addition, data governance should be based on a systemic approach in which all sectors benefit from the data exchange, especially when implementing smart cities[801].

747 The European Commission considers that start-ups and technology developers need an agile regulatory framework to pilot and deploy their products. It therefore intends to work towards facilitating testing and

[799] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.3 p. 47.
[800] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.3.3 p. 47.
[801] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 668 p. 160.

trials, and towards making the regulatory environment fit for innovation, so as to support the deployment of solutions on the market[802].

748 The digital transformation of the transport and mobility sector requires further efforts related to data availability, access and exchange. Currently, they are often hampered due to unclear regulatory conditions, a lack of an European market for data provision, the absence of an obligation to collect and share data, incompatible tools and systems for data collection and sharing, different standards, or data sovereignty concerns. The availability of data and statistics is also essential, in particular real time data, as it enables better services to citizens or transparency of supply chains in freight transport[803].

749 According to the Smart and sustainable mobility strategy, the European Commission will take into consideration the horizontal governance set out in the data strategy and the Data Act (see Appendix A § 3.2.4 above) and the principle of technology neutrality. The aim is to collect, connect and make data available to meet European objectives, from sustainability to multimodality[804].

750 As mentioned previously, the European Commission intends to create a Mobility Data Space that should function in synergy with other key systems, including energy, satellite navigation and telecommunications, while being cyber safe and compatible with Union data protection standards. At the same time, a level playing field for data in the value chain shall be preserved so that innovation can thrive and new business models emerge. The European Commission will consider different regulatory options to give operators a safe and trustworthy space to share their data within and across sectors, without distorting competition and while respecting privacy and the Union's international obligations[805].

[802] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 64 p. 13.

[803] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 70 p. 14.

[804] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 71 p. 14.

[805] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020, N 71 p. 14.

SMART MOBILITY

Flagship 6 - **Making connected and automated multimodal mobility a reality**

36.	Revise Delegated Regulation 2015/962 on real time traffic information services to extend geographical coverage and datasets; revise Delegated Regulation 2017/1926 on multimodal travel information services to include mandatory accessibility of new dynamic datasets	**2021; 2022**
37.	Assess the need for regulatory action on rights and duties of multimodal digital service providers and issue a recommendation to ensure public service contracts do not hamper data sharing and support the development of multimodal ticketing services, together with an initiative on ticketing, including rail ticketing	**2022**
38.	Revision of the Directive on Intelligent Transport Systems, including a multimodal ticketing initiative	**2021**
39.	Complete the EU legal framework on the approval of automated vehicles	**2021**
40.	Assess the need for an agency or other body to support safe, smart and sustainable road transport operations [13]	**2022**
41.	Adopt the implementing legislation for the approval of connected and automated vehicles	**2021**
42.	Adopt railway technical standards and specifications package on ERTMS/Control-Command and Signalling (CCS); and develop mandatory deployment plans for automatic train operation, automated traffic management and advanced CCS	**2022**
43.	Revision of the Directive on Harmonised River Information Services	**2022**
44.	Propose measures on electronic documents for inland crew and vessels	**2021**

Figure 2 – Extract of the Action plan (Annex) of the Sustainable and Smart Mobility Strategy dedicated to Smart Mobility for connected and automated mobility

Flagship 7 - **Innovation, data and AI for smart mobility**

45.	Develop/renew R&I partnerships: Connected, cooperative and automated mobility; Shift2Rail; SESAR; Waterborne; Clean Aviation; Clean Hydrogen Partnership; Smart Networks and Services; AI, Data and Robotics; and Key Digital Technologies	**2020-2021**
46.	Further develop the regulatory framework for drones and unmanned aircraft, including U-Space; adopt a Drone Strategy 2.0	**2021-2023; 2022**
47.	Assess the need for regulatory actions to ensure safety and security of new entrants and new technologies, such as hyperloop	**2021**
48.	Set up a high-level group ('New Mobility Tech Group') as a first step toward the development of a coherent EU approach and a set of recommendations on facilitating testing and trials of emerging mobility technologies and solutions in the EU ('European Mobility Test Beds')	**2022**
49.	Develop a common European mobility data space and establish a stronger coordination mechanism for the national access points established under the ITS Directive	**2021**
50.	Set out an AI roadmap for mobility	**2021**
51.	Review the regulatory framework for interoperable data sharing in rail transport (ERTMS, rail telematics applications)	**2022**
52.	Review the current EU type approval legislation to facilitate car data-based services including interaction with energy system	**2021**
53.	Propose a new regulatory framework to open up access to car data to mobility services	**2021**
54.	Propose rules on a trusted environment for corridor data exchange to support collaborative logistics	**2022**

Figure 3 – Extract of the Action plan (Annex) of the Sustainable and Smart Mobility Strategy dedicated to Smart Mobility for Innovation, data and AI for smart mobility

3.5.2 Intelligent Transport Systems Directive

751 Further data related aspects of the ITS Directive (that has already been briefly presented in § 1.2.5.1 and § 2.2.7 above) will be presented here.

752 The issue of personal data protection and security is addressed with a reference to the privacy framework: Art. 10 ITS Directive states that processing of personal data must be carried out in accordance with both the GDPR and the ePrivacy Directive. Member States are also required to protect personal data against misuse, including unlawful access, alteration or loss. When using intelligent transport system applications, purpose limitation and data minimization principles should be applied and anonymisation should also be promoted as one of the principles to enhance the privacy of individuals[806].

3.5.2.1 Revision

753 As mentioned previously, the ITS Directive is under revision and a proposal[807] as well as an impact assessment[808] have been published end of 2021. The feedback period has been closed on 20 March 2022 and the European Commission's adoption is pending.

754 According to the European Commission, the revision's aims mainly at:

- assessing the availability of infrastructure and traffic/travel data across the whole European transport network; and
- cover new technological developments:
  - i) connected and automated mobility (e.g. self-driving vehicles) and
  - ii) online platforms allowing users to access several modes of transport[809].

3.5.2.2 Delegated Regulation on road safety-related minimum universal traffic data

3.5.2.2.1 Overview

755 The ITS Directive and its Delegated Regulation 886/2013 of 15 May 2013 on road safety-related minimum universal traffic data mandate the creation of National Access Points ("**NAP**") as a single point of access

[806] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 9 and quoted references.

[807] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/40/EU of the European Parliament and of 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, COM(2021) 813 final, 14 December 2021.

[808] Commission Staff Working Document, Impact Assessment Report, SWD(2021) 474 final, 14 December 2021.

[809] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12534-Intelligent-transport-systems-review-of-EU-rules-_en (last consultation 31 August 2022).

for users to the ITS data to facilitate access, easy exchange and reuse of transport data (multimodal, road safety-related, safe and secure parking, real-time traffic and travel data)[810].

756 In particular, the Delegated Regulation 886/2013 specifies conditions for the deployment, data use and procedures related to an European-wide free, where possible, road safety-related universal traffic information services[811].

757 Road operators, services providers and specialised broadcasters must provide to road users real-time information, advice and location relating to a set of identified road safety events (e.g. slippery road, obstacles, unprotected accident).

758 To this end, road operators and service providers must develop special means to detect relevant events, identify conditions and collect safety-related traffic data (Art. 6 Delegated Regulation 886/2013). They must also share and update their data in a fully compatible and interoperable machine-readable format (Art. 7 para. 1 Delegated Regulation 886/2013). Member States must create a national digital access point gathering data from road operators and service providers to enable re-use of their data within an adequate timeframe[812].

3.5.2.2.2 Assessment of the European Commission

759 Since the adoption of the delegated regulations, National Access Points have been established in Member States as well as in other countries such as Norway, the United Kingdom and Switzerland[813].

760 The early stages of implementation made it apparent that Member States are faced with common challenges and are looking for common solutions through working further together. Yet, currently there is no place where NAPs operators and National Bodies/competent authorities can work together on common issues related to the development, operation and evolution of NAPs or on new challenges such as e.g. data collection activities and negotiations with private data providers and/or global players[814]. A project called NAPCORE will be launched in 2022 until 2024 with the objective of coordinating the NAPs and National Bodies in a long-lasting and future-oriented platform organisation[815].

761 Although NAPs allow data to be shared, the usage of the data provided by them is still relatively low, partly due to the fact that they have been created only recently. The services related to the exchange of static road attribute data used for updating digital maps are an exception, progressing well but in need to expand to local levels. For the multimodal information services a lot of static data (such as schedules and

[810] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 676 p. 161.

[811] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 66.

[812] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 66.

[813] https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/action-plan-and-directive/national-access-points_en (last consultation 31 August 2022).

[814] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 677 p. 161.

[815] https://www.uitp.org/projects/napcore/ (last consultation 31 August 2022).

basic fares for all transport modes) has also become more accessible. Still, the accessibility of dynamic data (e.g. real-time information on disruption and delays, dynamic fares and seat availability) has been left to discretion of Member States making it difficult for service providers to have access to them[816].

762 Despite the legislation in place, reluctance to share data continues to be a limiting factor. This is due to issues of lack of trust, high expected costs and unclear benefits for those providing the data. Also, the quality of safety-related data is not yet optimal. Last but not least, the data layers (e.g. road and multimodal data, traffic and travel data) are not yet structured and coordinated well enough and tools allowing effective accessibility, exchanging and data collection are missing[817].

3.5.2.3 Traffic Information Services

3.5.2.3.1 Delegated Regulation 2015/962

763 The Delegated Regulation 2015/962 of 18 December 2014 on traffic information services[818], also called Real-Time Traffic Information Services Regulation ("**RTTI**"), specifies conditions for development and provision of EU-wide compatible, interoperable and continuous real-time traffic information.

764 The RTTI makes it compulsory to render accessible a specific list of existing road and traffic data for the provision of EU-wide real-time traffic information services (this includes data on regulations and restrictions such as traffic circulation plans and data on the state of the network such as road closures or works)[819].

765 Art. 2 RTTI distinguishes between three types of data:

- static road data (i.e. data that do not often change, such as the location of services area);
- dynamic road data (i.e. data describing the status of the road and often changing such as availability of parking places) and
- traffic data (i.e. data on road traffic characteristics such as traffic volume).

766 The RTTI requires that Member States create a digital interface gathering road data and traffic data (including metadata) retained by road authorities and road operators to enable search and re-use of these data. Road authorities and road operators must provide these data through the national interface on a non-discriminatory basis and in an adequate timeframe. Formats for each type of data are also specified. Data may, therefore, be used to develop or operate AV products or services such as real-time itineraries

[816] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 678 p. 161.

[817] European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020, N 679 p. 161.

[818] Commission Delegated Regulation 2015/962 of 18 December 2014 supplementing Directive 2010/40 of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services, OJ L 157 of 23.06.2015.

[819] HUET/AMSLER/MARSANDE (UITP Europe), The EU's data strategy and its impact on public transport, Version 6, 17 March 2022, p. 16.

optimisers. Finally, this delegated regulation provides specific rules on the update parameters of each kind of data to enable real-time traffic information services based on up to date data[820].

3.5.2.3.2 Delegated Regulation 2022/670

767 The European Commission has published the Delegated Regulation 2022/670 on 2 February 2022[821], which will repeal the RTTI (Delegated Regulation 2015/962) as of 1 January 2025.

768 The new provisions of the Delegated Regulation 2022/670 aim to:

- Extend the geographical scope to entire road network (beyond TEN-T, motorways);
- New data types: location of service areas and rest areas; location of refuelling points and stations for all other fuel types; weight/length/width/height restrictions; one-way streets; boundaries of restrictions, prohibitions or obligations with zonal validity, current access status and conditions for circulation in regulated traffic zones;
- Extend the requirements regarding standards and supporting collaboration for creation of new standards;
- Obligations on service providers to re-use data types related to traffic regulations, circulation plans and temporary traffic management measures;
- Right for public authorities to request data types related to traffic management and road maintenance under FRAND[822] conditions from service providers and holders of in-vehicle generated data[823].

3.5.2.4 Multimodal Travel Information Services

3.5.2.4.1 Overview

769 The Delegated Regulation 2017/1926 of 31 May 2017 on multimodal travel information services[824] ("**MMTIS**") ensures the provision of accurate multimodal travel information services available at European level.

770 The Delegated Regulation 2017/1926 distinguishes between three types of data:

[820] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 66.

[821] Commission Delegated Regulation (EU) 2022/670 of 2 February 2022 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services.

[822] Fair, Reasonable And Non-Discriminatory.

[823] Presentation of the European Commission, Update from DG MOVE, Intelligent Transport Systems Directive 2010/40/EU Delegated Regulation 2015/962 on the provision of real-time traffic information services, 21 September 2021, https://uvarbox.eu/wp-content/uploads/2021/09/UVARBox_WS3_Presentation-on-revision-of-ITS-Directive-and-DR2015-962.pdf (last consultation 31 August 2022).

[824] Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services.

- historic traffic data[825];
- static travel data and traffic data[826] and
- dynamic travel and traffic data[827].

771 Member States must create a digital interface gathering historic traffic data and static travel and traffic data (including relevant metadata) of the transport authorities, transport operators, infrastructure managers and transport on-demand service managers (potentially including mobility as a service providers operating AV-based services) to enable search and re-use of these data[828].

772 Data must be accessible in the format defined in the Delegated Regulation. Member States can also decide to provide dynamic data. Data must be accessible on a non-discriminatory basis. Travel information services shall provide routing results to other travel information services upon request (linking services). Linking must be subject to contractual agreements, and costs must be reasonable and proportionate. Finally, reuse of data must be neutral, non-discriminatory and not biased. Criteria used for ranking must be transparent, not based on factors related to user identity and applied without discrimination to all users[829].

3.5.2.4.2 Revision

773 In accordance with the European Union's data strategy, the Delegated Regulation 2017/1926 is currently under revision and its new provisions are scheduled to be published in the fourth quarter of 2022.

774 According to the European Commission, the MMTIS revision should focus on further enhancing the development of information services and will focus on technical aspects:

- Accessibility of dynamic data (as listed in the Annex of the MMTIS);
- Updating the list of data to be made accessible (including new data types) pursuant to the MMTIS;
- Requiring the use of certain standards for payment and booking interfaces;
- Ensure alignment with data categories of the Delegated Regulations on Real-Time Traffic Information Services[830].

[825] Art. 2 para. 14 defines "historic traffic data" as traffic characteristics depending on the hour, day, season based on previous measurements, including rate of congestion, average speeds, average travel times, as listed in the Annex of the Delegated Regulation (EU) 2017/1926.

[826] Art. 2 para. 8 defines "static travel and traffic data" as data relating to different transport modes that does not change at all or does not change often, or change on a regular basis, as listed in the Annex.

[827] Art. 2 para. 7 defines "dynamic travel and traffic data" as data relating to different transport modes that changes often or on a regular basis, as listed in the Annex.

[828] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 66.

[829] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 67.

[830] Overview of the Commission's initiative on Multimodal Passenger Mobility, DG Move – Unit B4, 8 April 2022, https://fsr.eui.eu/wp-content/uploads/2022/03/20220502-2-Florence-forum-on-ticketing-B4.pdf (last consultation 31 August 2022).

3.6 Revised General Safety Regulation

3.6.1 Event data recorder

775 The event data recorder ("EDR") is a new safety/security feature in-vehicle according to Regulation 2019/2144 dated 27 November 2019 ("revised General Safety Regulation" or "GSR"), which applies since 6 July 2022.

776 Art. 3 para. 13 GSR defines the event data recorder as a system with the only purpose of recording and storing critical crash-related parameters and information shortly before, during and immediately after a collision. All motor vehicles will be equipped with an event data recorder when specific requirements will be met according to Art. 6 para 4 and 5 GSR[831].

777 Detailed rules concerning the specific test procedures and technical requirements for event data recorder and other advanced vehicle systems will be regulated by the European Commission delegated acts[832].

778 According to the guidelines on the exemption procedure for European approval of automated vehicles of 12 February 2019, the vehicle manufacturer is obliged to provide the following information:

- Type of stored data;
- Storage location;
- Storage duration;
- Means to ensure security and data protection; and
- Access to the data[833].

779 Recital 14 GSR clarifies that any processing of personal data, such as information about the driver processed in event data recorders or information about the driver's drowsiness and attention or the driver's distraction, should be carried out in accordance with Union data protection law[834].

780 Art. 6 GSR puts in place several safeguards with relevance in the context of personal data protection, starting by mandating that they shall operate in closed-loop systems. Art. 6 para. 4 GSR provides that event data recorders shall operate in a way that should not allow the vehicle or owner to be identified. They shall be able to make the data recorded available to national authorities through a standardised interface for the purpose of accident research and analysis, in compliance with the GDPR[835].

---

[831] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 8.

[832] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 8 and quoted references.

[833] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 8 and quoted references.

[834] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 50.

[835] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 50.

4 Overview of the legal framework as regards personal privacy and data protection

781 In January 2014, during a panel discussion on consumer privacy at the Consumer Electronics Show ("CES"), an important electronics convention in Las Vegas, an executive of Ford's Marketing and Sales department claimed that "*We [Ford] know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone* ". Unsurprisingly, this statement was officially qualified as a mistake and retracted on the following day[836].

782 This already eight years old declaration shows how vehicle manufacturers have access to many personal information, including sensitive information such as information about road traffic infringements. It also highlights how data processing in the field of road mobility is a sensitive topic, as many conclusions can be drawn from location data as regards religion or sexual orientation for instance (amongst others, see § 4.2.4.5.1 below).

783 Privacy in the context of automated vehicles can be defined as each individual's authority to determine a private sphere for personal conduct and self-development, including privacy of communications and the ability to control the terms and conditions of personal information sharing. Privacy is not only an ethical imperative but an enforceable fundamental right in the European Union (as we will see below). Standardly, respect for privacy requires a valid legal basis for any collection, processing, use or exchange of personal data[837] (as defined by Art. 6 GDPR, see § 4.2.8 below).

784 The vehicle type-approval regulations seen above does not specifically tackle the issue of personal data protection (as it is mainly focused on road safety), and cybersecurity is only addressed in a marginal way at this stage[838].

[836] https://www.businessinsider.com/ford-jim-farley-retracts-statements-tracking-drivers-gps-2014-1?IR=T (last consultation 31 August 2022).

[837] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.1 p. 35.

[838] According to Recital 62 AMSVR (Regulation 2018/858 of l30 May 2018), it is considered important that manufacturers take all necessary measures to ensure compliance with the rules on processing and transfer of personal data arising from the use of a vehicle.

4.1 International framework

785 The right to personal privacy is protected by various (international) legal conventions[839], amongst others by the following provisions.

786 Art. 12 of the 1948 Universal Declaration of Human Rights provides that "*No one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*".

787 Art. 8 para. 1 of the 1950 European Convention on Human Rights foresees that "*Everyone has the right to respect for his private and family life, his home and his correspondence*".

788 Similarly, Art. 8 of the 2000 Charter of Fundamental Rights of the European Union provides that "*Everyone has the right to the protection of personal data concerning him or her*" (para. 1) and that "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*" (para. 2).

789 More recently, one of the topics of the joint agenda of the 2016 Declaration of Amsterdam was to ensure privacy and data protection, by "*respecting existing legislation on privacy and data protection*" and clarifying "*the conditions for the (re-) use and sharing of data generated by connected and automated vehicles*"[840].

790 Regarding regional law, Art. 16 para. 1 TFEU states that "*Everyone has the right to the protection of personal data concerning them*". Paragraph 2 of the same provision provides that the European Parliament and the Council shall lay down rules relating to the protection of individuals with regard to the processing of personal data, which was done with the (now repealed) Directive 95/46/EC and, more recently, with the GDPR.

791 The influence of the European framework on the international scene is also reflected in its relationship to the Convention 108 of the Council of Europe. The latter, first amended in 2001 to align with the EU Directive 95/46/CE, was again modernised in 2018 and includes some of the latest innovations of the GDPR. The Convention 108 is the only binding international data protection instrument since it is open to ratification by states outside the Council of Europe[841].

---

[839] For further details, see AVENUE 2020 Deliverables D6.5 First Iteration Cybersecurity and privacy control action plan and recommended technologies, § 4.3 p. 32; D6.6 Second Iteration Cybersecurity and privacy control action plan and recommended technologies, § 6 p. 41.

[840] Declaration of Amsterdam, Cooperation in the field of connected and automated driving, Navigating to connected and automated vehicles on European roads, 14-15 April 2016, Joint Agenda, litt. c p. 6.

[841] SALIOU (LINC — Laboratoire d'innovation numérique de la CNIL), The European model: point of convergence, source of divergence?, 27 October 2021, https://linc.cnil.fr/fr/european-model-point-convergence-source-divergence (last consultation 31 August 2022).

792 In addition to these international legal instruments, dedicated national laws have also historically foreseen the protection of personal privacy within the European Member States, in particular related to the processing of personal data. For instance, in France the legal framework is defined by the "*Loi du 6 janvier 1978 Informatique et Libertés*" and in Germany by the "*Bundesdatenschutzgesetz*", which first entered into force on 1 January 1978 and has been updated since.

793 Today, with the adoption of the General Data Protection Regulation (GDPR) which applies since 25 May 2018, the scope of these national frameworks has become more limited[842].

794 In the context of car connectivity, the general personal data protection and privacy rules are laid down in two Europeans legislations: the GDPR and the ePrivacy Directive. In addition to them, there are (European) sectoral regulations with certain relevance in the field of privacy, to the extent that they impose certain obligations in this regard and regulate access to data collected from connected vehicles[843].

795 Besides, the Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities was published on 27 April 2016. As it merely focuses on criminal law aspects of data processing by state authorities, this directive will not be detailed in this deliverable.

4.2 General Data Protection Regulation (GDPR)

4.2.1 Introduction

796 By way of a reminder, the relevant provisions of the GDPR from a technical point of view as regards cybersecurity and privacy have already been presented in Deliverables D6.5 and D6.6[844] (First and second cybersecurity and privacy control action plans). Deliverable D6.6 has also briefly presented the legislation efforts concerning privacy in Asia, Australia and America[845].

797 This section presents key provisions, concepts and principles that might somehow conflict with the deployment of automated vehicles and the services they provide and that should be further studied and adressed.

