

Policy paper

# Responsible Innovation in Self-Driving Vehicles

Published 19 August 2022

## Contents

[Introduction](#)

[Glossary](#)

[Regulatory lifecycle](#)

[Context](#)

[Summary of recommendations](#)

- [1. Road safety](#)
- [2. Data privacy](#)
- [3. Fairness](#)
- [4. Explainability](#)
- [5. Data sharing](#)
- [6. Public trust](#)
- [7. Governance](#)

[Next steps](#)

[Annex A: Safe and Ethical Operational Concept and Safety Management Systems](#)

[Annex B: List of recommendations](#)

List of Abbreviations

Acknowledgments



© Crown copyright 2022

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gov.uk](mailto:psi@nationalarchives.gov.uk).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/publications/responsible-innovation-in-self-driving-vehicles/responsible-innovation-in-self-driving-vehicles>

# Introduction

Self-driving vehicles have the potential to radically transform the UK's roads. They offer the opportunity to deliver significant improvements to road safety and efficiency by reducing driver error, can improve accessibility by enhancing mobility for people unable to drive, and have the potential to reduce emissions. There is also a significant economic opportunity: the automotive and digital sectors are already important contributors to the UK economy and self-driving vehicles could grow this considerably. Recent [research](https://www.gov.uk/government/publications/connected-and-automated-vehicles-market-forecast-2020) (<https://www.gov.uk/government/publications/connected-and-automated-vehicles-market-forecast-2020>) commissioned by the Department for Transport has shown that by 2035, the UK connected and automated vehicles market could be worth £41.7 billion.

To enable these benefits and achieve the government's ambition to '[make the UK the best place in the world to deploy connected and automated vehicles](https://www.gov.uk/government/news/uk-on-the-cusp-of-a-transport-revolution-as-self-driving-vehicles-set-to-be-worth-nearly-42-billion-by-2035)' (<https://www.gov.uk/government/news/uk-on-the-cusp-of-a-transport-revolution-as-self-driving-vehicles-set-to-be-worth-nearly-42-billion-by-2035>) manufacturers need clarity about the regulatory landscape they are operating in. The general public also needs to have confidence in the safety, fairness and trustworthiness of these vehicles.

To provide this clarity and confidence, the legal and regulatory frameworks that govern conventional vehicles and their drivers will need to be updated. Under our current legal and regulatory systems, we licence drivers as competent to drive and then hold them accountable for their actions. In the context of vehicles that are self-driving, we will need new mechanisms to ensure that the systems these vehicles use, and the organisations that develop and deploy them, are similarly held accountable for performing in a safe and ethical manner.

With the right design, regulation and governance can actively promote innovation. As the UK Government's 'Plan for Digital Regulation' [puts this](https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation) (<https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation>), 'well-designed regulation can have a powerful effect on driving growth and shaping a thriving digital economy and society, whereas poorly-designed or restrictive regulation can dampen innovation...the right rules can help people trust the products and services they're using, which in turn can drive take-up and further consumption, investment and innovation'.

Building on the [recent proposals](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf) (<https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf>) set out by the Law Commissions, this report provides a comprehensive view of how these proposals can be supported by a responsible and trustworthy regulatory and assurance framework. This report takes a broad view of the factors that are crucial to deliver public trust: safety, data privacy, and fairness. We also look at the areas that will be important enablers to

responsible innovation: facilitating sufficient explainability to ensure accountability, data sharing, promoting public trust, and effective governance.

The flexible, pro-innovation approach taken in this report furthers the government's approach to the regulation of AI and its intent to establish [‘the most trusted and pro-innovation system for AI governance in the world’](https://www.gov.uk/government/publications/national-ai-strategy) (<https://www.gov.uk/government/publications/national-ai-strategy>). It also supports the CDEI's programme of work on AI Assurance, which seeks to achieve [‘effective, pro-innovation governance of AI’](https://www.gov.uk/government/publications/the-roadmap-to-an-effective-ai-assurance-ecosystem) (<https://www.gov.uk/government/publications/the-roadmap-to-an-effective-ai-assurance-ecosystem>).

These recommendations aim to ensure a fair, trustworthy and proportionate approach to the regulation and governance of self-driving vehicles to build public trust and confidence in their use, which in turn will drive adoption and innovation. They have been shaped by the expert contributions of Professor John McDermid and Professor Jack Stilgoe and through engagement with key stakeholders, including the Centre for Connected and Autonomous Vehicles (CCAV), the Law Commission of England and Wales and the Scottish Law Commission, the Information Commissioner's Office, members of the Centre for Data Ethics and Innovation Advisory Board, Home Office, the Office of the Biometrics and Surveillance Camera Commissioner, the Driver and Vehicle Standards Agency, and the Vehicle Certification Agency.

This work will support the Department for Transport in delivering ‘Connected & Automated Mobility 2025: realising the benefits of self-driving vehicles’, a roadmap which commits to developing a new legislative framework that builds trust in self-driving vehicles while enabling innovation. In particular, this report will inform the design of the new safety framework for self-driving vehicles, proposing detailed recommendations on what features and capabilities a new safety framework for self-driving vehicles will need to possess, and how to manage interdependencies between different parts of the regulatory ecosystem. Following consultation, the Department for Transport expects to publish further guidance on what constitutes a sufficient safety case by Authorised Self-Driving Entity (ASDE) and No-User-in-Charge (NUiC) Operators, which will be shaped by the recommendations of this report. More broadly, this report will guide the Department for Transport in developing secondary legislation that will set out the details of the requirements and processes of the new legislative framework. This secondary legislation is due to be consulted on in 2023, marking the next stage of an ongoing public dialogue about how self-driving vehicles should be governed.

## Glossary

**Authorisation authority:** A new role recommended by the Law Commissions. ‘It will be the government agency responsible for the second stage

(authorisation) of AV safety assurance in Great Britain. When authorising the vehicle, the authorisation authority will assess each of the vehicle's ADS features and specify those which are 'self-driving'. The authorisation authority will also assess whether the entity putting the vehicle forward for authorisation has the reputation and financial standing required to be an ASDE'. [\[footnote 1\]](#)

**Authorised Self-Driving Entity (ASDE):** A new legal actor proposed by the Law Commissions. 'It is the entity that puts an AV forward for authorisation as having self-driving features. It may be the vehicle manufacturer, or a software designer, or a joint venture between the two'. [\[footnote 2\]](#)

**Automated Vehicle (AV):** 'A general term used to describe vehicles which can drive themselves without being controlled or monitored by an individual for at least part of a journey'.

**Data minimisation:** Under the data minimisation principle of UK GDPR, [Personal data shall be] 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. [\[footnote 4\]](#)

**Data protection by default:** As [defined by the ICO \(https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dspd3\)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dspd3), 'data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation'.

**Data protection by design:** As [defined by the ICO \(https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dspd3\)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dspd3), 'data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle'.

**Dynamic driving task:** A term used by the Law Commissions to describe 'the real-time operational and tactical functions required to operate a vehicle in on-road traffic. It includes steering, accelerating and braking together with object and event detection and response'. [\[footnote 5\]](#)

**Explainability:** This term [refers to \(https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making\)](https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making) 'the ability to understand and summarise the inner workings of a model, including the factors that have gone into the model'.

**Lidar:** An acronym that stands for 'light detecting and ranging'. Lidar is a remote sensing method for determining ranges.

**NUiC Operator:** A new legal actor proposed by the Law Commissions. As [explained \(https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf\)](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf) by

the Law Commissions: ‘Some features will be authorised for use without a user-in-charge. We refer to these as “No User-In-Charge” (NUiC) features. We recommend that when a NUiC feature is engaged on a road or other public place, the vehicle is overseen by a licensed NUiC Operator’.