[842] For instance by implementing so-called "opening clauses" of the GDPR. These provisions permit a Member State to modify the provisions of the article in which the clause resides. In effect, opening clauses permit the Member State to introduce a more restrictive application of the GDPR obligation via local legislation.

[843] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 28.

[844] AVENUE 2020 Deliverables D6.5 First Iteration Cybersecurity and privacy control action plan and recommended technologies, § 4.3 p. 32 et seq.; D6.6 Second Iteration Cybersecurity and privacy control action plan and recommended technologies § 6 p. 41 et seq.

[845] AVENUE 2020 Deliverable D6.6 Second Iteration Cybersecurity and privacy control action plan and recommended technologies § 6.4.2 p. 43 et seq.

4.2.2 Opening remarks

798 The GDPR replaced the Directive on the protection of personal data 95/46/EC adopted in 1995. It is directly applicable in all European Member States pursuant to Art. 288 para. 2 TFUE. It thus takes precedence over all national provisions, unless opening clauses allow for deviations or more specific national laws[846].

799 The GDPR's objective is essentially two-fold. On the one hand, it seeks to facilitate the free flow of personal data between the European Member States. On the other hand, it establishes a framework of fundamental rights protection, based on the right to data protection in Art. 8 Charter of Fundamental Rights[847].

800 The applicability of the GDPR ensures far-reaching protection of personal data and places data processing under a ban of principle, subject to the possibility of a permission[848]: without a proper legal basis, the processing of personal data is prohibited (Art. 6 para. 1 litt. a to f GDPR, see Appendix A § 4.2.8 below).

801 It is generally recognised that since its entry into force, the GDPR is accompanied by a strong signalling power that goes far beyond its actual material and territorial scope of application[849]. The GDPR has set the global standard for personal data protection and processing. It has also largely influenced the legislation of non-European States[850]. Besides, the GDPR has a strong shaping influence on data sharing practices in the European Union, simply due to the breadth of the personal data concept and because of the prevalence of mixed datasets containing both personal and non-personal data[851].

802 As we will see below, as a relatively recent and horizontal (general/cross-sectoral) regulation, important discussions are currently taking place around concepts set by the GDPR that are prone to interpretation, which leads to implementation questions in practice, especially in the absence of further guidance from courts or data protection authorities.

4.2.3 Material and territorial scope of the GDPR (Art. 2 and 3 GDPR)

803 The GDPR applies to companies, public bodies and associations, regardless of their size or activity, as long as they process personal data of natural persons located in the European Union (see Art. 2 and 3 GDPR). The criterion for applicability is therefore not the place of establishment of the entity processing personal data.

---

[846] Be Open, European forum and oBsErvatory for OPEN science in transport, D 4.1 Open Science in transport research: legal issues and fundamental principles, 31 August 2020, § 3.2 p. 30.

[847] European Parliamentary Research Service (EPRS), Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?, Scientific Foresight Unit (STOA) PE 634.445, July 2019, p. I.

[848] "*Verbot mit Erlaubnisvorbehalt*" in German.

[849] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 2 p. 3 and the quoted references.

[850] GYSIN (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation – UVEK), Datenschutz Mobilitätsdaten, Bericht, ASTRA-D-DB3D3401/359, 30 November 2020, p. 7.

[851] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.1.1.1 p. 14.

804 According to Art. 4 para. 2 GDPR, "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

805 In application of the "marketplace principle" (Art. 3 para. 2 GDPR), the GDPR also applies to (foreign) companies, based outside the European Union, that process personal data of European citizens located in the European Union: the GDPR has an extra-territorial scope.

806 This broad international application is aimed at reaching high privacy standards for individuals in the European Union and binding people and entities involved in processing personal data within the European Union to these high standards[852].

807 As a horizontal piece of law, the GDPR sets generic principles and does not provide detailed rules on sector-specific questions, such for instance as how consent requirements relate to vehicle-generated data[853].

808 Amongst others, the GDPR applies to common tracing of internet activities through device identifiers such as IP-addresses and cookie-IDs, which must first be assigned to a specific natural person in order to establish the personal reference[854], as described in the next section.

4.2.4 Personal data (Art. 4 para. 1 GDPR)

809 Drawing a dividing line between personal data and non-personal data is paramount to determine the scope of application of the GDPR. In addition, the concept of personal data is also used in many other existing or upcoming legislations such as the Free Flow Regulation, the Data Governance Act, the Digital Markets Act, the Data Act etc. (seen above) which often refer to the GDPR.

810 Whereas personal data is subject to the GDPR, non-personal data is not. Determining whether a given data item qualifies as personal data is thus crucial and increasingly burdensome as more data are being generated and shared[855].

---

[852] Be Open, European forum and oBsErvatory for OPEN science in transport, D 4.1 Open Science in transport research: legal issues and fundamental principles, 31 August 2020, § 3.2.1 p. 38.

[853] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 123.

[854] Be Open, European forum and oBsErvatory for OPEN science in transport, D 4.1 Open Science in transport research: legal issues and fundamental principles, 31 August 2020, § 3.2.1 p. 38 and the quoted reference.

[855] FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11 et seq., p. 13.

4.2.4.1 Definition

811 The GDPR (and the European data protection framework) acknowledges two categories of data: personal and non-personal data. There is data that is always non-personal (because it never related to an identified or identifiable natural person) and there is also data that once was personal but no longer is (as linkage to a natural person has been removed)[856]. The latter category of data is sometimes called "depersonalised data".

812 Personal data is defined by Art. 4 para. 1 GDPR as "**any information relating to an identified or identifiable natural person ("data subject")**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (emphasis added).

813 The legal test to differentiate between personal and non-personal data is embodied in Recital 26 of the GDPR:

> "The principles of data protection should apply to any information concerning an identified or identifiable natural person. […]
>
> To determine whether a natural person is identifiable, account should be taken of **all the means reasonably likely to be used**, such as singling out, **either by the controller or by another person to identify the natural person directly or indirectly.** To ascertain whether means are reasonably likely to be used to identify the natural person, **account should be taken of all objective factors, such as the costs of and the amount of time required for identification**, taking into consideration the available technology at the time of the processing and technological developments.
>
> The principles of data protection should therefore **not apply to anonymous information**, namely information which **does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable**. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes." (emphasis added)

814 According to the Article 29 Data Protection Working Party (i.e. the predecessor of today's European Data Protection Board) a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able")[857].

---

[856] FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11 et seq., p. 11.

[857] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (WP 136) 01248/07/EN, Adopted on 20 June 2007, p. 12.

815 The following figure depicts a test to be applied to determine whether information constitutes personal data:

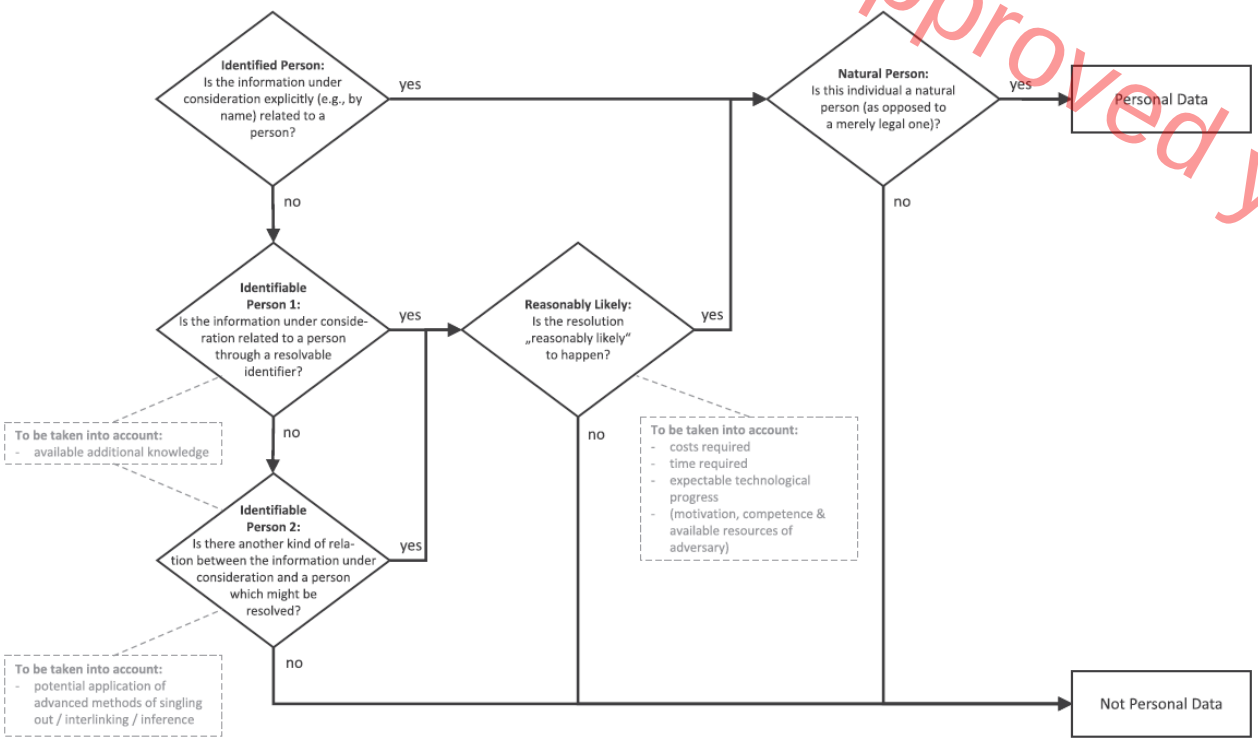

Figure 4: Assessment scheme for person-relatedness of data under the GDPR as proposed by Michèle FINK and Frank PALLAS[858]

4.2.4.2 A vast category of data

816 As we will see below in the context of connected and automated vehicles and minibuses, the GDPR's general and broad definition of personal data encompasses many types of data.

817 The Court of Justice of the European Union considered that the use of the expression "any information" in Art. 2a Directive 95/46 (now Art. 4 para. 1 GDPR) reflects "[…] the aim of the European legislature to assign a **wide scope** to that concept [of personal data], which is not restricted to information that is sensitive or private, but **potentially encompasses all kinds of information**, not only objective but also subjective […] **provided that it relates to the data subject**"[859] (emphasis added).

818 In a judgment published in 2016, i.e. before the entry into force of the GDPR[860], the Court of Justice of the European Union ruled that IP addresses are personal data in certain circumstances (see also N 856 below). The Court of Justice has also ruled that metadata (such as location data or IP addresses combined with log files on retrieved web pages) which only allows for the indirect identification of the data subject can nonetheless be personal data[861].

[858] FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11 et seq., p. 14.

[859] ECJ Case C-434/16, ECLI:EU:C:2017:994 dated 20 December 201, N 34 – Peter Nowak.

[860] ECJ Case 582/14, ECLI:EU:C:2016:779 dated 19 October 2016, N 44 – Patrick Breyer.

[861] ECJ Cases C-293/12 and C-594/12, EU:C:2014:238 dated 8 April 2014, N 26 – Digital Rights Ireland Ltd.

819 Based on this case law and on reasoning by analogy, it is commonly accepted that license plates of vehicles qualify as personal data.

820 Regarding the format or the medium on which that information is contained, the concept of personal data includes information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic, for example. It includes information kept on paper, as well as information stored in a computer memory by means of binary code or on a videotape, for instance[862].

821 The technical nature of vehicle data does not preclude its legal qualification as personal data, to the extent that it can be related to an identified or identifiable individual[863].

822 In relation with connected cars, the following (non-exhaustive) data catalogue has been qualified as relevant from a data protection point of view:

- Vehicle Identification Number (VIN);
- IP address, mac address, fingerprint devices;
- Location data (current position, whereabouts, routes) with time and timestamps;
- Registration data like name, address, date of birth, gender, payment information;
- Cookies;
- Maintenance dates, repair requirements;
- Data for assistance systems and automated driving;
- Traffic situation;
- Driving style, acceleration, braking, speed;
- Attention level, drowsiness detection, driving time, health status, eye tracking, eye movements;
- Biometric data in the sense of Art. 9 GDPR;
- Seat position, seat belt use;
- Passengers in the vehicle;
- Other road users such as cyclists, pedestrians, etc.;
- Media use such as telephone, SMS, e-mail, radio etc.;
- Road information such as traffic signs, condition of the road;
- Image data such as camera recordings;
- Accident data;
- Movement profile;
- Compliance with traffic regulations (speed, parking, overtaking, braking, driving direction and glance);
- Status of the vehicle (windows, doors, etc.);
- Temperatures, brightness, rain, visibility[864].

4.2.4.3 Divergent interpretations of Recital 26

823 The fact that Art. 4 GDPR's definition of personal data uses concepts prone to interpretation (namely "any information relating to an identifiable natural person") has opened the door for different interpretations that might have important impacts for automated vehicles.

[862] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (WP 136) 01248/07/EN, Adopted on 20 June 2007, p. 7.

[863] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 94.

[864] Table 1 in SCHUBERT/MARTIN/SCALLA, in: Stiftung Datenschutz, Datenschutz im vernetzten Fahrzeug, 1. Aufl. 2020, 173 (174 ff.).

824 A point of debate has been the interpretation of Recital 26 presented above, which often proves complex to implement in practice.

825 In a nutshell, according to the "relative" approach to identifiability, Recital 26 shall be interpreted with a focus on the means available to the controller of data (see Art. 4 para. 7 GDPR and N 887 below for this notion), while the "absolute" approach considers that means available to any third party, and not only to be controller of data, should be taken into account[865].

826 This has led to significant divergence amongst others between Article 29 Data Protection Working Party and national supervisory authorities. The GDPR admits that there can be a remaining risk of identification, even in relation to anonymous data, but others have insisted that no such risk is acceptable[866] (see also N 854 below).

4.2.4.4 Relevant time scale of Recital 26

827 Another important question is the relevant time scale: Recital 26 of the GDPR requires that the "means" to be taken into account are not just those that are presently available, but also "technological developments". It is, however, far from obvious what timescale ought to be considered in this respect[867].

828 The existing legal framework might provide help in this context, as some frameworks foresee the necessity to save personal data for a particular timeframe (for instance five or ten years, often corresponding to the statute of limitation) and then to delete it.

829 Therefore, this timeframe might serve as the timeframe to be taken into account, but it might result in an unpractical solution, as for long periods of time, such as five or ten years, the technological developments that will have occurred then are hardly predictable today.

830 The (technical) lifetime of the data itself might also constitute a key factor.

4.2.4.5 Personal data warranting special attention

831 In the context of its "Guidelines on connected vehicles and mobility related applications", the European Data Protection Board has identified three categories of data that may warrant special attention given their sensitivity and/or potential impact on the right and interests of data subjects[868]:

- location data;
- biometric data and
- data that could reveal offences or traffic violations.

[865] For a more detailed overview, see amongst others SPINDLER/SCHMECHEL, Personal Data and Encryption in the European General Data Protection Regulation, (2016) 7 JIPITEC 163, N 12 et seq. p. 165.

[866] See Finck/Pallas, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 1.

[867] Finck/Pallas, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11 et seq., p. 16 and seq.

[868] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 62 et seq. p. 15.

832 It should be noted that these categories of data partially overlap with the special categories of personal data as defined by Art. 9 GDPR.

833 According to Art. 9 para. 1 GDPR, "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited". Exemptions to this prohibition regime are defined under Art. 9 para. 2 et seq. GDPR.

4.2.4.5.1 Location data

834 Location data is particularly revealing of the life habits of data subjects. The journeys carried out may be very characteristic, as they enable one to infer the place of work and of residence, as well as the centres of interest (leisure). They may possibly reveal sensitive information such as religion through the place of worship or sexual orientation through the places visited[869].

835 Therefore, the European Data Protection Board advises the vehicle and equipment manufacturers, the service provider and other data controllers to be particularly vigilant not to collect location data, except if doing so is absolutely necessary for the purpose of processing. As an example, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data[870].

836 In general, for connected vehicles, the European Data Protection Board considers that collecting location data is subject to compliance with the following principles:

- Adequate configuration of the frequency of access to, and of the level of detail of location data collected relative to the purpose of processing. For instance, a weather application should not be able to access the vehicle's location every second, even with the consent of the data subject.
- Providing accurate information on the purpose of processing (e.g. is location history stored? If so, what is its purpose?).
- When the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use, for example on the on-board computer.
- Activating location only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started.
- Informing the user that location has been activated, in particular by using icons (e.g. an arrow that moves across the screen).
- The option to deactivate location at any time.
- Defining a limited storage period[871].

[869] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 63 p. 15.

[870] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 63 p. 15.

[871] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 64 p. 16.

837 For automated vehicles, precise location of the vehicle at every second (or at an even higher frequency) is important for safety reasons and it should be assessed on how to best comply with such contradictory interests (e.g. the safety requirements needing precise geolocalisation every second versus the privacy requirement requesting that geolocalisation should only be activated when needed and not continuously).

4.2.4.5.2 Biometric data

838 According to Recital 10 of the Regulation 2019/2144 (the revised General Safety Regulation), any of the safety systems it regulates[872] should function without the use of any kind of biometric information of drivers or passengers.

839 In the context of connected and automated vehicles, biometric data used for the purpose of uniquely identifying a natural person may be processed, within the remit of Art. 9 GDPR and the national exceptions, amongst other things, to enable access to a vehicle, to authenticate the driver/owner and/or to enable access to a driver's profile settings and preferences[873].

840 Services studied during the AVENUE project involved processing of biometric data, such as the recognition of facial expressions and emotions of passengers of the automated minibuses etc.

841 When considering the use of biometric data, guaranteeing the data subject full control over his or her data involves, on the one hand, providing for the existence of a non-biometric alternative (e.g. using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory), and on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal[874]. The European Data Protection Board has also defined principles related to biometric data[875].

4.2.4.5.3 Offence-related data

842 According to Art. 10 GDPR, processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law.

843 In practice, automated vehicles might record administrative infringements, such as speeding or failing to stop at a red light, or even criminal offences[876].

844 In order to process data that relates to potential criminal offences within the meaning of Art. 10 GDPR, the European Data Protection Board recommends to resort to the local processing of the data where the

[872] Namely advanced emergency braking systems, intelligent speed assistance, emergency lane-keeping systems, driver drowsiness and attention warning, advanced driver distraction warning and reversing detection.

[873] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 65 p. 16.

[874] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 65 p. 16.

[875] See Guidelines 3/2019 on processing of personal data through video devices and Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.

[876] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 9.

data subject has full control over the processing in question. Indeed – except for some exceptions (such as accidentology studies) – external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data[877].

845 Some categories of personal data from connected and automated vehicles could reveal that a criminal offence or other infraction has been or is being committed ("offence-related data") and therefore be subject to special restrictions (e.g. data indicating that the vehicle crossed a white line, the instantaneous speed of a vehicle combined with precise location data). Notably, in the event that such data would be processed by the competent national authorities for the purposes of criminal investigation and prosecution of criminal offence, the safeguards provided for in Art. 10 GDPR would apply[878].

4.2.4.6 Anonymisation

846 Anonymisation (or anonymisation) nowadays is used as a common denominator for different types of techniques such as randomisation, generalisation etc.[879]. It can be described as "a process by which information is manipulated (concealed or hidden) to make it difficult to identify data subjects"[880] or "a technique of processing personal data to reduce the likelihood of identifiability of individuals"[881].

847 The use of anonymisation is specifically encouraged by Recital 13 of the ITS Directive as "*one of the principles of enhancing individuals' privacy*".

4.2.4.6.1 Difference between pseudonymisation and anonymisation

848 Anonymisation and pseudonymisation techniques are both privacy-enhancing techniques.

849 Pseudonymisation is defined by Art. 4 para. 5 GDPR as processing in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

850 Pseudonymisation is not aimed at rendering a data subject unidentifiable (to the contrary of anonymisation), given that – at least in the hands of the data controller – the original data are either still

[877] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 67 p. 17.

[878] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 68 p. 17.

[879] For a presentation and a discussion of these techniques, see Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) 0829/14/EN, Adopted on 10 April 2014, p. 11 et seq and BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, p. 14.

[880] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.4.1 p. 93 and the quoted reference.

[881] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.4.1 p. 96.

available or deductible[882]. Therefore, pseudonymised personal data still qualifies as personal data in accordance with Recital 26 GDPR.

4.2.4.6.2 Different approaches to anonymisation

851 As provided by Recital 26 (see N 813 above), the principles of data protection should not apply to anonymous information, namely:

- information which does not relate to an identified or identifiable natural person or
- to **personal data rendered anonymous** in such a manner that the data subject is not or no longer identifiable (e.g. depersonalised data, emphasis added).

852 As regards the concept of "personal data rendered anonymous", the Irish Data Protection Authority followed a liberal approach in 2019 when it considered that "Organisations don't have to be able to prove that it is impossible for any data subject to be identified in order for an anonymisation technique to be considered successful. Rather, **if it can be shown that it is unlikely that a data subject will be identified given the circumstances** of the individual case and the state of technology, the data can be considered anonymous"[883] (emphasis added).

853 To the contrary, Article 29 Data Protection Working Party[884] followed a strict/absolute approach in 2014 (i.e. before entry into force of the GDPR), when it considered that "the outcome of anonymisation as a technique applied to personal data should be, in the current state of technology, **as permanent as erasure**, i.e. making it impossible to process personal data" and that "importance should be attached to contextual elements: **account must be taken of "all" the means "likely reasonably" to be used for identification by the controller and third parties**, paying special attention to what has lately become, in the current state of technology, "likely reasonably" (given the increase in computational power and tools available)"[885] (emphasis added).

854 Critics have been raised against this approach, highlighting that the Article 29 Working Party applies an absolute definition of the acceptable risk in the form of zero risk. It was argued that the GDPR itself at Recital 26 GDPR does not require a zero risk approach and that, if the acceptable risk threshold is zero for any potential recipient of the data, there is no existing technique that can achieve the required degree of anonymisation[886].

---

[882] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.4.2 p. 96.

[883] Data Protection Commission (Ireland), Guidance Note: Guidance on Anonymisation and Pseudonymisation, June 2019, p. 5 https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf (last consultation 31 August 2022).

[884] Which has been replaced by the European Data Protection Board after entry into force of the GDPR and should not be confused with the UNECE's WP.29 World Forum for Harmonization of Vehicle Regulations.

[885] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) 0829/14/EN, Adopted on 10 April 2014, p. 6; for more details see FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11 et seq., p. 15.

[886] EMAM/ALVAREZ, A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques, International Data Privacy Law, Volume 5, Issue 1, January 2014, p. 73-87.

855 Despite these critics, the French Commission Nationale de l'Informatique et des Libertés ("**CNIL**") also followed a strict/absolute approach in 2020, i.e. after the entry into force of the GDPR, when it considered that "anonymisation is a processing which consists of using a set of techniques in such a way as to make it impossible, in practice, to identify the person **by any means and in an irreversible manner**"[887] (emphasis added).

856 As regards existing case law, the judgment from the Court of Justice of the European Union ("**CJEU**") dated 19 October 2016 in the "Breyer" case[888], though still rendered before the GDPR era, might indicate another, more practical, mindset.

857 In that judgment, which dealt with the question whether dynamic IP addresses may constitute personal data, the CJEU held that the possibility to combine a dynamic IP address with additional data held by the internet service provider does not constitute a means likely reasonably to be used to identify the data subject "*if the identification of the data subject is prohibited by law or* ***practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power****, so that the risk of identification appears in reality to be insignificant.*"[889] (emphasis added).

858 Therefore, it might be argued that the Court of Justice of the European Union tends to steer towards a risk-based approach (also applied by the Irish Data Protection Authority recently) and away from the Article 29 Working Party's and CNIL's strict/absolute approach. This being said, it should also be taken into consideration that this case law has been published in 2016 and that the technological and legal landscape, as well as the opinions regarding the processing of personal data, has seriously changed and evolved since then.

859 According to a recent and convincing scholar's article, acceptance of a residual risk of identification, even where data is anonymized, appears to be the only realistic option in light of contemporary developments. Research has amply highlighted that anonymisation is never absolute. If the law were to insist that it must be, the only logical conclusion would be that data that once was personal data can only ever be pseudonymised, but never anonymized[890].

860 And according to the legal experts of the 2018 LeMO study, when contemplating to apply anonymisation techniques, any company should (at least) adopt a risk-based approach, in line with the "Breyer" case, whereby it considers the possible re-identification risks that may remain after application of the technique[891].

---

[887] Commission Nationale de l'Informatique et des Libertés (France), L'anonymisation de données personnelles, 19 mai 2020, https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles (last consultation 31 August 2022).

[888] ECJ Case 582/14, ECLI:EU:C:2016:779 dated 19 October 2016, N 44 – Patrick Breyer, § 45-46.

[889] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.4.1 p. 101.

[890] FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 35; see also BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 4.2 p. 15.

[891] DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018, § 3.4.1 p. 101.

861 As a conclusion, it should be retained that the current legal definition of anonymous data is subject to uncertainty. Indeed, the definitions adopted in the GDPR, by the Article 29 Working Party and by national supervisory authorities diverge significantly. Whereas the GDPR admits that there can be a remaining risk of identification even in relation to anonymous data, others have insisted that no such risk is acceptable[892].

4.2.4.6.3 Data anonymisation and the preservation of relevant information for perception systems

862 From a technical point of view, anonymisation techniques can also trigger issues and interfere with the functioning of AI obstacle detection processes.

863 In the field of automated vehicles, one of the most common anonymisation approaches is to perform automated blurring of faces, bodies and license plates on images capture by front, rear and side cameras. Image blurring is just one of the many possible techniques amongst others such as pixelisation, mosaic, cartooning, masking, warping, morphing[893], etc.

864 However, these approaches are not suitable for tasks such as pedestrian and vehicle detection, as they corrupt the nature of the data, and may negatively affect the generalization capability of the learning process. The same applies in cases where it is necessary to detect gaze direction, body pose or intrinsic attributes of the agents such as sex, age, skin tone or even emotional expressions. The most important challenge is to anonymize the data while preserving relevant information for perception and HMI systems. This is particularly important for predictive perception, i.e. for predicting the actions, including intention and motions of road users[894].

865 This is the main objective of image de-identification methods which attempt to replace directly identifying characteristics such as faces or license plates with synthesized and realistic features, while still preserving relevant non-identifying attributes. For example, license plates numbers can be replaced by using a different but realistic number. If other unrealistic transformations are applied to de-identify license plates, vehicle detection systems may learn synthetic features that will not exist in real conditions, with the risk of obtaining unpredictable results, as well as reduced performance[895].

866 Generative Adversarial Networks ("**GAN**") are well suited for de-identification since they can produce natural-looking synthesized images of any given object using adversarial training and a considerable number of approaches have recently emerged. When these techniques are applied to de-identify vehicles, the transformation may involve specific requirements to preserve some attributes and replace some others[896].

---

[892] FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11.

[893] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 40.

[894] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 40 and quoted references.

[895] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 40 and quoted references.

[896] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 40 and quoted references.

4.2.4.7 Data processed by connected and automated vehicles

867 As mentioned previously, connected and automated vehicles already process many information and data today and the amount of data processed by these vehicles is expected to hugely increase in the future, positioning the automotive sector as one of the largest data generators and one of the first fields where Internet of Things ("**IoT**") will be deployed at large scale.

868 The overall performance of automated driving systems is based on data processed by multiple sensors, including enhanced high-definition maps, 3D point clouds, images sequences from on-board cameras pointing outside and inside, inertial measurement systems, audio systems for speech recognition[897] etc.

869 In order to illustrate the issues arising from the processing of personal data by automated vehicles, the case of videocameras will be detailed in the next section.

4.2.4.7.1 Videocameras

870 Video data processed by videocameras is one of the most relevant from a privacy point of view, as it potentially enables to (directly) identify natural persons as defined above.

871 As signalled by the European Data Protection Board[898], videocameras triggers the issue of filming public places, which requires an assessment of the specific relevant legislative framework of each Member State, which exceeds the scope of this deliverable and will not be examined in this deliverable.

872 According to the case law of the European Court of Justice, the image of a person recorded by a camera falls under the concept of "personal data" if it enables the identification of the concerned person. This is based on the assumption that a visible person is also identifiable. The means of the controller (relative approach) or third parties (absolute approach) to identify the concerned person are considered as sufficient[899].

873 But according to some opinions, it is not convincing to assume the processing of personal data if the identifiability requires a further processing step, such as the storage of the video data on a physical support (hard drive etc.) in order to be seen by the controller for instance. If the necessary further step (such as storing the data in a durable manner) cannot even occur or is not possible for technical reasons, the process should not qualify as processing of personal data[900].

---

[897] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.1 p. 38.

[898] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 35 p. 11.

[899] SCHRÖDER, Datenschutz beim Kameraeinsatz im Automobil, Zeitschrift für Datenschutz, ZD Heft 6/2021, C.H. Beck, p. 304; ECJ Case C-212/13, ECLI:EU:C:2014:2428 dated 11 December 2014, N 22 – František Ryneš; ECJ Case C-345/17, ECLI:EU:C:2019:122 dated 14 February 2019, N 31 – Sergejs Buivids.

[900] See SCHRÖDER, Datenschutz beim Kameraeinsatz im Automobil, Zeitschrift für Datenschutz, ZD Heft 6/2021, C.H. Beck, p. 304.

874 In the case of cameras used in motor vehicles, a decisive role for the risk assessment would be whether the video data can leave the vehicle, which entails additional identification risks, or whether it remains "on-board"[901].

875 Recital 14 of the 2019 revised General Safety Regulation[902] considers that no identifiability can be assumed in a closed system[903]: "[…] *Event data recorders should operate on a closed-loop system, in which the data stored is overwritten, and which does not allow the vehicle or holder to be identified.* […]". As mentioned above (see N 780), it should be noted that the question of the applicability of the GDPR to personal data processed in closed systems is unclear.

876 Regarding the various types of cameras that can be found in a vehicle, SCHRÖDER came to the following conclusions[904]:

- In the case of "dashcams"[905], which store a file that can be further processed (i.e. also outside the vehicle) and thus enables the identification of the person, the possibility of relating to a person (and thus a responsibility under data protection law) for everyone who has access to the stored data has to be affirmed. Concerned persons are pedestrians, possibly also drivers of other cars and passengers, as well as other third parties and road users, if the owner of the dashcam (controller) or a third party has access to the video data.
- For videocameras that functionally replace rear-view mirrors, the possibility of relating to a person is doubtful, especially for temporal and possibly also optical reasons, but may be present in individual cases, for instance if the safety operator (or the driver or another person accessing to the video data) happens to see a person that he knowns (e.g. a neighbour etc.) in the monitor […].
- In the case of camera systems that are not designed to reproduce an image for a viewer, but only to process an image in order to identify road markings, traffic signs, traffic lights or even persons (as a category of road user, but not singularised) and then immediately delete it, there is no processing of personal data at all, despite the temporary storage of personal data – not for the driver in any case, but also not vehicle manufacturer or maintenance service, as long as they have no technical access to the data, at any time.
- On-board camera-based monitoring for drowsiness, declining attention or declining concentration on the part of the "driver" is a special case, because the driver is the person concerned, whereas in the other cases mentioned above the concerned person is located outside the vehicle. This scenario is also similar for passengers of automated minibuses, as they are identified (and can potentially provide, amongst others, their consent to the processing of personal data).

  In this scenario, it is nevertheless also possible to record external third parties unintentionally. In this case, data protection liability can only arise if someone – in particular the vehicle

[901] See SCHRÖDER, Datenschutz beim Kameraeinsatz im Automobil, Zeitschrift für Datenschutz, ZD Heft 6/2021, C.H. Beck, p. 304 and quoted references.

[902] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019.

[903] See SCHRÖDER, Datenschutz beim Kameraeinsatz im Automobil, Zeitschrift für Datenschutz, ZD Heft 6/2021, C.H. Beck, p. 304.

[904] See SCHRÖDER, Datenschutz beim Kameraeinsatz im Automobil, Zeitschrift für Datenschutz, ZD Heft 6/2021, C.H. Beck, p. 305 and quoted references.

[905] A dashcam is a video camera mounted usually on the dashboard of a vehicle and used to continuously record activity through the vehicle's windshield.

manufacturer – gains access to the image data, but not in the case of a closed system, i.e. if no one can access the data, whether "over the air" or through a wired connection.

4.2.4.7.2 Intermediate conclusion

877 In-vehicle data follows multiple purposes and helps to ensure correct operation of the vehicle, checks proper functioning, identifies and corrects errors and refines and optimizes vehicle functions. This data can be used for different purposes, such as repair and maintenance, road safety and traffic management, fleet management, quality management, product development and non-automotive uses (e.g. car sharing, car rental, insurance)[906].

878 This data can be processed within the vehicle and, under some circumstances, exchanged through communication channels with other vehicles, external infrastructure and vehicle manufacturers or other third parties. Connected and automated vehicles can also receive data from external sources (e.g. roadside units, other vehicles etc.)[907].

879 Vehicle-generated data and data produced by the driver, the safety operator or passengers are valuable to many parties, not only to vehicle manufacturers but also for public authorities (e.g. road traffic data) and entities who would like to provide services to car users and passengers (e.g. automotive aftermarket services, online shopping providers, insurance companies etc.)[908]. As described in the AVENUE vision's loops, the use and re-use of vehicle data will be crucial for the further development of automated minibuses.

880 Whether or not all vehicle-generated data can be considered as personal data is still under discussion amongst scholars and there is no clarity on this question. Different groups of stakeholders have diverse views on what types of car-generated data should be classified as personal[909], often depending of their position on the data driven economy.

881 Non-personal data processed by a vehicle may be defined as technical data and can be assimilated to vehicle performance data such as tyre pressure, vehicle speed, oil level, fuel consumption, mileage, wear and tear on vehicle parts, battery charge status, etc. This data is mostly generated within the vehicle control unit(s)[910].

---

[906] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 10 and the quoted reference.

[907] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 10.

[908] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 10 and the quoted reference.

[909] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 147.

[910] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, p. 147.

882 The sensors of automated minibuses such as videocameras, high definition LIDAR's and RADAR's process data that could be attributed to a natural person under the definitions of Art. 4 para. 1 GDPR and Recital 26 and therefore should be considered as personal data.

883 These sensors tend to collect data which may pinpoint the date and time an individual was at a precise location (GPS/geolocalisation data), which may also reveal their identity (for videocameras providing images of the passengers and other natural persons) and may as well allow to draw inferences about their personal lives[911].

884 According to the European Data Protection Board, much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g. the driver's complete identity), as well as indirectly identifiable data such as the details of journeys made (speed, distance travelled), the vehicle usage data (e.g. data relating to driving style or the distance covered), or the vehicle's technical data (e.g. data relating to the wear and tear on vehicle parts such as engine coolant temperature, engine RPM, tyre pressure), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status[912].

885 Therefore, in order to lift this situation of clarity, it would be welcome either to receive further guidance from the competent authorities (for instance the EDPD) or to provide more refined definitions within an upcoming legal act (for instance in an upcoming "mobility data act").

4.2.5 Controller and processor of personal data

4.2.5.1 Concepts and delimitations

886 The GDPR defines two functional concepts, namely the "controller" and the "processor" of personal data.

887 The "controller" of personal data ("*Verantwortlicher*", "*responsable du traitement*") is any person or entity which determines the purposes and means of the processing of personal data (see Art. 4 para. 7 GDPR and Art. 24 et seq. GDPR).

888 To the contrary, the "processor" ("*Auftragsverarbeiter*", "*sous-traitant*", see Art. 4 para. 8 GDPR and Art. 28 et seq. GDPR) only processes personal data on behalf of the controller: the processor is bound by the controller's instructions.

[911] Arcade, Proceedings of workshop on data sharing, Contribution to D2.4, D2.4 Joint CCAM Networking Report, 29 March 2021, Version 1.0, § 2.3 p. 8.

[912] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 29 p. 9 and N 62 p. 15.

889 When two or more controllers jointly determine the purposes and means of processing, the GDPR also foresees the possibility of "joint controllers" (Art. 26 para. 1 GDPR). In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of relevant information to the data subjects (Art. 13 and 14 GDPR)[913]. The case law of the Court of Justice of the European Union has adopted a broad definition of the notion of "joint controllers"[914].

890 As seen previously, "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see art. 4 para. 2 GDPR).

891 According to Article 29 Working Party, determining the purposes and means amounts to determining respectively the "why" and the "how" of certain processing activities. This underlines that controllership is a functional concept "intended to allocate responsibilities where the factual influence is"[915].

892 In the context of automated vehicles, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, Art. 28 GDPR sets out data processors' obligations[916].

4.2.5.2 Responsibilities and obligations

893 The definition of the roles of controller and processor determine their various responsibilities and obligations defined within the GDPR, amongst others:

- fulfilling the data protection principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality etc., see § 4.2.6 below for further details);
- applying and maintaining technical and organisational safety measures (i.e. compliance with the principles of privacy by design, privacy by default, security of processing etc.);
- implementing mandatory contractual structures (data processing agreements, joint controller arrangements, if applicable, etc.);
- organisational documentation of processing activities including risk-based data protection impact assessments (Art. 35 GDPR);
- data-breach obligations and precautions;

[913] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 41 p. 12.

[914] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.3 p. 9 and the quoted references.

[915] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) 00264/10/EN, Adopted on 16 February 2010, p. 13.

[916] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 41 p. 12.

- data subject access requests as well as other rights of the data subjects (rectification and erasure, restriction of processing, portability etc.);
- information obligations to the data subjects.

894 For further details, it can be referred to the dedicated article on GDPR and automated minibuses published recently by BENYAHYA and others[917].

4.2.5.3 Personal data processed by automated vehicles

895 As of today, in the context of automated vehicles, the functions of controller and processor as defined by the GDPR can be performed by many various entities and encompass various scenarios.

896 The controller can be the vehicle manufacturer, the fleet operator/PTO[918], although the latter can also be a processor[919]. If the vehicle owner is a legal person, such as for instance a PTO, it could also be considered as a processor.

897 However, if the vehicle owner is a natural person, he can hardly be seen as responsible for the data processing: if it is assumed that the controller is the one who "offers" the data processing, derives the benefit from it and also has an actual possibility to influence the type and scope of the data processing, they are to be regarded as persons affected by the processing[920] and the qualification as controller would be problematic[921].

898 The data processor can also be an equipment manufacturer and automotive supplier that process data on behalf of the vehicle manufacturer (which does not imply they cannot be a data controller for other purposes)[922] as well as the software developer(s)[923], service providers, insurers[924] etc.

---

[917] See BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.3 p. 9.

[918] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 39.

[919] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 6.2 p. 4.

[920] GYSIN (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation – UVEK), Datenschutz Mobilitätsdaten, Bericht, ASTRA-D-DB3D3401/359, 30 November 2020, p. 15.

[921] ALGORIGHT e.V (HESSEL), Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, Saarbrücken, 30 April 2021, § 2 p. 7.

[922] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 41 p. 12.

[923] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 6.2 p. 4.

[924] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 41 p. 11.

Table 1. Roles according to the GDPR, depending on different circumstances, as described by MULDER/VELLINGA [925].

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

899 The loops described in the AVENUE vision involve to have many stakeholders processing and re-processing data, which will require to assess if these definitions are fit or if they should be somehow amended, for instance by creating new legal entities (also taking into consideration new entities such as data intermediates created by the DGA, see Appendix A § 3.2.2.3 above).

4.2.6 Key principles of the GDPR (Art. 5 GDPR)

900 Art. 5 GDPR sets out seven key principles related to the processing of personal data, which controllers need to be aware of and comply with when collecting and otherwise processing personal data:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

[925] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 6.2 p. 4; see also BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, Figure 3 p. 11.

901 These principles will be briefly described in the following section.

4.2.6.1 Lawfulness, fairness, and transparency

902 Art. 5 para. litt. a GDPR provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency").

4.2.6.1.1 Lawfulness

903 Lawfulness means that any processing of personal data carried out by a controller must have a legal basis under the GDPR (see N 942 et seq. below), be otherwise compliant with the requirements of the GDPR (see in particular Art. 6 to 9 GDPR, e.g. lawfulness of the processing, the conditions for consent and for child's consent etc.) and not involve any otherwise unlawful processing or use of personal data[926].

4.2.6.1.2 Fairness

904 Fairness is a relatively broad principle, which requires that any processing of personal data must be fair towards the individual whose personal data are concerned and avoid being unduly detrimental, unexpected, misleading or deceptive[927].

905 Fairness requires that personal data collection, processing, uses and outcomes do not discriminate negatively against any individual or group of data subjects. This entails that data-driven connected and automated vehicle operations should be as inclusive as possible and that equal access and opportunities need to be safeguarded for all parties, particularly for potentially vulnerable persons and groups[928].

4.2.6.1.3 Transparency

906 Transparency is a particularly important principle of data protection within the GDPR, with various related rights and obligations seeking to ensure that processing of personal data is clear and transparent to individuals and regulators. Controllers must provide individuals with information regarding the processing of their personal data in a format that is concise, easily accessible, easy to understand and in clear and plain language. This should be done before personal data are collected and subsequently whenever changes to the processing operation are made[929].

907 Specific rules regarding transparency obligations are found in Art. 12 to 14 GDPR, including details on the specific types of information which must be provided to data subjects and the manner in which it must be provided. In order to be transparent, controllers must ensure the means of conveying information is the most appropriate for their platform and target audience. In particular, the principles of fair and transparent processing require that the individual be informed of the existence of the processing operation and its purposes[930].

---

[926] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 2.
[927] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 2.
[928] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.1 p. 35.
[929] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 2.
[930] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 2.

4.2.6.2 Purpose limitation

908 According to Art. 5 para. 1 litt. b GDPR, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("Purpose limitation").

909 The aim of this principle is to ensure that controllers are clear and open from the outset about the proposed processing of personal data and to ensure that the purposes are in line with individuals' reasonable expectations. Careful consideration of and robust compliance with this principle also assists data controllers with the principles of data minimisation and accountability[931].

910 The principle of purpose limitation creates an obligation for data controllers to map the purposes for which they collect personal data and avoid reuse, combination or repurposing of those data for incompatible purposes[932].

911 In its opinion on purpose limitation, Article 29 Working Party considered that any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered "further processing" and must meet the requirement of compatibility[933] foreseen at Art. 6 para. 4 GDPR.

912 Further processing is only appropriate where the new purpose for processing is not incompatible with the original purpose. Whether any subsequent processing could be compatible with the original purpose will depend on any link with the original purpose, the context in which the personal data has been collected, the nature of the personal data, the possible consequences of the intended further processing for individuals and the existence of appropriate safeguards[934] (see Art. 6 para. 4 GDPR).

913 According to the EDPB, when data is collected on the basis of consent as required by Art. 5 para. 3 ePrivacy Directive or on one of the exemptions of Art. 5 para. 3 ePrivacy Directive and subsequently processed in accordance with Art. 6 GDPR, it can only be further processed either if the controller seeks additional consent for this other purpose or if the data controller can demonstrate that it is based on a Union or Member State law to safeguard the objectives referred to in Art. 23 para. 1 GDPR[935].

914 The EDPB considers that further processing on the basis of a compatibility test according to Art. 6 para. 4 GDPR is not possible in such cases, since it would undermine the data protection standard of the ePrivacy directive. Indeed, consent, where required under the ePrivacy directive, needs to be specific and informed, meaning that data subjects must be aware of each data processing purpose and entitled to refuse specific ones. Considering that further processing on the basis of a compatibility test according to

[931] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 3.

[932] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.4 p. 8 and the quoted references.

[933] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN, Adopted on 2 April 2013, § III.2.1 p. 21.

[934] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 3.

[935] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 53 p. 14.

Art. 6 para. 4 GDPR is possible would circumvent the very principle of the consent requirements set forth by the current ePrivacy directive[936] (see also Appendix A § 4.3.3 N 995 et seq. below).

4.2.6.3 Data minimisation

915 Pursuant to Art. 5 para. 1 litt. c GDPR, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").

916 This essentially means that data controllers should collect the minimum amount of data they require for their intended processing operation; they should never collect unnecessary personal data. This principle complements, in particular, the principle of purpose limitation[937].