**Operational Design Domain (ODD):** As defined by the Law Commissions, the ODD is ‘(...) the domain within which an automated driving system can drive itself. It may be limited by geography, time, type of road, weather or by some other criteria’.[\[footnote 6\]](#)

**Personal data:** As set out in UK GDPR, ‘personal data’ refers to ‘any information relating to an identified or identifiable natural person (...)’.[\[footnote 7\]](#)

**Safety by design:** Guiding the design with information derived from hazard and safety analysis both to achieve safety more cost-effectively and to make it easier to assure safety.

**User-in-charge (UiC):** As defined by the Law Commissions, the UiC is, ‘An individual who is in the vehicle and in position to operate the driving controls while a self-driving ADS feature is engaged. The user-in-charge is not responsible for the dynamic driving but must be qualified and fit to drive. They might be required to take over following a transition demand. They would also have obligations relating to non-dynamic driving task requirements including duties to maintain and insure the vehicle, secure loads carried by the vehicle and report accidents. An automated vehicle would require a user-in-charge unless it is authorised to operate without one’.[\[footnote 8\]](#)

**Vulnerable road users:** Road users requiring extra care. As set out in the Highway Code, this includes pedestrians, particularly children, older or disabled people, cyclists, motorcyclists and horse riders.[\[footnote 9\]](#)

## Regulatory lifecycle

The table below describes the key responsibilities of different actors across the regulatory lifecycle of a self-driving vehicle under our recommendations, from trials to the ongoing response and change needed to ensure vehicles remain safe. It is supplemented by a regulatory lifecycle flowchart in an annex to this report, that more fully describes the interdependencies between different parts of the regulatory lifecycle, and situates our recommendations within them.

Phases	Trials and pre-authorisation	Authorisation	Operator Licensing (where NUiC)
<hr/>			

Key assurance question	How do we develop the evidence that a vehicle is safe enough to drive itself?	Should the vehicle be permitted to drive itself?	Where the vehicle needs no driver in the vehicle, is there a responsible operator behind it?
Policy and advice	<p><b>DfT (advised by CAVES)</b> issues guidance to (prospective) ASDEs, interpreting primary legislation, UNECE regulations, and technical standards, equality and data protection/surveillance issues</p>	<p><b>DfT and regulatory agencies (advised by CAVES)</b> interpret and apply legislation, regulations and DfT policy, including:</p> <ul style="list-style-type: none"> <li>* Road rules</li> <li>* Equality impacts</li> <li>* Privacy/surveillance impacts</li> <li>* Human-machine interfaces for drivers (handover) and other road users (labelling)</li> </ul>	<p><b>DfT and regulatory agencies (advised by CAVES)</b> interpret and apply legislation, regulations and D policy, including:</p> <ul style="list-style-type: none"> <li>* Road rules</li> <li>* Equality impacts</li> <li>* Privacy/surveillance impacts</li> <li>* Human-machine interfaces for drivers (handover) and other road users (labelling)</li> </ul>
Regulator(s)	<p><b>Authorisation body</b> reviews Vehicle Safety Case Reports (VSCRs)s, audits safety management system, and relevant type approval certificates</p> <p><b>Authorisation body and ASDE</b> agree basis for authorisation, based on the type approval granted, agreed VSCR, ODD</p>	<p><b>Authorisation body</b> assesses suitability for self driving, including consistency with road rules, collision risks, equality impacts, privacy/data protection and driver interfaces and labelling</p> <p><b>Authorisation body</b> issues authorisation of AV as capable of driving itself</p>	<p>(where NUiC) <b>Licensing body (or delegate)</b> test the deployment domain, in particular the suitability of remote operation</p> <p><b>Licensing body</b> issues licence to operate a NUiC service</p>
ASDE	<b>(Prospective) ASDE</b> trials potential self-	<b>ASDE</b> publishes authorisation	



driving system with safety driver and labelling in place, in line with a Safety Management System

**ASDE** develops and submits Vehicle Safety Case Reports and Safety Management System for Authorisation, on the basis of the agreed ODD

notice, and summary of authorised safety case report

**ASDE** shares more detailed safety information with prospective NUiC Operator(s)

---

NUiC Operator

(where NUiC) **(Prospective) NUiC Operator** develops Deployment Safety Case Report on the basis of a Vehicle Safety Case Report, and Operator Safety Management System

(where NUiC) **NUiC Operator** submits Operational Safety Case Report and Operator Safety Management System for Licensing

(where NUiC) **NUiC Operator** publishes licence operate and make available to any passengers

---

## Context

The Centre for Data Ethics and Innovation (CDEI) was commissioned by the Centre for Connected and Autonomous Vehicles (CCAV) to provide expert advice to inform future regulation and policy on self-driving vehicles. We use the acronym 'AV' to refer to self-driving vehicles as this is the commonly-used shorthand.

## **Methodology**

The recommendations have been developed by CDEI in consultation with subject matter experts. They have been informed by primary research and interviews with 32 experts from across industry, academia and the public sector. We have designed the recommendations to be as specific and practically focused as possible. For example, we highlight the intended 'implementer' for each recommendation. We have also set out a visual guide to the roles and responsibilities set out by our recommendations that situates them within the current regulatory ecosystem (see separate Annex).

## **Relationship to proposals made by the Law Commissions**

The report's recommendations are intended to be read alongside the regulatory proposals developed by the Law Commission of England and Wales and the Scottish Law Commission (the Commissions), as part of their joint review of the legal framework for AVs in Great Britain. These recommendations have been designed to complement (and avoid duplicating) the Law Commissions' proposals. Our hope is that the recommendations below clearly bound the ethical problem for regulating AVs. We recognise that some requirements have already been set out by other projects, such as the need for AVs to comply with road rules. Where appropriate, we use the terminology coined by the Commissions, such as 'in-use regulator', without prejudice to how the government finally implements the Commissions' recommendations.

## **Scope**

This report examines the most pressing ethical and governance issues that relate to the regulation of AVs. For this reason, we made the decision not to cover the following issues which, while important, are not within the scope of this work:

- the impact of AVs on regional inequalities and the 'levelling up' agenda

- environmental impacts of AVs and the contribution to Net Zero targets
- wider societal implications of AVs (e.g. relating to land use policy, employment, public transport passenger safety or taxation).

## Summary of recommendations

	Recommendations for policymakers	Recommendations for Authorised Self Driving Entities (ASDEs), NUI Operators, and trialling organisations
<b>Road safety</b>	<p>The authorisation authority, in concert with the in-use regulator, shall develop and publish guidance on Road Rules (RR) in the context of self-driving vehicles.</p> <p>The authorisation authority shall define a scheme for determining what changes to AV performance are significant enough to require re-authorisation prior to ASDEs supplying updates to deployed AVs.</p>	<p>The Operational Design Domain (ODD) should be consistent with the relevant road rules and cover all classes of road users, including vulnerable road users that can reasonably be expected in the ODD.</p> <p>The ASDE should define 'Safe and Ethical Operational Concept' (SEOC) that sets out high-level principles that will govern the design and</p>

<b>Data privacy</b>	<p>The AV regulator(s) should issue guidance for ASDEs and NUiC Operators clarifying how Data Protection <a href="https://www.gov.uk/government/consultations/data-a-new-direction">obligations</a> (<a href="https://www.gov.uk/government/consultations/data-a-new-direction">https://www.gov.uk/government/consultations/data-a-new-direction</a>) apply to AVs, in consultation with the Information Commissioner's Office.</p> <p>The Home Office should issue guidance clarifying how the Investigatory Powers Act 2016 applies to ASDEs and NUiC Operators.</p>	<p>In line with UK GDPR, ASDEs and NUiC Operators should ensure that 'data protection by design and by default' measures are incorporated throughout the AV development process, for example, by anonymising facial image data that is unavoidably captured in video of the AV's surroundings at the point it is collected and before further processing.</p>
<b>Fairness</b>	<p>The in-use regulator, advised by CAVES, should collect data on fairness and safety outcomes in order to allow feedback to operators and collective learning.</p> <p>The authorisation authority and licensing authority should ensure that AV services are non-discriminatory in terms of access (e.g. who can be a passenger, who can access services) as part of authorisation and licensing decisions.</p>	<p>ASDEs should report on the feedback between their training data and their ODC to minimise risk of algorithmic bias as part of the equality impact assessment and safety case reports submitted during the authorisation process.</p>

ASDEs should facilitate independent scrutiny of risk and biases so that distribution of risks can be assessed.