917 Implementing data minimisation supports data protection/privacy by design and by default (see § 4.2.7 below), limits the amount of personal data which could be lost or stolen in the event of a personal data breach, assisting with ensuring the integrity and confidentiality of personal data and it makes it easier for organisations to ensure that the personal data they hold are accurate and up to date, supporting compliance with the principles of accuracy[938].

918 The GDPR does not define what amount of personal data is "adequate, relevant and limited". This will have to be assessed by controllers depending on the circumstances of their intended processing operations. Controllers should also periodically review the amount and nature of personal data which they process, ensuring it remains adequate, relevant, and necessary, including by deleting data which no longer fulfil these criteria[939].

4.2.6.4 Accuracy

919 Art. 5 para. 1 litt. d GDPR provides that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy").

920 In general, the reasonable steps controllers are required to take to ensure the accuracy of personal data will depend on the circumstances and in particular on the nature of the personal data and of the processing. Controllers need to also keep in mind their obligations in relation to data subjects' right to rectification – to have inaccurate personal data rectified, or completed if it is incomplete[940].

---

[936] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 53 p. 14; see also. BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 2.4 p. 9.

[937] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 3.

[938] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 3.

[939] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 3.

[940] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 4.

4.2.6.5 Storage limitation

921 According to Art. 5 para. 1 litt. e GDPR, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […] ("storage limitation").

922 Controllers should therefore, in general, delete personal data as soon as it ceases to be necessary for the purposes for which it was originally collected. To this end, the GDPR recommends that time limits should be established by the controller for erasure or for a periodic review. In line with the principle of transparency, controllers should also ensure that individuals are aware of retention periods or the criteria used to calculate them[941].

923 Depending on the circumstances, it may also be appropriate for controllers to anonymise data once it is no longer necessary that the individual be identified or identifiable[942].

924 This is a challenging principle to comply with in the connected and automated vehicles scenario, as the data collected is of very diverse nature, used for very different purposes and shared with different entities, making it difficult to have an effective control over the retention periods[943].

925 Data controllers must be able to control the periods for which they store data and protocol the periodic deletion of personal data[944].

4.2.6.6 Integrity and confidentiality

926 Pursuant to Art. 5 para. 1 litt. f GDPR, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

927 In other words, controllers must ensure that their security measures adequately protect against accidental or deliberate harm, loss or dissemination of the personal data they process. These security measures should cover not only cybersecurity but also physical and organisational security measures. Organisations must also routinely check that their security measures are up-to-date and effective[945].

928 As a horizontal and cross-sectoral instrument, the GDPR does not specify the security measures which organisations should implement, as technological and organisational best practices are constantly evolving. Controllers should consider a range of options to determine the most appropriate measures under the circumstances, as there is no "one size fits all" approach to data security[946].

---

[941] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 4.

[942] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 4.

[943] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 31.

[944] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 31.

[945] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 5.

[946] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 5.

929 Relevant considerations when assessing appropriate measures include, but are not limited to: the principle of data minimisation (Art. 5 para. 1 litt. c GDPR, seen above under § 4.2.6.3); the principles of data protection by design and by default (Art. 25 GDPR, see § 4.2.7 below); transparency with regard to the functions and processing of personal data, enabling the individual to monitor the data processing; and the pseudonymisation and/or encryption of personal data[947].

930 The main obligations for data controllers stemming from this principle are the following:

- Data controllers must elaborate a record of processing activities to list and keep record of the data processing activities followed in the organization.
- Data controllers must perform, prior to beginning processing, an assessment of the risks the processing activity has on the privacy of the data subjects. To do that, it shall be necessary to perform two distinct risk management procedures, based on the level of foreseeable risk of the activity: (i) if the foreseeable risk is high, a data protection impact assessment ("**DPIA**") must be performed; and (ii) if the risk is not high, a basic risk analysis shall be conducted.
- They also need to put in place procedures to make them capable of dealing effectively with personal data breaches. Where necessary, data controllers have the obligation to notify personal data breaches to a data protection authority or to even communicate the breach to the natural persons affected[948].

931 Given the scale and sensitivity of the personal data that can be generated and processed via automated vehicles, it is likely that processing – particularly in situations where personal data is processed outside of the vehicle – will often result in a high risk to the rights and freedoms of individuals[949]. Therefore, DPIA should be performed before deploying automated vehicles and minibuses.

4.2.6.7 Accountability

932 Art. 5 para. 2 GDPR provides that the controller shall be responsible for and be able to demonstrate compliance with Art. 5 para. 1 GDPR.

933 This means that controllers need to ensure they comply with the principles seen above, but also have appropriate processes and records in place to demonstrate compliance[950].

4.2.7 Privacy by design and privacy by default

934 Data processing must take into account the principles of "Privacy by Design" and "Privacy by Default" already during design and manufacture[951].

[947] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 5.

[948] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 32.

[949] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 32.

[950] Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, p. 5.

[951] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 5.2.3 p. 25.

4.2.7.1 Privacy by design

935 Art. 25 para. 1 GDPR sets the obligation for data protection by design. Data protection by design entails taking data protection into account from the start of the very early phases of designing, in this case, the system for the automated vehicle. The technical and organisational measures to safeguard data protection by design depend on several elements, such as: "[…] the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"[952].

936 The development process starts with designing a system. It is important, in the earliest stage possible, for developers to consider data protection regulation when they design a system that will process personal data. However, data protection by design does not stop after the first phases of a development process. On the contrary, data protection by design is important "throughout the technological lifecycle" of any system processing personal data[953].

937 Sometimes, technical changes are made or become possible throughout the lifecycle of a system, for instance through a software update of the system of the automated vehicle. This can affect the way in which a system processes personal data. In that case, it is once more important to take the principle of data protection by design into consideration. Art. 25 para. 1 GDPR adds to this that data protection by design should take place "both at the time of the determination of the means for processing and at the time of the processing itself"[954].

938 Encryption by means of state-of-the-art algorithms is one of the measures to achieve privacy by design in the field of automated vehicles[955].

4.2.7.2 Privacy by default

939 Data protection by default refers to the implementation of safeguards that protect the right to data protection as a default setting. Art. 25 para. 2 GDPR states that the obligation of data protection by default applies to: "[…] the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility".

940 According to the European Data Protection Supervisor, this means that the most privacy friendly configuration should be set by default. This configuration, pursuant to Art. 25 para. 2 GDPR, concerns at

[952] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 8.2 p. 9 and quoted references.

[953] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 8.2 p. 9 and quoted references.

[954] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 8.2 p. 9 and quoted references.

[955] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.2 p. 40 and quoted references; see also BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 2.3 p. 4 et seq.

least the general principles of data minimisation, purpose limitations, storage limitation and confidentiality[956].

941 The principles of privacy by design and by default affect primarily vehicle manufacturers (and other data controllers) in regard to the design of the means to collect, store and process the data collected through vehicles, as well as to provide a setup which is privacy friendly by default. Privacy by design and by default is an open issue for the industry. According to a report published end of 2021, vehicle manufacturers of connected vehicles collected geolocation data by default unless the car user activated the privacy mode[957].

4.2.8 Lawfulness of processing personal data

As mentioned above, the GDPR imposes the principle of a ban of processing personal data which can only be performed under one of the legal basis defined by Art. 6 GDPR, which will be presented in the following section.

4.2.8.1 Consent of the data subject

942 According to Art. 6 para. 1 litt. a GDPR, processing of personal data shall be lawful only if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

943 The European Data Protection Board underlines that, when the data processing is based on consent, all elements of valid consent have to be met. This means that consent shall be free, specific and informed and constitute an unambiguous indication of the data subject's wishes as interpreted in the EDPB guidelines on consent. Data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given[958].

944 Classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of automated vehicles: valid consent may be gathered from driver/safety operator of the vehicles as well as for the passengers.

945 But as regards data from the surroundings of the automated vehicles' environment processed by sensors such as videocameras including other external road users (drivers of other vehicles, cyclists and pedestrians on the street etc.) can hardly be obtained on the basis of consent, so other mechanisms are needed to ensure privacy (e.g. privacy-by-design)[959].

---

[956] MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021, § 8.3 p. 10 and quoted references.

[957] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 34.

[958] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, § 1.5.2 N 48 p. 13.

[959] See FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, § 5.3.1 p. 39.

4.2.8.2 Performance of a contract

946 Pursuant to Art. 6 para. 1 litt. b GDPR, processing of personal data shall be lawful only if the processing is necessary for the performance of a contract to which the data subject is party[960].

947 In the context of automated vehicles, for some data subjects such as passengers of automated minibuses, a contractual relationship will exist in the form of a transportation agreement. Other specific scenarios may exist[961]. But similar issues than for consent arise: for external third parties such as drivers of other vehicles, pedestrians on the street etc., it seems difficult to identify which contractual relationship might serve as legal basis.

4.2.8.3 Public interest

948 According to Art. 6 para. 1 litt. e GDPR, processing of personal data shall be lawful only if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

949 The C-ITS Working Group noted that in order to apply public interest as legal basis, the necessity for this processing must be laid down in a national or European law. This could be envisaged in implementing the European strategy for road safety, transport efficiency and environmental sustainability. The ITS Directive 2010/40/EU allows the European Commission to adopt binding specifications in this field via delegated acts[962].

950 Public interests that can be pursued with automated driving can be seen, for example, in the reduction of the number of road accidents, in more efficient traffic control (also in coordination between private and public transport) or in the reduction of emissions[963].

951 A scholar has considered that public interest will be appropriate when personal data is processed as a part of the regular transportation service with the involvement of public authorities (e.g. the local government)[964].

952 However, invoking public interests seems too vague to be able to justify the processing of personal data in the field of automated driving. Legal basis' allowing the processing of personal data in the concrete cases and defining limits will be needed. This applies in particular when public authorities are involved, as their actions must rely on a legal basis from the outset[965].

---

[960] Or in order to take steps at the request of the data subject prior to entering into a contract.

[961] See Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (WP 252) 17/EN, Adopted on 4 October 2017, § 3.2 p. 5.

[962] Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (WP 252) 17/EN, Adopted on 4 October 2017, § 3.2 p. 5.

[963] Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 3: Handling Data, SVI 2017/044, October 2020, p. 47.

[964] BU-PASHA, Legal aspects, public interest, and legitimate interest in processing personal data to operate autonomous buses in the regular transportation system, Security and Privacy, 2022;e247, May 2022, § 4 p. 7.

[965] Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 3: Handling Data, SVI 2017/044, October 2020, p. 47.

4.2.8.4 Legal obligation

953 In accordance with Art. 6 para. 1 litt. c GDPR, processing of personal data shall be lawful only if the processing is necessary for compliance with a legal obligation to which the controller is subject.

954 For example, such legal obligation might arise from provisions related to Event Data Recorders and/or Data Storage Systems for Automated Driving, such as Art. 6 para. 1 litt. g and para. 4 and 5 GSR[966] on Event Data Recorders.

955 Legislations in Member States such as France amongst others with the "*Ordonnance n° 2021-442 du 14 avril 2021 relative à l'accès aux données des véhicules*" and Germany (Art. 1g StVG "*Datenverarbeitung*") already provide legal obligations to process personal data.

956 According to some scholars, a distinction should be made between data processed to develop the AI systems of the automated vehicle so that they meet the safety requirements for type-approval and placing on the market and data used to improve the AI systems once the automated vehicle has been deployed. In the first case, the main legal basis is related to vehicle type-approval requirements. In the second case, data collection and processing must be subject to some legal basis, such as the consent of the in-vehicle user[967].

4.2.8.5 Legitimate interests

957 Pursuant to Art. 6 para. 1 litt. f GDPR, processing of personal data shall be lawful only if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data[968].

958 On the possible application of the necessity to process data for a legitimate interest, Article 29 Working Party recalled that this should not be treated as a "last resort" opportunity for complex cases, where other grounds for lawful processing are difficult to apply[969].

959 The C-ITS Working Group has also considered the processing for the purpose of the legitimate interests pursued by the controller. In order to be able to rely on this legal ground, the data controller must ensure that the processing does not override the interests or fundamental rights and freedoms of the data subject. Many constraints stand in the way of the applicability of this legal basis[970].

---

[966] Regulation 2019/2144 dated 27 November 2019 ("revised General Safety Regulation" or "GSR"), which will apply on 6 July 2022.

[967] FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021, §5.3.1 p. 39.

[968] In particular where the data subject is a child.

[969] Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (WP 252) 17/EN, Adopted on 4 October 2017, § 4.4 p. 11.

[970] Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (WP 252) 17/EN, Adopted on 4 October 2017, § 3.2 p. 5.

960 According to some interpretation, road traffic safety might be invoked as a legitimate interest, but this should be assessed in further details.

4.2.9 Right to data portability

961 The right of data portability (Art. 20 GDPR) is granted directly to the data subject (i.e. the natural person to whom personal data relates) and is therefore not available to legal entities.

962 In a nutshell, it allows the data subject under certain conditions "*to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided*"[971].

963 This concept is similar to the concept of "Porting of data" provided by Art. 6 of Regulation 2018/1807 as regards the free flow of non-personal data (see also § 3.4.2.3 N 730 above).

964 Data portability is highly relevant for autonomous vehicles and IoT ecosystems. It applies to access of personal data by promoting interoperability to protect the data subjects from having personal data stored in an incompatible format or manner. Developing interoperable formats that enable data portability across applications and platforms in the ecosystem also supports the digital single market in general. The right to data portability is one of the fundamental data subject rights in the GDPR[972].

4.2.10 Data subjects' control rights

965 In addition to the right of portability seen above, the GDPR implements various rights to data subjects.

966 To ensure transparency and fairness of data processing, the GDPR grants the data subjects specific control rights. It should be mentioned that, at every stage of data processing, data subjects remain the owners of their personal data as verified by the right of access to personal data (granted by Art. 15 GDPR)[973].

967 By providing individuals access rights, the GDPR imposes a number of obligations to the entities that collect and process data and allows the data protection authorities to request demonstrations of accountability or impose fines if data subjects' rights are not secured[974].

968 Therefore, data controllers have to provide specific practices and technologies to the data subjects to control and exercise their rights during the entire data processing. For instance, the information about the exercise of rights is available in the privacy policy at the controller's website. Controllers can facilitate,

[971] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.1.1.2 p. 15.

[972] Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D5.4, IoT Policy Framework for autonomous vehicles applications, 26 December 2018, Version 1.0, § 3.6.4 p. 81.

[973] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.2 p. 8.

[974] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.2 p. 8.

specifically, the access, deletion, transfer or removal of personal data by providing modification settings[975].

4.2.10.1 Right to information

969 Data subjects have the right to be informed by the data controller about the purposes and other aspects of the processing performed on the data subject's personal data (see Art. 13 and 14 GDPR and Recital 39 GDPR).

970 Prior to the processing of personal data by the controllers, the data subjects shall be informed, in a transparent way, of the identity of the data controller, the purpose of processing, the data recipients, the data retention period and the data subjects' rights[976].

971 In the case of automated vehicles, this right to be informed is particularly problematic for external roads users such as drivers of conventional vehicles, cyclists and pedestrians, due to the fact that is seems practically difficult to provide them will the required information.

4.2.10.2 Right of access

972 According to the right of access (Art. 15 GDPR), data subjects have the right to obtain confirmation from the data controller as to whether or not personal data concerning the data subject is being processed and, where that is the case, right to access to the personal data and the following information:

- the purposes of processing;
- the categories of personal data concerned;
- who the data has been transferred to (data recipients);
- how long the data is going to be stored;
- the possibility to exercise additional rights, such as the erasure of the data, limitation of the processing or the right to object to commercial communications;
- to acknowledge the procedure to file any kind of claim before the corresponding authority[977].

973 The right of access is also a key control tool at the disposal of data subjects to be aware of the scope of the processing derived from the use of automated vehicles. The complex set of information that data controllers such as vehicle manufacturers and other actors could be processing recommend that data controllers provide for easily accessible and easy to use mechanisms for data subjects to access their information[978].

[975] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.2 p. 8.

[976] BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022, § 3.2 p. 8.

[977] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

[978] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

4.2.10.3 Right to rectification

974 The right to rectification (Art. 16 GDPR) ensures that the data subject can request the data controller to modify the personal data that is inaccurate without undue delay[979].

4.2.10.4 Right to erasure (or "right to be forgotten")

975 According to Art. 17 GDPR, data subjects have the right to obtain from the data controller the erasure of personal data that is no longer necessary, under certain circumstances[980].

976 This is also an important right for the connected and automated vehicle environment, as it allows users to request the deletion of data about them stored in connection to specific vehicle(s)[981].

4.2.10.5 Right to object and to withdraw consent

977 The right to object (Art. 21 GDPR) grants data subjects the possibility to object, at any time, to the processing of personal data with direct marketing purposes or to the processing of personal data based on a public interest of the data controller or a legitimate interest of the data controller or a third party[982].

978 The right to withdraw consent also provides a right to revoke the consent provided by the data subject to the data controller at any time (Art. 7 para. 3 GDPR).

4.2.10.6 Right not to be subject to automated decision-making

979 This right grants not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her[983].

4.2.11 Administrative fines

4.2.11.1 Overview

980 According to Art. 83 para. 5 GDPR, infringements shall be subject to fines up to EUR 20 million, or in the case of undertakings, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

981 As of September 2022, the highest fines were[984]:

---

[979] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

[980] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

[981] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

[982] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

[983] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 33.

[984] https://www.tessian.com/blog/biggest-gdpr-fines-2020/ (last consultation 31 August 2022).

- EUR 746 million issued by the Luxembourg National Commission for Data Protection in July 2021 against Amazon.com Inc for non-compliance with cookie consent (an appeal has been fined against this decision[985]);
- EUR 405 million issued by the Irish Data Protection Authority in September 2022 against Instagram after an investigation found the social media platform mishandled teenagers' personal information[986];
- EUR 225 million issued by the Irish Data Protection Authority in September 2021 against WhatsApp for failure to properly explain its data processing practices in its privacy notice (an appeal has been fined against this decision[987]);
- EUR 90 million issued by the CNIL in December 2021 against Google Ireland Ltd for non-compliance with cookie consent procedures on Youtube.

4.2.11.2 Example: fine issued by the Data protection authority of Lower Saxony

982 In July 2022, the State Commissioner for Data Protection of Lower Saxony (Germany) imposed a fine of EUR 1.1 million to a vehicle manufacturer, in connection with the use of a service provider for research trips for a driver assistance system to avoid traffic accidents[988].

983 A test vehicle from the vehicle manufacturer was stopped for a traffic check by the police, which noticed unusual attachments on the vehicle, which turned out to be cameras on site. The vehicle was used to test and train the functionality of a driver assistance system to avoid traffic accidents. The traffic situation around the vehicle was recorded, amongst other things for error analysis[989].

984 The State Commissioner for Data Protection of Lower Saxony established four violations of the GDPR[990].

985 First, due to a mistake, the vehicle was missing magnetic signs with a camera symbol and other mandatory information for those affected by data protection law, in this case the other road users, which breached Art. 13 GDPR[991].

---

[985] https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/ (last consultation 31 August 2022).

[986] Ireland fines Instagram €405 million over protection of children's data | Euronews (last consultation 6 September 2022).

[987] https://iapp.org/news/a/details-emerge-on-appeal-of-whatsapps-225m-euro-gdpr-fine-2/ (last consultation 31 August 2022).

[988] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022); see also the press release of the State Commissioner https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/1-1-millionen-euro-bussgeld-gegen-volkswagen-213835.html (last consultation 25 August 2022).

[989] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022).

[990] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022).

[991] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022).

986 Second, further investigation also revealed that the vehicle manufacturer had not concluded a data processing contract with the company that carried out the journeys, although this would have been required under Art. 28 para. 3 GDPR[992].

987 Third, the vehicle manufacturer did not proceed to a data protection impact assessment, contrary to Art. 35 GDPR[993].

988 Finally, there was no explanation of the technical and organizational protective measures in the list of processing activities, which constituted a violation of the documentation requirements under Art. 30 GDPR[994].

4.3 ePrivacy directive

4.3.1 Introduction

989 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "**ePrivacy Directive**"), as amended by Directive 2009/136/EC dated 25 November 2009 (the "**Cookies Directive**"), provides the basic legal framework for data protection in electronic communications. Its scope is not limited to traditional telecommunications (i.e. phone-based services), as the ePrivacy Directive applies to "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service"[995].

990 Published in 2002, it was initially planned to have the ePrivacy Directive revised in the same time than the issuance of the GDPR, but despite the efforts of the European legislator, it was not possible to reach an agreement on time for the revision of the ePrivacy Directive. A proposal for a new text (called "Regulation on Privacy and Electronic Communications"[996]) has been published in 2017 but has yet to be adopted (as of August 2022). With a proposed two year implementation wanted by the European Council[997], it does not seems that this upcoming regulation will enter into force quickly.

4.3.2 Relation to GDPR

991 The ePrivacy Directive is a *lex specialis* to the GDPR, which means that it particularises and complements the GDPR as regards personal data in the electronic communications sector. All matters not specifically

[992] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022).

[993] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022).

[994] https://gdprhub.eu/index.php?title=LfDI_%28Lower_Saxony%29_-_Volkswagen (last consultation 31 August 2022).

[995] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.1 p. 47.

[996] See https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (last consultation 31 August 2022).

[997] https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-protection-day-2022 (last consultation 31 August 2022).

addressed by ePrivacy rules in relation to personal data are, therefore, regulated by the GDPR (for instance, the requirements for a valid legal consent)[998].

992 For an overview of the interplay between GDPR and the ePrivacy Directive, it can be referred to the study published by FIA Region I end of 2021[999] or to the 2020 EDPB's Guidelines on processing personal data in the context of connected vehicles[1000].

4.3.3 Application to connected and automated vehicles

993 Automated machine to machine communications (including most IoT applications) falls out of scope of the ePrivacy Directive[1001].

994 Nonetheless, according to the European Data Protection Board, connected vehicles (and thus also automated vehicles) should be considered as terminal equipment (like a computer or a smartphone) under the ePrivacy Directive and the provisions of Art. 5 para. 3 ePrivacy Directive apply where relevant[1002]. Storing information on an end-user's terminal equipment, or gaining access to information already stored, happens through the use of "cookies" and other tracking technologies[1003].