---

**Explainability**    The Committee on AV Ethics and Safety (see below) should review the degree of explainability needed for regulatory oversight.

The ASDE should design the AV so that it is possible to construct an explanation of key decisions made during the Dynamic Driving Task (DDT) for a bounded test scenario, and the lead up to notifiable events.

For collisions, near misses and other notifiable events, the ASDE should design the AV so that it is possible to construct an explanation of the key decisions made by the AV leading up to the event, however caused.

---

**Data sharing**    The disclosure of safety-relevant data should be standardised across ASDEs. The in-use regulator should define a consistent format for

In consultation with the authorisation

safety-relevant data to facilitate sharing between ASDEs, the authorisation authority and a collision investigation unit.

authority, the ASDE shall publish a summary of the SEOC, which will be made publicly and freely available upon authorisation of the vehicle to drive itself.

The ASDE and NUiC Operator should communicate safety-relevant data with other organisations in the AV ecosystem when requested, including other ASDEs, the in-use regulator, the authorisation authority and the collision investigation unit, using agreed data formats, where this contributes to road safety.

---

## Public trust

CCAV should continue to commission public dialogue and social research to seek public views on: Balancing the tensions between achieving a 'safety-first culture' and ensuring sufficient accountability for the consequences of AV behaviour; The distribution of AV risks and benefits; Future changes to infrastructure and rules of the road and any associated costs; Explainability of decisions made by AVs; Labelling of vehicles.

Prospective ASDEs and NUiC Operators should engage with local communities, including local authorities, when an AV trial is planned in a

If trials on public roads become de facto deployments - e.g. by removing a safety driver, substantially increasing numbers of vehicles or starting to transport customers, there should be increased scrutiny and renewed safety assessments.

particular areas [footnote 10\]](#) This engagement should inform testing or deployment (e.g. placing conditions on times, places, public information, maximum speeds etc).

AVs should be clearly labelled. Where vehicle have the capability to drive themselves or be driven conventionally at different times, signals should indicate the status of operation. This external labelling should be in addition to information inside the vehicle that clearly indicate mode of operation.

---

## **Governance**

The authorisation authority and in-use regulator should establish a joint Committee on AV Ethics and Safety (CAVES) to provide contestable advice and recommendations on policy and ethical issues regarding the safety of AVs. CAVES should be composed of experts and lay members with a diverse range

# 1. Road safety

## Introduction

Road safety is a key consideration for AVs. If the technology is not seen as 'safe enough', it is unlikely to be accepted by the public. However, there is no empirically verifiable answer to the question of 'how safe is safe enough?' The hope is that AVs will offer dramatic improvements in overall road safety, but in changing the scale of risk, they will also affect the type and distribution of risks experienced by road users. Average improvements in road safety, even if they can be clearly demonstrated, will not engender public trust if crashes are seen as the fault of faceless technology companies or lax regulation rather than fallible human drivers. Evidence from past studies of risk perception shows that risks that are seen as new, uncontrolled, catastrophic and artificial are consistently amplified in the minds of the public.<sup>[\[footnote 11\]](#)</sup> If AVs are seen by the public as equivalent to trains or aircraft, mobility technologies that users feel are not under their control, the public could expect a 100x improvement in average safety over manually-driven vehicles.<sup>[\[footnote 12\]](#)</sup> Uncertainty about a socially tolerable risk threshold for AVs will remain until the technology is mature and deployed at scale. Our approach is intended to support the safe and ethical introduction of AVs, which will allow this risk threshold to be established over time, based on a carefully managed introduction of the technology.