995 Similarly, a report on the GDPR considers that "when the data collected from the connected vehicle qualifies as personal data under the GDPR, both the ePrivacy Directive and the GDPR apply". The report also highlights the sometimes difficult interaction between these two pieces of legislation[1004] (see below).

996 When the data collected from the connected vehicle qualifies as personal data under the GDPR, both the ePrivacy Directive and the GDPR applies. There is an open debate on the question of the legal basis applicable to subsequent processing operations involving the information gathered from the connected vehicle[1005].

997 According to the EDPB, as a general rule, where consent is necessary pursuant to Art. 5 para. 3 ePrivacy Directive, data controllers cannot rely on one of the legal basis in Art. 6 GDPR other than consent for

[998] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 36.

[999] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 38 et seq.

[1000] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 53 et seq. p. 14.

[1001] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.1 p. 47.

[1002] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 13 p. 7.

[1003] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 38.

[1004] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 11.

[1005] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 11.

subsequent processing operations, especially in relation to tracking and profiling processing activities. This opinion is not necessarily followed by the industry, especially in the digital advertising ecosystem[1006].

998 Nonetheless, the EDPB acknowledges that service providers can rely on the performance of a contract as a legal basis as per Art. 6 para. 1 litt. b GDPR for subsequent processing operations if certain conditions are met. In addition, the EDPB acknowledges that in some cases and subject to transparency and additional safeguards, tracking and profiling may also be permissible to prevent fraudulent use of the services offered[1007].

4.3.4 Consequences

999 Under the current framework, where both the GDPR and the ePrivacy Directive apply, the situation is complex.

1000 Amongst others, Art. 5 para. 3 ePrivacy Directive provides that "[…] the subscriber or user concerned is provided with clear and comprehensive information […] *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller. […]".

1001 In the context of the connected (and automated) vehicles, Art. 5 para. 3 ePrivacy Directive takes precedence over Art. 6 GDPR with regards to the activity of "storing or gaining access to information" collected[1008].

1002 The European Data Protection Board considers that prior consent is required for the storing of information or the gaining of access to information already stored[1009].

1003 The parties targeted by the ePrivacy Directive include principally traditional telecommunications service providers, but not online service providers offering functionally comparable services, nor IoT applications providers. The elevated level of protection of traffic data and location data as specified in the ePrivacy Directive is therefore limited to those stakeholders; other service providers collecting, processing or sharing traffic data and location must instead abide by the GDPR[1010] (and not the ePrivacy Directive).

[1006] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 11.

[1007] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 11.

[1008] Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021, p. 10; see also BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, p. 1.

[1009] European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021, N 14 p. 7.

[1010] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.3 p. 48.

1004 The ePrivacy Directive contains high level provisions requiring such communications to be appropriately secured and in relation to the confidentiality of electronic communications. In addition, it contains rules relating to location data and other traffic data, restricting the conditions under which such data can be collected and used. Other provisions relate to traditional communications issues (such as caller identification, unsolicited communications and subscriber directories)[1011].

1005 Similarly to the GDPR, the ePrivacy Directive focuses (amongst other topics) on ensuring that the confidentiality of electronic communications is appropriately ensured. As a result, data sharing is not a priority of the ePrivacy Directive. Nonetheless, location data and traffic data are of significant importance to the data economy, as key inputs for the creation of innovative services, and for this reason the constraints on collecting and sharing such data are highly relevant[1012].

1006 Traffic data is defined in Art. 2 of the ePrivacy Directive as follows: "Any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".

1007 It is a very broad data category comprising most types of metadata that are required to connect communications or enable transactions between devices. Location data is a specific kind of traffic data, which indicates the geographic position of the terminal equipment of a user. Given the importance of geolocation in the data economy (e.g. to enable localised services), access to such information is both economically important and privacy sensitive[1013].

1008 The ePrivacy Directive imposes strict rules for such data types. Traffic data may only be retained by the provider of a public communications network or publicly available electronic communications service for as long as required to enable the service or billing; thereafter it must be deleted or anonymised. Any other use (notably for added value services) requires the prior informed consent of the users involved, which must be revocable at any time[1014].

1009 Location data other than traffic data similarly requires either consent or anonymisation[1015].

1010 Collectively, the rules imply that such data cannot be shared with third parties by providers of a public communications network or publicly available electronic communications service, with the exception of

[1011] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.1 p. 47.
[1012] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.2 p. 48.
[1013] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.2 p. 48.
[1014] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.2 p. 48.
[1015] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.2 p. 48.

third parties that they have authorised to engage in processing activities that the service providers themselves are already permitted to engage in[1016].

1011 The ePrivacy Directive has had a significant impact on data sharing (and more broadly data collection and data processing) in the telecommunications industry, since processing of communications contents, traffic data and location data are generally only permissible if required for the provision and management of the service, or based on the consent of the subscriber. This provides an admittedly high level of protection for potentially very sensitive communication, but also acts as a clear disincentive for data sharing. As underlined above, there is a consistency challenge due to the scoping of the Directive, which targets only traditional telecommunications services but excludes most types of IoT services, which are critical e.g. in the context of smart mobility, smart cities etc.[1017].

1012 As mentioned, the ePrivacy Directive is currently under review (since 2017) and a Proposal for a new text has been published in 2021[1018].

* * *

[1016] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.2 p. 48.

[1017] Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020, § 3.3.4.5 p. 49.

[1018] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

5 Overview of the legal framework as regards cybersecurity

1013 As with many other fields involving connected and automated vehicles, cybersecurity is a new and very important field for the automotive industry that has been covered only partially until today. It will require a specific and growing attention in the future.

5.1 Various definitions

1014 UN Regulation 155 defines cybersecurity as "the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components"[1019].

1015 Other definitions exists, which are more focussed on cybersecurity as an activity rather than a condition.

1016 For instance, according to Art. 2 para. 1 Cybersecurity Act[1020], cybersecurity means "the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats".

1017 For this deliverable, it is not necessary to establish a particular definition and this question can be left open.

5.2 Existing legal framework

5.2.1 UN Regulations

1018 From mid-2022 onwards, two recent UN Regulations dedicated to cybersecurity will become applicable[1021]:

- UN Regulation 155 related to Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system and
- UN Regulation 156 related to Uniform provisions concerning the approval of vehicles with regards to software update and software update management.

[1019] Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, Submitted by the Working Party on Automated/autonomous and Connected Vehicles, ECE/TRANS/WP.29/2020/79 REVISED, § 2.2 p. 3, see also E/ECE/TRANS/505/Rev.3/Add.154.

[1020] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[1021] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 5.

1019 These regulations set minimum requirements that need to be met in order to have a vehicle approved for use on public roads. Both of these new Regulations are of importance to the cybersecurity of new vehicles[1022].

5.2.1.1 UN Regulation 155

5.2.1.1.1 Issuance of Certificate of Compliance for Cyber Security Management System

1020 In order to have vehicle of the categories M and N[1023] approved for use on public roads, Art. 7.2.1 UN Regulation 155 requires the vehicle manufacturer to issue of a "Certificate of Compliance for Cyber Security Management System" ("**CSMS**").

1021 According to Art. 2.3 UN Regulation 155, the CSMS is defined as "a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyberattacks".

1022 These "organisational processes" include:

- processes used for the identification of risks to vehicle types (Art. 7.2.2.2 litt. b UN Regulation 155) and
- processes used for testing the cybersecurity of a vehicle type (Art. 7.2.2.2 litt. e UN Regulation 155).

5.2.1.1.2 Approval

1023 The approval authority shall grant type-approval with regard to cyber security only to such vehicle types that satisfy the requirements of UN Regulation 155 (Art. 5.1 UN Regulation 155).

1024 According to Art. 5.1.1 litt. a to e UN Regulation 155, the approval authority or the technical service verifies that the manufacturer has, amongst other things, taken the necessary steps to:

a) collect and verify the information required under the Regulation through the supply chain so as to demonstrate that supplier-related risks are identified and managed;
b) document risks assessment (conducted during development phase or retrospectively), test results and mitigations applied to the vehicle type, including design information supporting the risk assessment;
c) implement appropriate cybersecurity measures in the design of the vehicle type;
d) detect and respond to possible cybersecurity attacks; and
e) log data to support the detection of cyberattacks and provide data forensic capability to enable analysis of attempted or successful cyberattacks.

1025 The duty to maintain the systems and account for current risks is ongoing. Approval for the systems may be withdrawn by the original approval authority if it comes to light that the system no longer conforms to the specifications of UN Regulation 155. Vehicle manufacturers who gain approval in accordance with this

[1022] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 5.
[1023] See Art. 1.1 UN Regulation 155.

Regulation must maintain and keep their cybersecurity systems up to date throughout the lifecycle of a vehicle[1024].

1026 Such processes are intended to contribute to ensure the cybersecurity of the vehicle. This is also reflected in Annex 5 of the Regulation, which sets out mitigation methods to different cybersecurity risks, including "Measures to prevent and detect unauthorized access" (Art. 9.1 UN Regulation 155). Therefore, the UN Regulation 155 seeks to ensure that no one can gain unauthorised access to the vehicle's systems[1025] and thus contributes to the principles on cybersecurity formulated in vehicles in Recommendation § 2.2.3.

1027 In accordance with Art. 5.3 UN Regulation 155, type-approval authorities shall not grant any type-approval without verifying that the vehicle manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects covered by UN Regulation 155.

1028 Therefore, it should be noted that the provisions of this regulation are not limited to the vehicle type but also to the management of cyber security by the vehicle manufacturer.

5.2.1.1.3 Requirements for the Cyber Security Management System

1029 The type-approval authority has to verify that the vehicle manufacturer has a CSMS in place and verify its compliance with UN Regulation 155 (Art. 7.2.1 UN Regulation 155).

1030 The vehicle manufacturer has to demonstrate that the CSMS applies to the development phase, the production phase and the post-production phase (Art. 7.2.2.1 UN Regulation 155, see also Recommendations for deployment of AVs in chapter § 2.2).

1031 According to Art. 7.2.2.2 UN Regulation 155, the vehicle manufacturer shall demonstrate that the processes used within their CSMS ensure security is adequately considered […].

5.2.1.2 UN Regulation 156

1032 UN Regulation 156 sets requirements on how to update the software of the vehicle.

1033 According to Art. 6.2 UN Regulation 156, the vehicle manufacturer will have to provide a Certificate of compliance for Software Update Management System ("**SUMS**").

1034 Art. 2.5 UN Regulation 156 defines the SUMS as a "systematic approach defining organisational processes and procedures to comply with the requirements for delivery of software updates" as defined by the UN Regulation 156.

1035 Similar to the certificate for the CSMS of UN Regulation 155, the vehicle manufacturer has to define a number of organisational processes in place to obtain a Certificate of compliance for the SUMS.

[1024] Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022, § 6.161 p. 120.

[1025] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 6.

1036 These are processes such as the mechanism whereby any interdependencies of the updated system with other systems can be identified (Art. 7.1.1.5 UN Regulation 155) and the process to establish the compatibility of the update with the target vehicle configuration before it is issued (Art. 7.1.1.7 UN Regulation 155).

1037 At European level, the European Commission's delegated regulation as regards the technical requirements for fully automated vehicles produced in small series makes UN Regulation 156 mandatory for approval under European scheme. The accompanying amendment to Annex IV of the framework EU Regulation 2018/858 updates the ongoing compliance obligations for vehicle manufacturers to ensure products continue to remain compliant once in production to include software update requirements as set by UN Regulation 156. This aims to ensure any software update does not render the vehicle non-compliant with its approval[1026].

5.2.1.3 Assessment

1038 UN Regulations 155 and 156 provide a first line of defence by setting up means to avoid having unauthorized access to road vehicles.

1039 According to legal literature, these regulations lack of provisions aiming to limit the damage when unauthorized access has been obtained by malicious third parties (i.e. hackers). In addition, they do not include measures such as the separation of safety-critical controls from safety irrelevant controls such as the entertainment system of the vehicle[1027].

1040 It has also been highlighted that they hardly provide concrete measures and that they contain so-called "undefined legal concepts" prone to interpretation. For instance, according to Art. 7.3.5 UN Regulation 155, the vehicle manufacturer shall put in place "appropriate and proportionate measures" to secure dedicated environments […][1028].

5.2.1.4 Revised General Safety Regulation

1041 The revised General Safety Regulation includes references to the UN Regulations and "other regulatory acts" at Recital 26 revised GSR:
"The connectivity and automation of vehicles increases the possibility for unauthorised remote access to in-vehicle data and the illegal modification of software over the air. In order to take into account such risks, UN Regulations or other regulatory acts on cybersecurity should be applied on a mandatory basis as soon as possible after their entry into force".

1042 Regarding software updates, Recital 27 revised GSR provides that:

[1026] https://www.gov.uk/government/publications/em-on-an-amendment-to-regulation-2018858-1055922-c20223823 (last consultation 31 August 2022).

[1027] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 6.

[1028] VON BODUNGEN, Wie sicher ist sicher genug? Manipulationsfreiheit und Verfügbarkeit der Daten als Zulassungsvoraussetzungen?, Zulassungsrechtliche Herausforderungen des Autonomen Fahrens, Universität Basel, Tagung vom 10. Oktober 2019, Slide 15.

"Software modifications can significantly change vehicle functionalities. Harmonised rules and technical requirements for software modifications should be established in line with the type-approval procedures. Therefore, UN Regulations or other regulatory acts regarding software update processes should be applied on a mandatory basis as soon as possible after their entry into force. However, those security measures should not compromise the obligations of the vehicle manufacturer to provide access to comprehensive diagnostic information and in-vehicle data relevant to vehicle repair and maintenance".

1043 Therefore, since its entry into force on 6 July 2022, the revised GSR requires software update compliance with UN Regulation 156 for European type-approval[1029].

1044 Besides provisions on the event data recorders foreseen at Art. 6 para. 1 litt. g revised GSR (see § 3.6.1 above), the revised GSR does not contain further provisions and requirements regarding cybersecurity.

5.2.2 Network and Information Systems Directive

5.2.2.1 Overview

1045 The Network and Information Systems ("**NIS**") Directive[1030] aims to ensure a high level of security for network and information systems in the European Union, meaning the ability to resist to actions compromising the availability, confidentiality, authenticity or integrity of such networks and systems.

1046 The NIS Directive requires that Member States establish a list of operators of essential services within their territories that are active in important economic sectors. For road transport, Annex II of the NIS Directive includes road authorities responsible for traffic management control[1031] and operators of intelligent transport systems[1032].

1047 As the European Union Agency for Cybersecurity ("**ENISA**") has identified intelligent transport systems as Essential Service Operators in the road transport sub-sector, it can be concluded that the NIS is applicable in the context of AVs. At the moment ENISA is in the process of addressing the security of smart cars in order to contribute to the existing regulatory framework. It is therefore safe to assume that as the adoption of AVs reaches a critical mass, that specific ITS operators will be designated as operators of essential services[1033].

[1029] https://www.tuvsud.com/en/industries/mobility-and-automotive/automotive-and-oem/autonomous-driving/assessment-of-automotive-software-updates (last consultation 31 August 2022).

[1030] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[1031] As defined by Art. 2 para. 12 Delegated Regulation (EU) 2015/962 (see also N 3.5.2.3.1 below).

[1032] As defined by Art. 4 para. 1 Directive 2010/40/EU (see also N 442 above).

[1033] BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, § 1 p. 3.

1048 Art. 14 NIS Directive requires that Member States set security requirements for identified operators of essential services. These requirements include at least ensuring that these operators: (i) adopt measures to have an appropriate level of security with regard to the risk of the service and to avoid and minimise security incidents and (ii) notify swiftly of any incident with significant effects on the service continuity[1034].

1049 Member States must also impose a similar requirement on digital services such as cloud providers. Finally, the NIS Directive requires that Member States adopt a national strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cybersecurity and designate a competent national authority[1035].

5.2.2.2 Assessment

1050 Due to NIS Directive's focus on the security of network and information systems and links to operators of intelligent transport systems, the NIS Directive is mainly of in importance in relation to V2V, V2I and V2X communication. By increasing the security of these communication means, the NIS Directive contributes to prevent unauthorised access to the vehicle's systems. In addition, the NIS Directive contributes to limiting the damage that can be done, as operators of essential services are obliged to take measures to minimise the impact of incidents[1036].

1051 Interestingly, there is an interplay between the NIS Directive and the GDPR when personal data are involved. While the NIS Directive was adopted at the same time as the GDPR, the two pieces of legislation do not reference each other in their respective texts. Nevertheless, whenever personal data are handled by either operators of essential services or digital service providers, both pieces of legislation need to be considered. The compliance requirements are assessed separately, which may increase the regulatory burden for stakeholders and particularly for SMEs[1037].

1052 The concrete implementation of the NIS Directive proved to be difficult, resulting in fragmentation at different levels across the internal market[1038].

5.2.3 NIS2

1053 To respond to the growing threats posed with digitalisation and the surge in cyberattacks, the European Commission has submitted a proposal to replace the NIS Directive ("**NIS2**") and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations and

[1034] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 71.

[1035] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 71.

[1036] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 10.

[1037] CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021, § 4.3.3 p. 176.

[1038] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (last consultation 31 August 2022).

introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the European Union. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term[1039].

1054 Overall, the NIS2 proposal sets itself three general objectives:

- Increase the cyber-resilience's level of a comprehensive set of businesses operating in the European Union across all relevant sectors, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures.
- Reduce inconsistencies in resilience across the internal market in the sectors already covered by the NIS Directive, by further aligning
  - i) the *de facto* scope;
  - ii) the security and incident reporting requirements;
  - iii) the provisions governing national supervision and enforcement; and
  - iv) the capabilities of the Member States' relevant competent authorities.
- Improve the level of joint situational awareness and the collective capability to prepare and respond, by
  - i) taking measures to increase the level of trust between competent authorities;
  - ii) by sharing more information; and
  - iii) setting rules and procedures in the event of a large-scale incident or crisis[1040].

5.2.4 Cybersecurity Act

1055 The Regulation on the European Union Agency for Cybersecurity and on information and communication technology cybersecurity certification[1041] (also called "**Cybersecurity Act**") published on 17 April 2019 creates an European cybersecurity certification framework in order to ensure that information and communication technology ("**ICT**") products, services and processes are evaluated in accordance with cybersecurity schemes (i.e. sets of rules, technical requirements, standards and procedures) established at the European level.

1056 AV-related products and services could be subject to such certification schemes[1042]. At the current stage, it is unclear whether ICT products include (automated) vehicles or parts of (automated) vehicles[1043], but it seems rather likely that they will qualify as ICT products.

[1039] European Parliamentary Research Service (EPRS), The NIS2 Directive – A high common level of cybersecurity in the EU, PE 689.333, June 2022, p. 1.

[1040] European Parliamentary Research Service (EPRS), The NIS2 Directive – A high common level of cybersecurity in the EU, PE 689.333, June 2022, p. 7.

[1041] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[1042] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 63.

[1043] VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, April 2022, p. 10.

1057 The Cybersecurity Act mandates ENISA to prepare European cybersecurity schemes at the European Commission's request. European certification schemes must be designed to guarantee that certified ICT products, services and processes meet a minimum set of cybersecurity requirements such as data integrity, confidentiality, authenticity, availability or having sufficient security updates mechanisms[1044].

1058 Cybersecurity schemes should also incorporate security by design and by default principles. Depending on the risk level of the certified product, each European scheme established will specify one or more assurance levels ranging from basic to high. Certification schemes with a high level of assurance are in principle issued only by national authorities and ensure that certificated product is evaluated to minimise the risk of cyberattacks carried out by actors with significant skills and resources. Cybersecurity certification can be made mandatory under national or European law for specific ICT products, services or processes. Thus, a mandatory cybersecurity certification could mitigate the potential risks associated with the development of automated vehicles and increase consumer trust in these products and services[1045].

1059 In November 2019, ENISA adopted good practices for the security of connected and automated vehicles[1046] which recommend that vehicle manufacturers and service providers encrypt personal data to prevent its disclosure to illegitimate parties[1047].

1060 Data exchange, networking and mobility products must meet the highest security standards, otherwise they will not be accepted by users in the long term. Appropriate guidelines must be developed for the trustworthy identification of the participants (mobility service providers, users/data subjects etc.), but also for other assets that require protection, such as contracts and business processes – at least to the extent necessary in the respective case (e.g. in the event of damage). Appropriate guidelines for the trustworthiness of the identification as well as the processes for handling transactions must be developed[1048].

1061 Furthermore, technical measures should be used to support the legally secure purpose limitation in the use of services[1049]. Mobility service providers must guarantee secure data transmission and storage according to the state of the art. Platform operators, in turn, must set up data processing in such a way that data is processed locally and redundantly wherever possible (means of transport or edge device, edge and cloud computing)[1050].

[1044] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 63.

[1045] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 63.

[1046] European Union Agency for Cybersecurity, ENISA good practices for security of smart cars, November 2019 https://www.enisa.europa.eu/publications/smart-cars (last consultation 31 August 2022).

[1047] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 63.

[1048] Nationale Plattform Zukunft der Mobilität (NPM), Ergebnisbericht der Nationalen Plattform Zukunft der Mobilität – Ergebnisse aus drei Jahren NPM (2018-2021), October 2021, § 3.3. p. 46.

[1049] See for example International Data Spaces Association (IDSA).

[1050] Nationale Plattform Zukunft der Mobilität (NPM), Ergebnisbericht der Nationalen Plattform Zukunft der Mobilität – Ergebnisse aus drei Jahren NPM (2018-2021), October 2021, § 3.3. p. 46.

1062 If anonymised mobility data is used, clear requirements for anonymisation must be formulated and further protection concepts that reduce the risk of de-anonymisation as far as possible must be developed (as mentioned previously, see Recommendation § 5.5 above). Technical guidelines defined by the competent authorities as well as international security standards for the development of secure communication infrastructures must be applied[1051].

1063 Important in the development of new legislation is that IT security in the automotive industry is generally not a vehicle type-specific property, but is determined within the framework of on-board network architectures and functional modules[1052].

1064 As of today, mutual recognition of the cybersecurity management system ("CSMS") certificate and the necessary documentation are not regulated at UNECE or European level. There is also no regulation regarding the qualification and skills of the auditors and the inspection bodies and authorities in order to be able to adequately audit the manufacturer's cyber security management system processes[1053].

1065 CSMS assessment criteria, the expected CSMS level of detail and the depth of testing are completely non-existent. Guidance and/or references to standardised solutions are, however, necessary in order to be able to assess objectively and professionally[1054].

5.2.5 Guidelines on the exemption procedure for European approval of automated vehicles

1066 The Guidelines of the European Commission dated 12 February 2019 (see also N 778 above) focus on personal data protection and cybersecurity in two parts. Firstly, the guidelines deal with the issue of installation of event data recorders, which is also regulated by the revised GSR[1055]. Secondly, the on-board device must be able to store data securely, comply with European data protection law and be protected from manipulation while allowing national authorities access to such data. Based on experience gained, more specific requirements for data recording devices can be developed (recording time, retention time, for what purposes the data is used, standardized approach, way of handling personal data etc.)[1056].

1067 In the section on cybersecurity, the guidelines call for the vehicle to be designed to protect the vehicle against automated hacking, using state-of-the-art techniques and to comply with European data

[1051] Nationale Plattform Zukunft der Mobilität (NPM), Ergebnisbericht der Nationalen Plattform Zukunft der Mobilität – Ergebnisse aus drei Jahren NPM (2018-2021), October 2021, § 3.3. p. 46.

[1052] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 5.1.1 p. 21.

[1053] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 5.1.1 p. 21.

[1054] Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, May 2020, § 5.1.1 p. 21.

[1055] See Appendix A § 3.6.1 above.

[1056] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 8 and quoted references.

protection legislation. This includes a manufacturer risk assessment, design measures and adequate processes to avoid, mitigate and respond to cyberattacks. Vehicle manufacturers should also adopt measures, such as those relating to software updates installed in automated vehicles necessary to ensure in-use cybersecurity over the vehicle's lifetime[1057].

5.3 Specific national provisions dedicated to data of automated vehicles

5.3.1 France

5.3.1.1 Ordinance no 2021-442 dated 14 April 2021 on access to vehicle data

1068 The Ordinance no 2021-442 dated 14 April 2021 on access to vehicle data[1058] grants access to vehicle data for specific purposes, such as better understanding of road accidents and the related risks, state of road infrastructure and road traffic, as well as the correction of defects.

1069 Access to some of the vehicle data is granted to several actors, including:

- road infrastructure managers ("*gestionnaires d'infrastructures routières*");
- mobility organising authorities ("*autorités organisatrices de la mobilité*");
- law enforcement authorities; and
- insurers[1059].

5.3.1.1.1 Accident prevention

1070 In view of road risks, incidents and accidents, the provisions of Art. L. 1514-1, L. 1514-4, L. 1514-5 and L. 1514-7 Transport Code provide for access to all data :

- necessary for "the detection of accidents, incidents or accident-causing conditions in the vehicle's driving environment, excluding data intended for communication systems to emergency call centres" for the prevention of accidents, with the aim of providing rapid responses to identified risks or improving the response in case of accidents;
- relating to "devices recording the driving status" ("*dispositifs d'enregistrement des données d'état de délégation de conduite*"), in the event of a road accident, for the purpose of studying and analysing accidents and for determining the necessary compensation;
- "collected by the vehicle's automation system while driving that is necessary to enhance the safety of driving delegation systems" for the reconstitution of scenarios characterising driving situations that could lead to serious injury to vehicle occupants or to other road users[1060].

[1057] ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, 24 September 2021, § 2.3.1 p. 8 and quoted references.

[1058] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043370884 (last consultation 31 August 2022).

[1059] https://www.argusdelassurance.com/juriscope/analyses-d-experts/l-acces-aux-donnees-des-vehicules-sous-le-controle-de-la-cnil.185034 (last consultation 31 August 2022).

[1060] https://www.argusdelassurance.com/juriscope/analyses-d-experts/l-acces-aux-donnees-des-vehicules-sous-le-controle-de-la-cnil.185034 (last consultation 31 August 2022).

5.3.1.1.2 Assessment of road infrastructure and observation of the traffic flows

1071 Articles L. 1514-2 et seq. Transport Code provide a framework for access to data for the purposes of knowledge and mapping of road infrastructure and its equipment, with a view to guaranteeing infrastructure safety conditions but also for the purposes of understanding and observation of the road traffic flows[1061].

5.3.1.1.3 Correction of defects

1072 Art. L. 1514-6 Transport Code grants the possibility to the vehicle manufacturer or the importer ("*importateur*") to correct by telematics ("*par voie télématique*") defects in systems, components or technical units that may affect a whole series of vehicles and that are likely to seriously compromise the safety of the vehicle, its occupants or other road users[1062].

5.3.1.1.4 Duty to notify cyberattacks

1073 Art. L. 1514-8 Transport Code requires the vehicle manufacturer or its representative ("*mandataire*") to notify the type-approval authority, without delay, after becoming aware of cyberattacks that may affect the information systems contributing to the operation or safety of the vehicles. Failure to do so may result in a fine of EUR 75'000.-. Moreover, the text specifies that these data may not be used as evidence for traffic offences.

5.3.1.1.5 Consent not required, but mandatory anonymisation

1074 Although the consent of data subjects is not required, as specified in the majority of the provisions, the Ordinance provides a privacy framework for processing by imposing the anonymisation "by a process guaranteeing the irreversible deletion"[1063] of the driver's data, as well as the vehicle's serial number or identifiers. This seems to follow the French CNIL's strict approach as regards anonymisation of personal data, see Appendix A § 4.2.4.6.2 N 855 above.

1075 In addition, the Ordinance will be supplemented by a decree specifying the conditions for accessing and storing the data, which has been notified to the European Commission in July 2022[1064].

[1061] https://www.argusdelassurance.com/juriscope/analyses-d-experts/l-acces-aux-donnees-des-vehicules-sous-le-controle-de-la-cnil.185034 (last consultation 31 August 2022).

[1062] https://www.argusdelassurance.com/juriscope/analyses-d-experts/l-acces-aux-donnees-des-vehicules-sous-le-controle-de-la-cnil.185034 (last consultation 31 August 2022).

[1063] Therefore

[1064] "Décret relatif à l'accès à certaines données des véhicules pour la prévention des accidents et l'amélioration de l'intervention en cas d'accident, la connaissance et la cartographie de l'infrastructure routière et de son équipement et la connaissance du trafic routier", notification number: 2022/494/F (France), see https://ec.europa.eu/growth/tools-databases/tris/fr/search/?trisaction=search.detail&year=2022&num=494 (last consultation 31 August 2022).

5.3.2 Germany

5.3.2.1 Introduction

1076 Data privacy has been a controversial topic during the legislative procedure enacting the second Amendment of the German road traffic law, which led to lawmakers being requested to draft a mobility data regulation defining the framework for processing non-personal data generated in vehicles (in particular clarifying rights of use of this data by citizens and possible access needs of private providers and government bodies)[1065].

5.3.2.2 Cybersecurity

1077 In the interest of road safety, the vehicle manufacturer must prove throughout the entire development and operating period of the automated vehicle that the electronic and electrical architecture of the vehicle and the associated electronic and electrical architecture are secured against attacks (§ 1f para. 3 (1) StVG). He also needs to carry out a risk assessment and demonstrate the existence of a sufficiently secure radio link with the vehicle (§ 1f para. 3 (2) and (3) StVG).

5.3.2.3 Processing of data by the vehicle owner

1078 In accordance with Art. 6 para. 1 litt. c GDPR, data processing is lawful if the processing takes place in order to comply with a legal obligation. Such an obligation can be found in § 1g para. 1 and 2 StVG and is specified by Part. 3 of Annex I of the Autonomous Vehicle Approval and Operation Ordinance.

1079 According to § 1g StVG, the owner of an autonomous vehicle is required to store certain personal data, such as the vehicle identification number, position data, environmental conditions and speed in relation to certain incidents and to transmit this data to the "*Kraftfahrt-Bundesamt*" upon request. Such incidents include accidents, unintended lane changes and evasive maneuvers. The owner is required to store this data from the time that an event occurs (for instance an accident) until the time that the vehicle is returned to a condition of minimal risk[1066].

1080 In this context, the transfer of responsibility for data protection to the owner might become problematic if the owner is a natural person. Natural persons, to the contrary of the vehicle manufacturer or the PTO, are unlikely to be in a position to implement the provisions of the GDPR[1067].

5.3.2.4 Duties for vehicle manufacturers and suppliers

1081 In accordance with § 1g para. 3 StVG, vehicles manufacturers are required to create the technical conditions necessary for storage of data by the owner.

[1065] AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.

[1066] https://www.reuschlaw.de/en/news/autonomous-vehicles-more-legal-certainty-with-regard-to-data-protection/ (last consultation 31 August 2022); see also AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021.

[1067] See ALGORIGHT e.V (HESSEL), Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, Saarbrücken, 30 April 2021, § 2 p. 7.

1082 In particular, they are required to adhere to the principles of privacy-friendly technical design, as well as taking appropriate technical and organizational measures for the protection of personal data.

1083 The safety concept provided in § 12 of the Autonomous Vehicle Approval and Operation Ordinance includes performance of a data protection impact assessment.

1084 The new requirements do not apply to suppliers directly, but they will have a strong indirect impact, since vehicle manufacturers will be required to ensure that supplied components meet the requirements of data protection legislation over their entire supply chain. As a general rule, vehicle manufacturers will pass on the requirements applying to them in their contracts with suppliers, since the technical equipment for these vehicles is provided at least in part by module and system suppliers. These companies, typically "Tier 1" suppliers, have the necessary technical expertise due to their proximity to the product and may therefore be contractually required to comply with these duties[1068].

* * *

[1068] https://www.reuschlaw.de/en/news/autonomous-vehicles-more-legal-certainty-with-regard-to-data-protection/ (last consultation 31 August 2022).

6 Overview of the legal framework as regards civil liability

6.1 Purpose of civil liability

1085 From an economical and societal point of view, civil liability rules pursue three functions: the first and most important one is the *ex post* compensation of the victim, as they force the person responsible for a damage to "make good" for the loss suffered by the victim. Secondly, they also ensure *ex ante* deterrence, as they make it economically inefficient for the agent to realize the harmful conduct, and thus incentives positive behaviours. Thirdly, and to a more limited extent, they may also function as *ex post* punishment in the sense that they ensure that the infringer does not get away with the illicit behaviour. This is particularly true in case of "disgorgement" or punitive damages, which aims to strip the infringer from the gains made through the harmful conduct or to punish particularly reprehensible conducts. However, there is a very limited availability of this types of damages under European law, where civil remedies are mostly directed to ensure compensation and react to the infringement in an effective, dissuasive and proportional way[1069].

1086 Liability rules have to strike a balance between protecting citizens from harm (of utmost importance for automated vehicles) while enabling businesses to innovate[1070].

6.2 Different types of regulation

1087 Liability can be regulated according to different mechanisms, which can summarily be categorized from less to more favourable to victims. We will briefly present them in this section.

1088 The current section focuses solely on the main concepts and principles with necessary simplifications, with the purpose of helping to understand the main points of discussion of the recommendations. It does not intend to provide an exhaustive and nuanced legal presentation of European tort law.

6.2.1 Contractual and non-contractual liability

1089 Damages can be recovered based on two broad categories of obligations: contractual and non-contractual (or extra-contractual) obligations.

[1069] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.5 p. 60.

[1070] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, p. 11.

1090 A contract concluded amongst parties can therefore stipulate the distribution of specific obligations, risks and damages. Accordingly, contractual liability and recovery of damages are based on the terms of contract and applicable jurisdictional provisions[1071]. Contractual liability will not be studied further in details this deliverable.

1091 Not all obligations and risks are necessarily covered by a contract. Therefore, a person can also be responsible for damages caused to a third party by actions that are not covered by any contractual provisions agreed between the parties[1072]. In the case of automated vehicles, this might be the case when an automated vehicle creates a damage to other road users, such as other vehicles, VRU's etc. where a contractual link binding the parties to the accident is missing.

1092 Non-contractual (or extra-contractual) liability can be divided into two categories:

- fault-based liability, with various regimes, and
- non fault-based (or strict) liability.

1093 As the definition suggests, fault-based liability requires the establishment of a party's fault, of a damage, and a causal link between the fault and the damage. Strict liability, however, does not require any specific fault and to recover the damage the affected party/victim often has just to establish the fact of damage caused by a breach of an obligation[1073].

6.2.2 Fault-based liability without presumption

1094 The fault-based liability regime is a general and standard framework for recovery of damages in all European Member States[1074]. Under such a regime, the claimant/plaintiff needs to prove three cumulative conditions to obtain compensation for a loss:

- Fault: Fault results from someone failing to act as could be expected from a reasonable person (the "wrongdoer" or "tortfeasor"). Fault consists of either a violation of the law or something that is against the normal cautiousness that can be expected. The diligence required is higher for professionals[1075].

- Damage/loss: To obtain compensation for damages/loss, the claimant/plaintiff must prove that the culpable conduct (fault) by the defendant (the "wrongdoer") resulted in the damage and, in

[1071] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4.1.1 p. 11.

[1072] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4.1.1 p. 11.

[1073] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4.1.1 p. 11.

[1074] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 4.1.2 p. 12 and its *caveat*; BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, §2.1 (a) p. 15.

[1075] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, §2.1 (a) p. 15.

some legal systems, that the legally protected interests of the claimant/plaintiff were violated. The damage/loss may cover material and immaterial damages[1076].

Damage/loss in case of road incidents with conventional road vehicles may be of various nature and cover:

(i) material damages such as the destruction or alteration of vehicle(s), public infrastructure or products within the vehicle(s) or on the road;
(ii) personal or bodily injuries on the driver, passengers, pedestrians etc. (which are also material damage) and
(iii) immaterial damages such as moral harm (psychological impacts, loss of time, profit and money etc.) [1077].

With automated vehicles, accidents will have similar consequences, except for moral harms which might be more various and encompass, for example, losses of data, privacy breaches, security breaches, data breaches etc.[1078].

- Causal link (causality): For a causal link to be established between the fault and the damage/loss, it often suffices that one element contributed to the damage/loss. In the case of complementary products or services, it suffices that one contributed to the damages to be responsible for the entire damage/loss[1079].

  With conventional vehicles, causality is quite straightforward and direct. A fault or negligence will have an impact, which will lead to an accident[1080]. For instance, if a vehicle crosses a junction at red light (i.e. fault/negligence of the driver) and crashes into another vehicle driving lawfully on the junction.

  With automated vehicles, the causality will be more difficult to establish, as the event itself giving rise to the damage/loss might be more complex and could imply virtual stakeholders such as software integrated into the automated driving system, Artificial Intelligence etc.[1081]. In addition, different parties (and with potentially conflicting interests) may be involved, such as the vehicle manufacturer, the manufacturer of the sensors, the software designer, the connectivity provider etc. Another hurdle is that even if the victim gets access to the relevant data (which is not fully guaranteed today, see Appendix A § 3.2.5 above), automated driving systems and functionalities

[1076] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, §2.1 (a) p. 15.
[1077] Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D4.10, Legal perspectives on the use of IoT for AD, 23 December 2019, Version 1.0, § 4.2.1.1 p. 33.
[1078] Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D4.10, Legal perspectives on the use of IoT for AD, 23 December 2019, Version 1.0, § 4.2.1.1 p. 33.
[1079] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, §2.1 (a) p. 15.
[1080] Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D4.10, Legal perspectives on the use of IoT for AD, 23 December 2019, Version 1.0, § 4.2.1.3 p. 34.
[1081] Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D4.10, Legal perspectives on the use of IoT for AD, 23 December 2019, Version 1.0, § 4.2.1.3 p. 34.

(that will involve AI/machine learning in the future) may operate as "black-boxes" that do not allow cognitive access and to understand how they generated a particular output, or what input factors or a combination of input factors have contributed to the decision-making process or outcome[1082].

1095 As the proof of each of those conditions may be difficult to establish for the affected party (e.g. the claimant, plaintiff or victim), some other – more victim-friendly – liability regimes have been enacted in Member States, for specific situations where the legislator (or the case-law) has estimated that the affected party needs to be better protected[1083].

6.2.3 Fault-based liability with presumptions

1096 A first victim-friendly regime consists in keeping the standard fault-based regime seen above, but by changing the standard of proof or some conditions. A rebuttable presumption[1084] for the fault requirement and/or for the causality can facilitate affected parties in obtaining compensation and/or can help reduce information asymmetry between the affected party and the "wrongdoer"[1085].

1097 A presumption regime may be linked to a diverse set of factual situations, generating different types of risks and damages, such as (amongst others):

- the responsibility of a person carrying out a dangerous activity (unless he/she proves that all appropriate measures to avoid the damage have been taken);
- the responsibility of the employer/the principal for the actions executed on his behalf or interest by his employees/agents (unless he proves that he used appropriate care in the selection and the management of the agent/employee)[1086].

6.2.4 Strict liability

1098 A second more victim-friendly regime consists of facilitating the burden of proof for the affected party by changing the conditions which needs to be proven to obtain compensation for a loss. Under a strict liability regime, the affected party needs to prove:

- the default or the risks taken by the "wrongdoer", which is easier to prove than the fault – or the negligence – of the "wrongdoer";

- the damage/loss, which types are often limited (in their nature) or capped (in their amount);

[1082] See Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020, § 2.3 p. 49 and quoted references.

[1083] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, §2.1 (a) p. 15.

[1084] In civil law, a rebuttable presumption is an assumption made by a court that is taken to be true, unless someone (often the other party) proves otherwise.

[1085] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (b) p. 15.

[1086] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, , § 2.1 (b) p. 15 and quoted reference.

- the causality link between the default/risks taken and the damage/loss, although in reality, the need to prove the causality link may represent an important obstacle for the affected party[1087] (as explained above, see Recommendation § 7.2).

1099 Such special standards are justified for different reasons. One of them is that the risk of damages/losses is linked to the exercise of dangerous activities. Some jurisdictions attribute liability to the person that carries out the activity (e.g. the operator of an aircraft or the driver of a car) or are ultimately responsible for the dangerous activity to happen (e.g. the owner of a vehicle). The rationale typically is that this person has created a risk, which has materialised in the occurrence of a damage/loss and that this person also derives an economic benefit from this dangerous activity at the same time[1088].

1100 Some forms of strict liability may go even a step further by linking liability simply to the materialisation of the risk and/or making the discharge of liability either impossible or possible only under the proof that the damaging event was caused by an exceptional/unforeseen circumstance that could not be avoided. These stricter regimes establish presumptions of a causality link between the default/risks taken and the damages/losses, in order to facilitate the compensation of the affected party in situations where the legislator considers it either too burdensome or unbalanced to require the affected party to prove such causality link[1089].

1101 As the strict liability regime tilts the balance in favour of the affected party at the expense of the responsible person(s), it is in general accompanied with limiting principles, especially regarding the type (nature) of damages which can be compensated or the maximum amount of damages which can be granted[1090], as mentioned above.

1102 Thus, relying on a strict liability regime (when it exists), the affected party may be compensated more easily than under the fault-based liability regime, but in a more limited manner. If the affected party seeks compensation for more damages than the ones covered by strict liability, the affected party needs to also launch a complementary action against the person responsible under fault-based liability. It is also interesting to note that strict liability regimes may also be coupled with mandatory insurance requirements[1091], as it is the case for motor vehicles in Europe (see Appendix A § 6.3.2.3 below).

6.2.5 Joint and several liabilities

1103 Where more than one party is liable for compensation of the same damage, tortfeasors are in general jointly and severally liable. Redress claims between tortfeasors are usually possible for identified shares

[1087] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (c) p. 16 and the quoted reference.

[1088] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (c) p. 16 and quoted reference.

[1089] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (c) p. 16.

[1090] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (c) p. 16.

[1091] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (c) p. 16.

of the victim of damages, in situations where the legislator considers it too burdensome or unbalanced to require the affected party to prove such causality link. Generally, groups will re-allocate the costs of liability by contractual agreement. Supply agreements amongst the manufacturers, i.e. end-producers and component suppliers, routinely include clauses that allocate the costs caused by defective components[1092].

6.3 Overview of the legal framework

6.3.1 International law

1104 In international law, there are no uniform liability rules. However, there are harmonised technical[1093] and road traffic rules[1094], which could influence liability, especially in determining eventual negligence of the driver and the vehicle manufacturer[1095].

1105 Automotive liability frameworks vary state by state. The automobile liability frameworks of each country depend on their contexts in road traffic under – generally speaking – the civil law and related special laws[1096].

1106 At UNECE level, although WP.1 has been discussing driving tasks that could lead to a consideration of driver liability and system liability in the context of automated vehicles, some states participating in WP.1 have stressed the importance of not working on liability issues in WP.1[1097].

6.3.2 European law

1107 Regulation of liability in the European Union is a mix of national rules and national procedures as well as EU-level legislation[1098]. Only the strict liability of producers for defective products is harmonised at Union level by the Product Liability Directive (see Appendix A § 6.3.2.1 below), while other liability regimes – apart from some exceptions in specific sectors or under special legislation – are regulated by the Member States themselves at national level[1099].

[1092] BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021, § 2.1 (d) p. 16 and the quoted reference.

[1093] Such as the UN Regulations for instance.

[1094] Such as material provisions of the Geneva and Vienna conventions for instance.

[1095] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 114 and the quoted references.

[1096] World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019, p. 10 and quoted reference.

[1097] World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019, p. 10 and quoted reference.

[1098] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3 p. 7.

[1099] European Commission (Expert Group on Liability and New Technologies - New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, p. 3.

1108 In relation to motor vehicles, there is currently no framework in place harmonising the rules on liability for damages caused by accidents in which motor vehicles are involved – the regulation of liability of the owner of a vehicle or of the driver differ between the Member States[1100].

1109 A specific directive relating to "insurance against civil liability in respect of the use of motor vehicles"[1101] establishes a European third-party liability insurance, and covers obligations and procedure for claims resolution for victims of road traffic accidents[1102] (see Appendix A § 6.3.2.3 below).