AVs are road vehicles, and many of the normal regulatory processes for road vehicles will continue to apply, including type approval, which ensures that a vehicle (or component) is compliant with established regulatory standards. A significant part of the existing regulatory framework is to licence drivers as competent to drive, and hold drivers accountable for safe driving. This framework no longer serves its purpose in a situation where vehicles are 'self-driving' where there is no such driver in control of the vehicle, whether there is a 'user-in-charge' who is not required to monitor the situation, or no user-in-charge within the vehicle at all. This means that additions to the current regulatory framework are needed. Specifically, these additions will have to address the transfer of safety responsibility from drivers to vehicle manufacturers and operators. There will also be a need for sufficient regulatory oversight of how these vehicles behave, both during upfront approval, and monitoring while deployed. While this is in part addressed by the recommendations made by the Law Commissions, this report builds on that legal framework by recommending a regulatory approach which assures vehicles, rather than drivers, and provides a level of technical detail that is intended to enable vehicles to be designed, assessed and authorised.



# Safety by design

Rather than attempting to define a level of acceptable risk, our approach is to outline a framework for the assurance of safe AVs as part of an emerging regime of standards, certification and inspection, with the further aim of continual safety improvements over time, to ensure that an acceptable level of risk is achieved before AVs become widespread. A safety assurance regime cannot guarantee safe outcomes in all cases, nor can it provide clear statistics on aggregate risk in advance of testing and deployment, particularly with new and complex technologies.<sup>[footnote 13]</sup> Our focus instead is on encouraging safety by design.

Safety by design involves informing and guiding the design and development of a system with the results of safety analyses, rather than viewing safety assessment as a process carried out at the end of the development process. The benefits are twofold: first, it is much more likely that a safe system will result; second, it will be easier to assure safety, as the safety evidence needed for the safety case will arise naturally out of the development process. This concept is well-established for “conventional” systems and is often encoded in four principles, here presented with respect to software:

1. Software safety requirements shall be defined to address the software contribution to system hazards.
2. The intent of the software safety requirements shall be maintained throughout requirements decomposition.
3. Software safety requirements shall be satisfied.
4. Hazardous behaviour of the software shall be identified and mitigated.

The first three principles relate to managing safety ‘top down’; the fourth is ‘bottom up’, recognising that there will never be complete foresight, and the design process needs to address unanticipated, low-level, failure modes. These four principles are often supplemented with a fifth (referred to as 4+1) that the confidence established in addressing the software safety principles shall be commensurate to the contribution of the software to system risk.

These principles can be seen in assurance processes for machine learning based systems, see for example the [Assurance of Machine Learning for Autonomous Systems \(AMLAS\) framework](https://www.assuringautonomy.com/) (<https://www.assuringautonomy.com/>).

The associated assurance framework is intended to seek sufficient evidence that safety by design principles have been followed and that developers and manufacturers have in place mechanisms to learn from experience, improve designs, and to achieve societally acceptable levels of risk over time. Thus, the safety framework is intended to seek meaningful data on who benefits, who is harmed, how they are harmed and who is responsible rather than just statistics on deaths and injuries per million miles. Recognising that this is a rapidly evolving technology, this framework does not aim to be prescriptive about technological approaches. Rather than examining the safety of AVs in isolation,

the assurance of AV safety is possible only in the context of their deployment domains.

## Elements of a safety framework

There are many important aspects of the proposed safety framework in terms of achieving safety, assuring safety, and in communicating to the public. We briefly outline the key elements of the framework.

### Operational Design Domain (ODD) and deployment domains

It is conventional to specify an ODD for an AV - that is a definition of the types of road layout, road users, including their ethically relevant features, weather conditions and lighting conditions in which an AV is expected to operate. AVs will be assured for operation in a particular ODD noting that, for example, the ODD for a valet-parking capability will be distinct from the ODD for a ‘motorway pilot’. When AVs are deployed, e.g. to provide mobility as a service, a check will be needed that the deployment context, i.e. where, and in what conditions, the vehicles are used, matches the ODD - for example if there are level crossings in the deployment domain, then these need to be present in the ODD for it to be appropriate for the vehicle to be approved for deployment in that domain.