6.3.2.1 European Product Liability Directive

6.3.2.1.1 Overview

1110 The Product Liability Directive[1103] ("**PLD**") was adopted in 1985. It provides a layer of protection that national fault-based liability alone does not provide and introduces a system of strict liability of the producer for damage caused by a defect in their products.

1111 The PLD serves two overall functions:

- balancing the need not to hinder socially economic activities and technological progress, with that of granting a fair allocation of the risks and costs arising thereof, through rules that ensure safe products and adequate compensation; and
- harmonising national rules on product liability, to ensure high level of consumer protection and fair competition amongst businesses across Member States, thus contributing to the establishment of the internal market[1104].

1112 The PLD contains generic rules, which also apply to automated vehicles. The PLD's provisions on liability of the producer are of mandatory nature and cannot be derogated by contractual clauses[1105].

6.3.2.1.2 Product

1113 Pursuant to Art. 2 PLD, a product means "all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable […]. Product includes electricity".

[1100] European Parliamentary Research Service (EPRS), Automated vehicles in the European Union, PE 573.902, January 2016, p. 10.

[1101] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.

[1102] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, footnote 20 p. 7.

[1103] Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, in brief "Product Liability Directive".

[1104] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.3 p. 51.

[1105] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, § B p. 118 and the quoted references.

1114 Automated vehicles as such are tangible movables and are undoubtedly "products" in the sense of Art. 2 PLD. However, the situation regarding software used in AV is less certain[1106], as we will see below.

6.3.2.1.3 Defective product

1115 According to the PLD-established system of liability, it is not the fault of the producer but a defect of the product that is decisive for triggering the liability of a producer[1107].

1116 Pursuant to Art. 6 PLD, a product is defective when "it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including:

- the presentation of the product (litt. a);
- the use to which it could reasonably be expected that the product would be put (litt. b);
- the time when the product was put into circulation (litt. c).

According to Art. 6 para. 2 PLD, a product shall not be considered defective for the sole reason that a better product is subsequently put into circulation.

6.3.2.1.4 Categories of defects

1117 The legal literature has classified the possible defects into three categories. If a single item deviates from the intended design, and thus does not conform to the batch of the other mass-produced products, the defect affecting the product constitute a "manufacturing defect". If information and warnings concerning the potential dangers deriving from the use of the devise are not adequately communicated, we face an "information defect". Finally, if it's the very design of the product that does not guarantee the required level of safety or is unreasonably dangerous, the product will be deemed affected by a "design defect"[1108].

1118 Despite not having explicit legal relevance, the aforementioned distinction offers a useful conceptual tool to analyse the concrete functioning of the product liability regime, as well as to assess its effectiveness, because the position of the claimant in a product liability case varies considerably depending on the type of defect involved (e.g. as far as the evidentiary burden is concerned) and so does the capacity of the producer to escape liability (for instance, the "state of art defence" only applies for a "design defect")[1109].

1119 According to the PLD, producers or the subject identified by Art. 3 PLD (the importer of a product within the European Union and the seller of the product, whenever the producer cannot be identified), are held liable to compensate for the damages caused from the use of the product, provided that product is

[1106] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, § B p. 120 and the quoted references.

[1107] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.1.1 p. 7.

[1108] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.3 p. 52.

[1109] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.3 p. 52.

defective and there is a causal nexus between the defect and the damage which compensation is sought for (Art. 4 PLD)[1110].

1120 As mentioned above, to succeed in the claim, the victim (plaintiff/claimant) is required to prove the three constitutive elements of its cause of action: i.e. the damage, the defect and the causal nexus. Since she does not need to prove that the producer was at fault, the producer is held objectively liable[1111].

6.3.2.1.5 Exemptions

1121 However, Art. 7 PLD provides producers and manufacturers with exemptions to the general presumption of liability for a defective product. Thus, the producer shall not be liable if he proves:

- that he did not put the product into circulation (litt. a);
- that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards (litt. b);
- that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business (litt. c);
- that the defect is due to compliance of the product with mandatory regulations issued by the public authorities (litt. d);
- that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered (litt. e);
- in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product (litt. f).

1122 It should be noted that while the PLD provides a liability framework, as related to the definition of a product, defect and derogations, national rules on civil liability still apply, for example, to the determination of causality or non-material damages[1112]. Due to the fact that the PLD rests on national procedural rules, this creates evidentiary-burden issues[1113] and difference between Member States.

1123 In case multiple persons are responsible for the same damage, they are held jointly and severally liable under European law, while national provisions may apply for internal distribution of the damage, on the

[1110] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.3 p. 52.

[1111] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.3 p. 52.

[1112] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.1.1 p. 8.

[1113] See European Commission (Expert Group on Liability and New Technologies - New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, https://data.europa.eu/doi/10.2838/25362 and European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.4.4 p. 59.

basis of contribution or recourse actions (Art. 5 PLD)[1114]. As mentioned above, joint liability might play an important role for automated vehicles, as they might involve numerous and new stakeholders with potential opposing interests.

6.3.2.1.6 Limitations in the context of digitalisation

1124 In the context of digitalization, academic and policy debates have increased, amongst others on following topics.

Concept	Issue	Description
Product (Art. 2 PLD)	Scope of the definition	Should the PLD cover all tangible and non-tangible items (including software)? The current formulation is not clear and divergent opinions exist as to the definition of software (is it a product or a service?)
Defect (Art. 6 PLD)	Notion of the defect as central element of liability determination	The current formulation of a defect in the PLD is closely related to the concept of safety. It is not clear what would be the safety expectations, for example, in relation to cybersecurity and artificial intelligence. The concepts of defect and safety, as well as notions of reasonable and expected use, might need thorough revision if software is to be included explicitly within the scope of the PLD
Existence of a damage and burden of proof	Type of damages covered	The type of damages covered is not harmonised. The scope of pure economic loss and non-material damage are highly contested. It might be excessively difficult and prohibitively costly for a consumer to prove a defect exists, especially for complex technological applications. Therefore, the burden of proof concept might need to be addressed to ensure balanced distribution of a burden between the parties.
Producer (Art. 3 PLD)	Scope of liable persons	Who should be a liable person for the purposes of the PLD? What should be the role of the different economic operators in the value chain? Specific producer? Software designer? To what extent should a producer be liable, for example, for third party software or

[1114] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 3.3 p. 53.

		applications installed in the product? Should joint liability of all actors involved be applied?
Exemptions and defences	Time limitation and exemptions that limit liability of the producer	10-year rules for the expiry of claims might be problematic. Moreover the so-called "development risk defence" might need to be clarified.

Table 1: Actual points of discussion relating to the application of the PLD (Tatjana EVAS)[1115]

1125 In a nutshell, the main limitations of the PLD in relation to the emergence of new technologies are the following.

6.3.2.1.6.1 Product and producer

1126 The scope of the PLD, and specifically the definition of a product under Art. 2 PDL and a producer under Art. 3 PLD: there is legally unsettled and divergent national interpretation of whether software is a product and thus covered by the PLD or not. Given complex value and production chains, the concept of producer within the PLD also needs clarification. Should only the final producer be liable, or should all the actors involved in the production and distribution chain share joint responsibility[1116]? This is of particular importance for automated vehicles.

6.3.2.1.6.2 Defect

1127 The concepts of defect (Art. 6 PLD), damage and burden of proof: the application of the PLD suggests that the determination of what is a defect is already a challenging task. In the PLD, determination of defect is linked to the level of safety that consumers are entitled to expect. With artificial intelligence it would become increasingly difficult for consumers and courts to establish the expected level of safety[1117].

6.3.2.1.6.3 Damage

1128 The relationship between cybersecurity and the concept of a defect are not clearly defined. Pure economic loss and damage to personal data or privacy is not explicitly covered by the PLD. Some Member States, such as France for example, allow for the recovery of both economic damages and pure economic loss, while other Member States do not. Pure economic loss and damage to personal data or privacy are likely to play a more important role in liability cases related to artificial intelligence in the future[1118].

6.3.2.1.6.4 Development risk defence

1129 Besides, the PLD provides for a number or exceptions in which producers can limit their liability. One of the exceptions available is the so-called "development risk defence" (Art. 7 litt. e PLD). Under this provision, the producer may argue that at the time when they put the product into circulation the state of scientific and technical knowledge was not such as to enable the discovery of a defect. Given the

[1115] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.1.1 p. 8 and quoted references.

[1116] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.2 p. 9.

[1117] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.2 p. 9.

[1118] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.2 p. 9.

technologically complex nature of artificial intelligence, this clause may be used increasingly to limit producer liability under the PLD[1119], which has been critized[1120].

6.3.2.1.7 Upcoming amendment of the PLD

1130 Due to its technologically neutral nature, the PLD has not required revision for more than three decades, being applied by courts to a wide range of products over the years, many of which did not exist when the directive entered into force in 1985. Nevertheless, in the face of the increasing challenges brought about by digital transformation and the development of the digital economy, there have been increasing calls to revise the PLD to respond to new challenges brought by technologies and data driven services[1121].

1131 In October 2021, the European Commission launched a public consultation on adapting liability rules to the digital age and artificial intelligence. 189 respondents provided their feedback with regard to:

- confirming the relevance of issues identified in the course of evaluating the PLD in 2018 (in particular, in relation to its application to products in the digital and circular economy), as well as gathering views on how to improve the PLD; and
- collecting information on the need and possible ways to address the specific challenges of AI in terms of the PLD and national liability rules[1122].

1132 The outcomes of the public consultation and the European Commission adoption are planned for the third quarter of 2022[1123].

6.3.2.2 General Product Safety Directive

1133 The regulations on product safety will be briefly presented here as they may also play a role in the potential liability of vehicle manufacturers. These rules lay down safety requirements, combined with technical standards and procedures, which aim at ensuring the safety of the consumer products sold in the European Union. Although these rules do not regulate directly product liability, they are often seen as rules protecting consumer interests and may create actionable rights against manufacturers, according to national tort rules on breach of statutory duty[1124].

[1119] European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020, § 3.2 p. 9.

[1120] See amongst others European Commission (Expert Group on Liability and New Technologies – New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, N 14 p. 6.

[1121] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 73.

[1122] https://www.nortonrosefulbright.com/en-de/knowledge/publications/dfbc5dc8/european-commission-considers-new-civil-liability-rules (last consultation 31 August 2022).

[1123] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en (last consultation 31 August 2022).

[1124] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 133 and the quoted references.

1134 The type-approval of a vehicle does not release the vehicle manufacturer from its liability, because the type-approval regulations are the minimum technical requirements and higher safety standard are usually expected in particular cases[1125].

6.3.2.2.1 Overview

1135 The General Product Safety Directive[1126] ("**GPSD**") ensures that only safe consumer products[1127] (i.e. that do not present any risk or only the minimum risks under normal conditions of use taking into account, inter alia, its characteristics and effects of the product on other products) are placed on the market by manufacturers (Art. 1 para. 1 GPSD).

1136 The GPSD sets a broad-based legislative framework with the objective of covering a sector-specific *lacunae* (gaps) and complementing the provisions of existing or forthcoming legislation related to product safety. It establishes a general obligation upon manufacturers (i.e. producers) to ensure that products, which do not fall within the scope of complementing sector specific legislation, are manufactured in compliance with the general state-of-the-art safety requirements provided therein. It hence works as a *lex generalis* in relation to more specific regimes under European sectorial safety laws, which work as *lex specialis*[1128].

1137 The GPSD set obligations for both the producers and distributors:

- Producers shall only place products on the market which are safe, inform consumers of any risks associated with these products, ensure any dangerous product presented on the market can be traced, and eventually removed to avoid any risks to consumers.
- Distributors shall act with due care to help ensuring compliance with the applicable safety requirements, participate in the monitoring of the safety of the products, and cooperate with producers and the competent authorities[1129].

1138 Under the GPSD, a product is safe when under normal or reasonably foreseeable conditions of use, including duration and, where applicable, putting into service, installation and maintenance requirements, it does not present any risks or only the minimum risks compatible with the product use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account particular aspects such as:

(a) the characteristics of the product;

[1125] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 134 and the quoted case law.

[1126] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

[1127] According to Art. 2 litt. a GPSD, "product" shall mean any product – including in the context of providing a service – which is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and is supplied or made available, whether for consideration or not, in the course of a commercial activity, and whether new, used or reconditioned.

[1128] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 24.

[1129] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 24.

(b) the effect on other products;
(c) the presentation of the product;
(d) the categories of consumers at risk when using the product[1130].

1139 The concept of defectiveness under the GPSD is therefore the lack of the safety which a person is entitled to expect, thus including the expectation that the products placed on the market do not present risks for the physical safety and health of persons (Art. 3 para. 2 GPSD). It is argued that the concept of "safety" on which the GPSD is based appears to be narrow, and risks failing to protect consumers from the risk of security breaches commonly associated with connected devices[1131].

1140 The relevance of GPSD for data and software applications has been discussed in legal literature. The GPSD applies to products that are supplied or made available to consumers (and thus not to professional users and businesses) in the framework of service provision for use by them[1132].

1141 Pure information and digital data as such fall outside the scope of the directive. However, material items that use and integrate those data seem affected by the application of the GPSD[1133].

6.3.2.2.2 Upcoming Regulation on Product Safety

1142 According to the European Commission, the GPSD has become outdated and needs to be revised to keep ensuring the safety net for European consumers[1134]. Therefore, it has adopted a Proposal for a Regulation on Product Safety[1135] in June 2021[1136].

1143 Amongst others, this revision focuses on:

- the safety of products linked to new technologies as well as on the challenges posed by the growth of online sales;
- ensuring a better enforcement of the rules and more efficient and even market surveillance;

[1130] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 24.

[1131] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 24.

[1132] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 24 and the quoted references.

[1133] PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, p. 24.

[1134] https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en (last consultation 31 August 2022).

[1135] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council.

[1136] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0346&qid=1628522210573 (last consultation 31 August 2022).

- improving the recall of dangerous products in the hands of consumers[1137].

6.3.2.3 Motor Vehicle Insurance Directive

6.3.2.3.1 Overview

1144 The Motor vehicles Insurance Directive[1138] ("**MID**") requires that all vehicles registered in the European Union hold mandatory third-party liability insurance to cover civil liability in respect of the use of motor vehicles.

1145 The MID has a dual objective:

- to ensure the free movement of vehicles normally based on European territory and of persons travelling in those vehicles;
- to guarantee that the victims of accidents caused by those vehicles receive comparable treatment irrespective of where in the European Union the accident occurred[1139].

1146 It is a minimum harmonisation Directive, which means that Member States may lay down measures more protective for victims than these provided for by the MID. It should be underlined that the MID does not seek to harmonise national laws on traffic liability, as Member States remain free to determine conditions and type of such liability (strict or fault-based)[1140].

1147 The MID defines vehicles as "any motor vehicle intended for travel on land and propelled by mechanical power, but not running on rails" (Art. 1 para. 1 MID). Automated vehicles are included in this definition.

1148 The MID also ensures that third party insurance covers physical damages (including to passengers of the vehicle[1141]) and damages to property. However, it does not harmonise liability regimes across Member States[1142].

1149 Art. 9 MID establishes mandatory minimum amounts for physical damages (i.e. EUR 1 million per victim or EUR 5 million per claim) and damages to property (i.e. EUR 1 million per claim). The MID establishes a

---

[1137] https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en (last consultation 31 August 2022).

[1138] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.

[1139] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 135 and the case law reference.

[1140] CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 135 and the quoted references.

[1141] The passenger can also be the owner of the vehicle, see CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 137 and the case law reference at footnote 239.

[1142] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 65.

mechanism to simplify and accelerate the settlement of claims and compensation for victims of vehicle accidents[1143].

1150 Additionally, the MID obliges Member States to set up victims' compensation funds for accidents caused by unidentified or uninsured vehicles, as well as for accident caused by a third-country vehicle (Art. 7 to art. 11 MID)[1144].

6.3.2.3.2 Mandatory insurance

1151 In accordance with the MID, the use of the vehicle must be insured[1145] and the insurer is always in practice the first point of claim for compensation for personal injury or material damage (see Art. 18 MID). According to these rules, the obligatory insurance compensates the victim and protects the insured person who is liable under national civil law rules to pay financial damages for the accident involving the motor vehicle[1146].

1152 Producers are not subject to mandatory insurance under the PLD. Automated vehicles are not treated in Union legislation any differently from non-autonomous vehicles as regards motor insurance[1147]. Such vehicles, like all vehicles, must be covered by the third party motor liability insurance, which is the easiest way for the injured party to get compensation[1148].

1153 Taking out proper insurance can mitigate the negative consequences of accidents by providing for a smooth compensation for the victim. Clear liability rules help insurance companies to calculate their risks and to claim reimbursement from the party ultimately liable for the damage. For example, if an accident is caused by a defect, the vehicle insurer can claim reimbursement from the manufacturer after compensating the victim[1149].

6.3.2.3.3 Recent assessment and amendments

1154 In the European Commission's report of 2018[1150], the Motor vehicle Insurance Directive was found to be appropriate to deal with automated vehicles without any amendments. Notably, this directive provides

[1143] European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Annex to Cost of non-Europe report, PE 645.212, January 2021, § 4.1.3 p. 65.

[1144] European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020, § 5.5.2 p. 108.

[1145] In most Member States strict liability is applied for the person in whose name the motor vehicle is registered.

[1146] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, p. 12.

[1147] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, p. 13; see also see CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020, p. 139.

[1148] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, p. 13.

[1149] European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020, p. 13.

[1150] European Commission, On the road to automated mobility: An EU strategy for mobility of the future, COM(2018) 283 final, 17 May 2018, p. 10-11 and quoted references.

for the establishment of guarantee funds which pay for losses not covered by liability insurance. In return for contributing to this fund, vehicle manufacturers, programmers, owners and drivers could see their liability being limited to a certain amount[1151].

1155 The MID was slightly updated end of 2021 by closing loopholes, with amongst others rules ensuring that victims of road accidents are compensated even if the insurance company goes bankrupt[1152].

* * *

[1151] Singapore Academy of Law (SAL) — Law Reform Committee, Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars, Impact of Robotics and Artificial Intelligence on the Law series, September 2020, § 3.2 p. 21 and quoted reference.

[1152] https://www.europarl.europa.eu/news/en/press-room/20211014IPR14929/parliament-adopts-new-rules-to-improve-protection-of-road-accident-victims (last consultation 31 August 2022).

Bibliography

AdaptIVe, Deliverable D2.3, Legal aspects on automated driving, 19 June 2017, Version 1.0.

ADPA (Automotive Data Publisher Association)/AIRC (Association Internationale des Réparateurs en Carrosserie)/CECRA (European Council for Motor Trades and Repairs)/EEGA (European Garage Equipment Association)/ETRMA (European Tyre and Rubber Manufacturers' Association)/FIA REGION I/FIGIEFA (International Federation of Automotive Distributors)/LEASEUROPE (European Federation of Leasing Company Associations), Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach, An in-vehicle, interoperable, secure and standardised telematics platform, Version 1.0, February 2021.

ALGORIGHT e.V (HESSEL), Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, https://algoright.de/2021/05/01/algoright-e-v-als-sachverstaendige-im-ausschuss-fuer-verkehr-und-digitale-infrastruktur-des-deutschen-bundestages/, Saarbrücken, 30 April 2021.

ANDRAŠKO/HAMUL'ÁK/MESARCÍK/KERIKMÄE/KAJANDER, Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union, https://doi.org/10.3390/su131910610, 24 September 2021.

ANZINI, The Artificial Intelligence Act Proposal and its implications for Member States, EIPA Briefing 2021/5, September 2021.

Arcade, Proceedings of workshop on data sharing, Contribution to D2.4, D2.4 Joint CCAM Networking Report, 29 March 2021, Version 1.0, § 2.3 p. 8.

ARRILLAGA/SANCHEZ BARRUECO (et al.), Contribution to the Public Consultation on the evaluation of the European Disability Strategy 2010-20, Performance Review of the implementation of Regulation 181/2011/EU, 13 November 2019, Deusto Law School.

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (WP 136) 01248/07/EN, Adopted on 20 June 2007.

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) 00264/10/EN, Adopted on 16 February 2010.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN, Adopted on 2 April 2013.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216) 0829/14/EN, Adopted on 10 April 2014.

Article 29 Data Protection Working Party, Opinion 08/2014 on Recent Developments on the Internet of Things (WP223) 14/EN, Adopted on 16 September 2014.

Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) (WP 252) 17/EN, Adopted on 4 October 2017.

Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D4.10, Legal perspectives on the use of IoT for AD, 23 December 2019, Version 1.0.

Autopilot Horizon 2020 (AUTOmated driving Progressed by Internet Of Things), Deliverable D5.4, IoT Policy Framework for autonomous vehicles applications, 26 December 2018, Version 1.0.

AXHAMN, Look out – Self-driving vehicles are around the corner!, in P. Wahlgren (Ed.), 50 years of law and IT: the Swedish Law and Informatics Research Institute: 1968-2018, Scandinavian Studies in Law; Vol. 65, Stockholm 2018.

AYAD/SCHUSTER/GOEPFERICH (Hogan Lovells), Germany takes a pioneering role with a new law on autonomous driving, 2 August 2021, https://www.engage.hoganlovells.com/knowledgeservices/dispatchContent.action?key=BcJlhLtdCv6%2FJTDZxvL23WDhlUt68lf8zGAckwosUSmlWlttVf7c5dw%2Fc9jGWruxmzF4%2Fk20N54puXrcRMYtC7pskrooXVOA&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&uid=yYIAhBWIrWo%3D.

BACH, Autonomes Fahren und gesetzliche Grundlagen, Universität Koblenz-Landau, Institut für Informatik, 21 July 2016.

BALBONI/BOTSI/FRANCIS/TABORDA BARATA, Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility, Paper presented at Workshop on Artificial Intelligence, Ethics and Law, Athens, Greece, 3 September 2020, http://ceur-ws.org/Vol-2844/ethics8.pdf.

BENYAHYA/KECHAGIA/COLLEN/NIJDAM, The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis, Applied Sciences, 2022, Vo. 12, No 9, p. 4413, 27 April 2022.

Be Open, European forum and oBsErvatory for OPEN science in transport, D 4.1 Open Science in transport research: legal issues and fundamental principles, 31 August 2020.

BERTOLINI/RICCABONI, Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules, European Journal of Law and Economics (2021) 51:243–284, https://doi.org/10.1007/s10657-020-09671-5, 20 November 2020.

BEWERSDORF, Zulassung und Haftung bei Fahrerassistenzsystemen im Strassenverkehr, Diss. Göttingen, Berlin 2005 (= Schriften zum Technikrecht, Heft 8).

BEWERSDORF, Zur Vereinbarkeit von nicht-übersteuerbaren Fahrerassistenzsystemen mit dem Wiener Übereinkommen über den Strassenverkehr vom 8. November 1968, in: NZV 6/2003.

Bitkom, Stellungnahme Gesetz zum autonomen Fahren & Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung, 1 February 2021.

BJELFVENSTAM, The path to automated driving – market introduction (SOU 2018:16), Report presented to the Swedish Minister for Infrastructure on 7 March 2018, Summary in English, https://www.government.se/497e60/contentassets/31cf2d8c8df1465da086e2390028d1cb/summary-sou2018-16.pdf

BRUCK/SOTEROPOULOS, Automatisiertes und vernetztes Fahren: Berücksichtigung des lokalen, räumlichen Kontextes und räumliche Differenzierung, Mitteregger et al. (Hrsg.), AVENUE21: Politische und planerische Aspekte der automatisierten Mobilität, pp. 7-16, https://doi.org/10.1007/978-3-662-63354-0_9

BU-PASHA, Legal aspects, public interest, and legitimate interest in processing personal data to operate autonomous buses in the regular transportation system, Security and Privacy, 2022;e247, May 2022, https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.247.

BUITEN/DE STREEL/PEITZ, Centre on regulation in Europe (CERRE), EU Liability rules for the age of artificial intelligence, Report, March 2021.

Bundesministerium für Verkehr und digitale Infrastruktur (Germany), *Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, Bearbeitungsstand 8. Februar 2021*.

Bundesministerium für Verkehr und digitale Infrastruktur (Germany), *Entwurf einer Verordnung zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Bearbeitungsstand 10. Juni 2021.*

Bundesministerium Verkehr, Innovation und Technologie (Austria), *Automatisiertes Fahren auf Straßen mit öffentlichem Verkehr – Rechtliche Rahmenbedingungen im Vergleich*, Marleen Roubik, August 2018.

CAMPMAS/IACOB/SIMONELLI/VU (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility, Annex III Potential market deficiencies and regulatory barriers, including a common industry-led position in the automotive sector, EASME/COSME/2018/004, 20 April 2021.

CCAM Strategic Research and Innovation Agenda, European leadership in safe and sustainable road transport through automation, Version 1.3, 1 December 2021.

CHATZIPANAGIOTIS/LELOUDAS, Automated Vehicles and Third-Party Liability: A European Perspective, SSRN Electronic Journal 2020(1):109-199, DOI:10.2139/ssrn.3519381, January 2020.

Congressional Research Service, U.S. and EU Motor Vehicle Standards: Issues for Transatlantic Trade Negotiations, CRS Report, 18 February 2014.

Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Rapporteur Mr. Ziya ALTUNYALDIZ, Legal aspects of "autonomous" vehicles, Doc. 15143, 22 September 2020.

CROZET/SANTOS/COLDEFY (CERRE), La régulation de la mobilité urbaine à l'épreuve de la mobilité partagée et du "MaaS", Rapport, Septembre 2019.

Data Protection Commission (Ireland), Guidance Note: Guidance on Anonymisation and Pseudonymisation, June 2019, https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf.

Data Protection Commission (Ireland), Quick guide to the principles of data protection, October 2019, https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf.

DEBUSSCHE/CÉSAR/DE MOORTEL (Bird & Bird), Leveraging Big Data for Managing Transport Operations (LeMO), Horizon 2020 770038, Deliverable D2.2 Report on Legal Issues, October 2018.

EBERS, Civil Liability for Autonomous Vehicles in Germany, available at SSRN: https://ssrn.com/abstract=4027594 or http://dx.doi.org/10.2139/ssrn.4027594, 5 February 2022.

EBERS, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022.

EMAM/ALVAREZ, A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques, International Data Privacy Law, Volume 5, Issue 1, https://doi.org/10.1093/idpl/ipu033, January 2014, p. 73-87.

Ernst & Young Abogados SLP and FIA Region I, Expert study on: "GDPR application in the context of car connectivity", Final Report, November 2021.

ERTICO – ITS Europe (editor), Mobility as a Service (MaaS) and Sustainable Urban Mobility Planning, September 2019.

Ethik-Kommission (eingesetzt durch den Bundesminister für Verkehr und digitale Infrastruktur), Automatisiertes und Vernetztes Fahren – Bericht, June 2017.

European Automobile Manufacturer Association (ACEA), ACEA Position Paper, Access to Vehicle Data for Third-Party Services, December 2016, https://www.acea.auto/files/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf

European Commission (BREEMERSCH et al.), Best practices guide on the carriage of persons with reduced mobility, Guide on future measures, policies and strategies aimed at creating a PRM-inclusive transport system in Europe, Final report for: European Commission, DG Mobility and Transport, 26 November 2018.

European Commission (Expert Group on Liability and New Technologies – New Technology Formation), Liability for artificial intelligence and other emerging digital technologies, Publications Office, 27 November 2019, https://data.europa.eu/doi/10.2838/25362.

European Commission (DG GROW I2), Call for evidence for an Impact Assessment, Access to vehicle data, functions and resources, Ares(2022)2302201, 29 March 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en.

European Commission, Commission staff working document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final, Brussels, 10 January 2017.

European Commission, Guidelines on the exemption procedure for the EU approval of automated vehicles, Version 4.1 supported by the Technical Committee on Motor Vehicles of 12 February 2019.

European Commission, Mapping and performance check of the supply of accessible tourism services: final report, Publications Office, 2015, https://data.europa.eu/doi/10.2873/584417.

European Commission, On the road to automated mobility: An EU strategy for mobility of the future, COM(2018) 283 final, 17 May 2018.

European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, Brussels, 19 February 2020.

European Commission, Strategy for the rights of persons with disabilities 2021-2030, COM(2021) 101 final, March 2021, https://data.europa.eu/doi/10.2767/31633.

European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020.

European Commission, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, Commission Staff Working Document, SWD(2020) 331 final, 9 December 2020.

Council of Europe, European Committee on Crime Problems (CDPC), Feasibility Study on a future Council of Europe instrument on Artificial Intelligence and Criminal Law, Document prepared by the Working Group on AI and Criminal Law with Dr. Sabine Gless as General Rapporteur, and in co-operation with the CDPC Secretariat, CDPC(2020)3Rev, Strasbourg, 4 September 2020.

European Commission, White paper on Artificial Intelligence – A European approach to excellence and trust, Brussels 19 February 2020, COM(2020) 65 final.

European Data Protection Board (EDPB), Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, Adopted on 9 March 2021.

European Data Protection Board (EDPB), Statement 05/2021 on the Data Governance Act in light of the legislative developments, Adopted on 19 May 2021.

European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), Joint Opinion 3/2021 on the proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), Version 1.1, 9 June 2021.

European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021.

European Disability Forum (EDF), EDF recommendations on the revision of the TSI-PRM 2019, Brussels, October 2019.

European Parliament, Artificial intelligence and civil liability – Legal affairs, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 621.926, July 2020.

European Parliament, IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 732.266, May 2022.

European Parliamentary Research Service (EPRS), Artificial intelligence in road transport, Cost of non-Europe report, PE 645.212, January 2021.

European Parliamentary Research Service (EPRS), Automated vehicles in the European Union, PE 573.902, January 2016.

European Parliamentary Research Service (EPRS), Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?, Scientific Foresight Unit (STOA) PE 634.445, July 2019.

European Parliamentary Research Service (EPRS), Civil liability regime for artificial intelligence – European added value assessment, PE 654.178, September 2020.

European Parliamentary Research Service (EPRS), The NIS2 Directive – A high common level of cybersecurity in the EU, PE 689.333, June 2022.

FABULOS Horizon 2020, Pre-Commercial Procurement of Future Automated Bus Urban Level Operations Systems, Policy paper, Deliverable 5.6 – Future application and impact of project results and learnings, 30 March 2021.

Federal Roads Office (Switzerland), Automated driving – fact sheet for conducting pilot tests in Switzerland, Version 3.0, 26 January 2021.

Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, SVI 2017/044, 1691, October 2020.

Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 3: Handling Data, SVI 2017/044, October 2020.

Federal Roads Office (Switzerland) et al., Impacts of automated driving – Insights and measures from the viewpoint of FEDRO, Effects of automated driving, Sub-project 6: Spatial impacts, SVI 2017/044, 1680, August 2020.

Federal Roads Office (Switzerland) et al., Transport of the future 2060: New types of service – organization and diffusion, SVI 2017/006, October 2020.

Federal Roads Office (Switzerland) et al., Transport of the future 2060: Synthesis Report, SVI 2016/002, 1685, September 2020.

FERNÁNDEZ LLORCA/GÓMEZ, Trustworthy Autonomous Vehicles, JRC Science for policy report, EUR 30942 EN, JRC127051, doi:10.2760/120385, Luxembourg 14 December 2021.

FINCK/BIEGA, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, Technology and Regulation, 2021, p. 44–61 https://doi.org/10.26116/techreg.2021.004.

FINCK/PALLAS, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, Vol. 10, No. 1, p. 11 et seq.

FRAZZANI/TARANIC/JENSEN/ZAMBONI/NOTI/PIANTONI, Remaining challenges for EU-wide integrated ticketing and payment systems, Final Report, published by the European Commission, Directorate-General for Mobility and Transport, July 2019.

Gecko Horizon 2020 (Governance principles and mEthods enabling deCisions maKers to manage and regulate the changing mObility systems), Governance and Regulation models to manage disruptive mobility services, Project brief, October 2021.

GLESS/WOHLERS, Strafrechtliche Verantwortlichkeit für "smarte" Produkte, Schweizerische Zeitschrift für Strafrecht, Stämpfli Verlag AG, ZStrR 137/2019 S. 366, pp. 366-399.

GILL, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 16 May 2022, available at SSRN: https://ssrn.com/abstract=4115443.

GYSIN (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation – UVEK), Datenschutz Mobilitätsdaten, Bericht, ASTRA-D-DB3D3401/359, 30 November 2020.

HACKER, AI Regulation in Europe, 7 May 2020, available at SSRN: https://ssrn.com/abstract=3556532 or http://dx.doi.org/10.2139/ssrn.3556532.

HANSSON, Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway, Research in Transportation Economics, Volume 83, November 2020.

HATZOPOULOS/MARIQUE, Centre on regulation in Europe (CERRE), Transport on demand – How to regulate ride-hailing in the EU?, Report, December 2021.

Hogan Lovells, Hogan Lovells White Paper – The Road to Autonomous Vehicles, October 2021.

Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability and responsibility, Luxembourg, June 2020.

HUET/AMSLER/MARSANDE (UITP Europe), The EU's data strategy and its impact on public transport, Version 6, 17 March 2022.

HUONDER/RAEMY, Autonomes Fahren, Rechtlicher Anpassungsbedarf: ein Werkstattbericht, 4. Zürcher Tagung, Dike Verlag AG, Strassenverkehr 1/2016, pp. 46-55.

IACOB/CAMPMAS/SIMONELLI (Centre for European Policy Studies – CEPS), Big Data and B2B platforms: the next big opportunity for Europe – Annex IV Recommendations to the EU and national policy makers and an action plan for the creation of shared EU-wide in-vehicle data platforms, EASME/COSME/2018/004, 20 April 2021.

ILKOVÁ/ILKA, Legal Aspects of Autonomous Vehicles – an Overview, Proceedings of the 2017 21st International Conference on Process Control, Štrbské Pleso, Slovakia, 6 – 9 June 2017, pp. 428-433. http://publications.lib.chalmers.se/publication/249781

International Association of Public Transport (UITP), Policy Brief, Autonomous vehicles: a potential game changer for urban mobility, Brussels, January 2017.

International Association of Public Transport (UITP), GECKO, Project Brief, Governance and regulation models to manage disruptive mobility services, Brussels, October 2021.

ISO/TC 204 Intelligent transport systems, Project: ISO/SAE Approved Working Item PAS 22736/SAE J3016, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (November 2020).

KEMPEN, Fahrerassistenz und Wiener Weltabkommen, SVT 2008, 3. Sachverständigentag, 25. und 26. Februar 2008.

KERBER/GILL, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10 (2019) JIPITEC 244 para 1.

LAGRANGE, The importance of UNECE Regulations for the EU legislation on Automated driving, Future Networked Car Symposium, Session 1: Regulatory advances in highly automated driving, 22 March 2021.

Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Consultation Paper 3 - A regulatory framework for automated vehicles – A joint consultation paper, 18 December 2020.

Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of responses to consultation Paper 3 and next steps, 2 July 2021.

Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: joint report, HC 1068 SG/2022/15, 26 January 2022.

Law Commission of England and Wales and the Scottish Law Commission, Automated Vehicles: Summary of joint report, HC 1068 SG/2022/15, 26 January 2022.

LOHMANN, Automatisierte Fahrzeuge im Lichte des Schweizer Zulassungs- und Haftungsrechts, Diss., Nomos 2016.

LOHMANN, Ein zukunftsfähiger Haftungsrahmen für Künstliche Intelligenz, in: HAVE 2021 S. 111, Schulthess Juristische Medien AG, p. 111 et seq.

LOHMANN, Erste Barriere für selbstfahrende Fahrzeuge überwunden – Entwicklungen im Zulassungsrecht, in: *sui-generis* 2015, pp. 135 et seq.

LOHMANN, Mobilität von morgen – Die Zulässigkeit automatisierter Fahrzeuge im Ländervergleich, Aktuelle Juristische Praxis / Pratique Juridique Actuelle 5/2021, p. 617 et seq.

MARTENS/MUELLER-LANGER, Access to Digital Car Data and Competition in Aftermarket Maintenance Services, Journal of Competition Law and Economics, ISSN 1744-6414, 16 (1), 2020, JRC119621, p. 116-141.

MARTIN/BRUCK/SOTEROPOULOS, Transformations of European Public Spaces with AVs, Mitteregger et al. (Hrsg.), AVENUE21. Politische und planerische Aspekte der automatisierten Mobilität, pp. 159-178 https://doi.org/10.1007/978-3-662-63354-0_9

Ministère de la transition écologique et solidaire (France), Ministère chargé des transports, Développement des véhicules autonomes, Orientations stratégiques pour l'action publique, Un an d'actions publiques, Mai 2018 – Avril 2019.

Ministry of Transport and Communications (Finland), Conclusions from the 4th high-level meeting on connected and automated driving, Helsinki, 7 October 2020.

MONTI/DE STREEL, Centre on regulation in Europe (CERRE), Improving EU institutional design to better supervise digital platforms, Report, January 2022.

MULDER/VELLINGA, Exploring data protection challenges of automated driving, Computer Law & Security review, Volume 40, April 2021.

Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Autonomes Fahren als Baustein einer inter- und multimodalen Mobilität, Siebter Zwischenbericht, December 2021.

Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 3, Digitalisierung für den Mobilitätssektor, Plattformbasierte intermodale Mobilität und Handlungsempfehlungen zu Daten und Sicherheit, Dritter Zwischenbericht, Juli 2020.

Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppen 3 und 6, Daten und Vernetzung – Standards und Normen für eine intermodale Mobilität, Juli 2021.

Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, Mai 2020.

Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, Standards und Normen für die Mobilität der Zukunft, Ergebnisse der Arbeitsgruppe 6 der NPM 2018–2021, Abschlussbericht 10/2021, October 2021.

Nationale Plattform Zukunft der Mobilität (NPM), Arbeitsgruppe 6, White Paper, Handlungsempfehlungen zur Typgenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, Mai 2020.

Nationale Plattform Zukunft der Mobilität (NPM), Ergebnisbericht der Nationalen Plattform Zukunft der Mobilität – Ergebnisse aus drei Jahren NPM (2018-2021), October 2021.

Opinion of the European Economic and Social Committee on "A European highway code and vehicle register", 2005/C 157/04, 28 June 2005.

PERARNAUD/FANNI (Centre for European Policy Studies – CEPS), The EU Data Act: towards a new European data revolution?, CEPS Policy Insights No 2022-05, March 2022.

PIANTONI/FIENGO/LOVASTE et al. (Grimaldi studio legale), Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study, dated 31 May 2021, published by FIA Region I on 11 June 2021, https://www.fiaregion1.com/wp-content/uploads/2021/06/FIA-Final-Report-ISPs-Liabilities-20210531.pdf.

PICHEREAU, Le déploiement européen du véhicule autonome — Pour un renforcement des projets européens, Assemblée nationale, 30 July 2021.

POP/ADOMAVICIUS, Sandboxes for Responsible Artificial Intelligence, EIPA Briefing 2021/6, September 2021.

PROBST, Das "selbstfahrende" Auto: entfernte Illusion oder nahe Realität?, Strassenverkehr 1/2021, Dike Verlag AG, 2021, pp. 52-58.

PUNEV, Autonomous Vehicles: The Need for a Separate European Legal Framework, European View 2020, Vol. 19(I) 95-102, https://doi.org/10.1177/1781685820912043, 2020.

Rödl & Partner, Innovationspapier zur automatisierten und fahrerlosen Personenbeförderung, erstellt im Auftrag des Verband Deutscher Verkehrsunternehmen e.V., Hamburg/Nürnberg, März 2021.

SALIOU (LINC — Laboratoire d'innovation numérique de la CNIL), The European model: point of convergence, source of divergence?, 27 October 2021, https://linc.cnil.fr/fr/european-model-point-convergence-source-divergence (last consultation 3 November 2021).

SCHRÖDER, Datenschutz beim Kameraeinsatz im Automobil, Zeitschrift für Datenschutz, ZD Heft 6/2021, C.H. Beck, p. 302 et seq.

Singapore Academy of Law (SAL) — Law Reform Committee, Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars, Impact of Robotics and Artificial Intelligence on the Law series, September 2020.

Sohjoa Baltic, The Legal Framework, The Roadmap to Automated Electric Shuttles in Public Transport, IKEM — Institut für Klimaschutz, Energie und Mobilität e.V., May 2020.

SPINDLER/SCHMECHEL, Personal Data and Encryption in the European General Data Protection Regulation, (2016) 7 JIPITEC 163.

STEEGE, Datenverarbeitung beim autonomen Fahren – Schafft die StVG-Novelle 2021 Rechtssicherheit bei der Datenverarbeitung?, Cologne Technology Review & Law, CTRL 2/22.

Support Centre for Data Sharing (SCDS), Analytical report on EU law applicable to sharing of non-personal data, Support Centre for data sharing, DG CONNECT, SMART 2018/1009 V2.0, 24 January 2020.

TSAPI et al. (Haskoningdhv Nederland BV for FIA Region I), How to maximize the road safety benefits of ADAS?, BH3649-RHD-ZZ-XX-RP-Z-0001, 14 December 2020.

THOUVENIN/TAMÒ-LARRIEUX, Data Ownership and Data Access Rights – Meaningful Tools for Promoting the European Digital Single Market?, Big Data and Global Trade Law, Cambridge University Press, July 2021, p. 316 et seq. https://doi.org/10.1017/9781108919234.020

VAN ASBROECK/DEBUSSCHE/CÉSAR (Bird&Bird), Big Data & Issues & Opportunities: Data Ownership, 25 March 2019 https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-data-ownership

Valdani Vicari & Associati (VVA) Economics & Policy, Study on market access and competition issues related to MaaS, June 2019.

VALLET, Commission Nationale de l'Informatique et des Libertés (CNIL), The GDPR and Its Application in Connected Vehicles – Compliance and Good Practices, January 2019.

VELLINGA, Automated driving and its challenges to international traffic law: which way to go?; *Law, Innovation and Technology, 11(2)*, 2019, p. 257 et seq. https://doi.org/10.1080/17579961.2019.1665798

VELLINGA, Connected and vulnerable: cybersecurity in vehicles, International Review of Law, Computers & Technology, https://doi.org/10.1080/13600869.2022.2060472, April 2022.

VELLINGA, Legal aspects of Automated driving, On drivers, producers and public authorities, University of Groningen, https://doi.org/10.33612/diss.112916838, Groningen, 2020.

Verband Deutscher Verkehrsunternehmen e. V., Eckpunkte zum Rechtsrahmen für einen vollautomatisierten und fahrerlosen Level 4 Betrieb im öffentlichen Verkehr, Positionspapier, September 2020.

Verband der Automobilindustrie, Stellungnahme Referentenentwürfe des Bundesministeriums für Verkehr und digitale Infrastruktur über ein Gesetz zur Änderung straßenverkehrsrechtlicher Vorschriften – Gesetz zum autonomen Fahren, Berlin, Februar 2021.

Verbraucherzentrale Bundesverband e.V. (Germany), Fahrerlose Mobilität, aber sicher und nutzerfreundlich, Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zum Entwurf eines Gesetzes sowie einer Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome Fahrzeug-Genehmigungs- und Betriebsverordnung – AFGBV), 1 February 2021.

Verbraucherzentrale Bundesverband e.V. (Germany), Vertrauen stärken durch verbraucherfreundliche Daten-Governance, Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance, 12 January 2021.

VON BODUNGEN, Wie sicher ist sicher genug? Manipulationsfreiheit und Verfügbarkeit der Daten als Zulassungsvoraussetzungen?, Zulassungsrechtliche Herausforderungen des Autonomen Fahrens, Universität Basel, Tagung vom 10. Oktober 2019.

WESTERMARK/GAETA/CURRAN/POLANCO LAZO, Legal opinion on the Regulation of certain aspects of Automated Driving, Current to: 01.03.2022, E-Avis ISDC 2022.

WIDMER, Wie sicher ist sicher genug? Sicht Datenschutz- und Cybersicherheit, Zulassungsrechtliche Herausforderungen des Autonomen Fahrens, Universität Basel, Tagung vom 10. Oktober 2019.

World Economic Forum, Filling legislative gaps in automated vehicles, White paper, April 2019.

* * *