Recommendation	Implementer
<p>1. The ASDE shall define the AV ODD to be consistent with the relevant Road Rules (RR) and to cover all classes of road users including vulnerable road users that can reasonably be expected in the ODD.</p> <p>The ODD definition should include all relevant features defined to an appropriate level of detail. The definition should cover the parameter ranges for fixed scenery elements, attributes of dynamic elements and environmental elements. It should also include all ethically salient features relating to other road users.</p> <p>Further guidance will be needed from DfT to define these ethically salient features.</p>	<p>ASDE, reporting to the Authorisation authority</p>
<p>2. The ASDE shall ensure that the deployment domain is compatible with the ODD prior to operational use of the AV.</p>	<p>ASDE reporting to the In-use regulator</p>

### Road rules

Road rules (RR) are customs or rules governing the behaviour of road users. These include, but are not limited to, relevant aspects of the Highway Code. For example, the custom of ‘flashing lights’ or making a beckoning motion to indicate that an oncoming vehicle can proceed is not enshrined in the Highway Code but is widely (if perhaps inconsistently) practised. Some have argued that the Highway Code or RR should be modified to accommodate AVs or that some RR need not apply to AVs as they will be demonstrably safer. We do not take this view, and believe that AVs should comply with existing RR so that they can integrate effectively with conventional vehicles and to avoid any sudden (and potentially hazardous) changes in behaviour when switching between self-driving and human-driven modes. However, we recognise that RR will evolve over time, and this needs to be done while being mindful of the capabilities and limitations of AVs and of societal attitudes to AVs, including changes in views as such vehicles become more widespread. We therefore recommend that CAVES has a role to advise on RR and see this as consistent with the Law Commissions’ report.

Recommendation	Implementer
<p>3. The authorisation authority, in concert with the in-use regulator, shall develop and publish guidance on RR in the context of self-driving vehicles, with input from the CAVES Road Rules Subcommittee, to inform the development of SEOCs that:</p> <ul style="list-style-type: none"> <li>a) give complete coverage of situations that an AV could reasonably be anticipated to encounter in the ODD;</li> <li>b) reflect rules of behaviour that are ethical and broadly acceptable across different types of AV; and</li> <li>c) identify precedence between the rules.</li> </ul>	<p>Authorisation authority</p>

### Safe and Ethical Operating Concept (SEOC)

It is necessary to understand how the AV will behave safely and ethically. Current road rules are defined based on the presence of a human driver. Several of the Highway Code rules for drivers include phrases such as ‘when it is safe to do so’, and ethical considerations, e.g. with respect to vulnerable road users, are also left to the discretion of the driver. Thus, for AVs, just complying with the RR is not sufficient, and it is necessary to ‘encode’ aspects of safe and ethical behaviour beyond the RR. It is common engineering practice to define a Concept of Operations (CONOPS) for a system and we build on this practice by introducing a Safe and Ethical Operating Concept (SEOC) which sets out constraints that will govern the behaviour of the AV. The SEOC will address, for example, issues of handover to drivers for AVs with a UiC feature on exiting an ODD, and how unavoidable emergency situations will be dealt with, including priority given to vulnerable road users. The SEOC will build on and help interpret the relevant RR, for example providing the context for interpreting

rules, such as for crossing double white lines, that say they may be ‘broken’ when it is safe to do so. The intent is that the SEOC can be communicated to the public and interested stakeholder groups so they can gain an understanding of how the AV is intended to achieve safe and ethical behaviour.

### What is a SEOC?

A Safe and Ethical Operating Concept (SEOC) would be a set of constraints on vehicle behaviour, including motion, signalling to other road users, and actions to preserve their own safety. The SEOC would be defined as a set of Self-Driving Constraints (SDCs) and precedence between these constraints, as they can conflict in certain circumstances.

In [Annex A](#), we have identified some example SDCs, some clear precedence rules, and some situation-dependent precedences so the concept is clear. For ease of understanding, these focus on motion rather than signalling. These are intended to be illustrative and an ASDE’s SEOC would need to be thought through from their perspective on safe and ethical behaviour for the capability of their AV and the intended ODD.

Recommendation	Implementer
<p>4. The ASDE shall define a SEOC, including Self-Driving Constraints (SDCs) (see <a href="#">Annex A</a> for more detail), for inclusion within its SCR submitted as part of authorisation, for the behaviour of the AV in its ODD, that:</p> <ul style="list-style-type: none"><li>a) complies with road rules (RR);</li><li>b) complies with any applicable regulations for automated driving system (ADS);</li><li>c) minimises occurrence of ‘at-fault’ collisions in its defined ODD;</li><li>d) mitigates risk of ‘non-fault’ collisions in its defined ODD;</li><li>e) manages entry to and exit from the ODD, ensuring a transition to safe control of the AV by the UiC where there is one, or a safe transition to a minimal risk condition (MRC) on exiting the deployment domain;</li><li>f) does not unfairly discriminate against road users or otherwise unfairly treat vulnerable road users;</li><li>g) does not require other road users to violate applicable rules or SDCs;</li><li>h) defines the priority of rules and SDCs where they can conflict in particular circumstances;</li><li>i) does not cause individuals in the vicinity of the AV unjustified concern about their safety;<a href="#">[footnote 14]</a></li></ul>	ASDE, reporting to the Authorisation authority

appropriately balances the need to make progress with the need to ensure safety.[\[footnote 15\]](#)

---

5. The ASDE shall demonstrate to the authorisation authority that they have designed the AV to be consistent with the SEOC, and provide supporting arguments and links to evidence in a SCR to gain authorisation for self-driving. The SEOC shall be made publicly available once authorisation is granted.	ASDE, reporting to the Authorisation authority
6. The ASDE shall monitor the operation of the AV to identify situations where it fails to implement the SEOC, inform the in-use regulator of 'notifiable events' and take action to resolve deviations from the SEOC that are not notifiable. Government will need to consider how this interacts with NUiC Operators and what their obligations in relation to the SEOC will be.	ASDE and NUiC Operator, with oversight from the In-use regulator

---

## **Safety Management Systems (SMS), Safety Cases and Safety Case Reports**

Safety Management Systems (SMS), Safety Cases and Safety Case Reports (SCRs) are key tools in ensuring and assuring safety. A Safety Case is a structured argument, supported by evidence, that a system is acceptably safe for a given application, in a specified environment (e.g. an ODD). Safety Cases are very large, so it is common to present the argument and evidence summaries in an SCR, e.g. in support of regulatory approval. Safety Cases and SCRs are well understood and are already part of the automotive industry practice (e.g. as required by ISO 26262). Our usage here is consistent with that standard, except that we would also expect to see ethical issues addressed in the SCR and the SEOC to be both prominent and publicly available. The SMS is a set of processes and procedures on how safety will be managed by an organisation including, but not limited to, how an SCR will be produced for an AV. For an Authorised Self-Driving Entity (ASDE), the SMS will define organisational structures, processes for handling ethical concerns, ways of responding to instructions from regulators and informing owners/users of issues they need to be aware of, and so on. For a No-User-in-Charge (NUiC) Operator the SMS will perform a similar role in setting out how safety is managed in the organisation but will be different in scope as it will need to include operator training and competence, maintenance procedures, emergency response, e.g. recovering a broken-down vehicle and providing a means of completing unfinished journeys, where appropriate. In [Annex A](#), we have outlined what, at a minimum, the contents of the SMS should be, both for ASDEs and NUiC Operators.[\[footnote 16\]](#)

Although there are many more details, the ODD, SEOC, SMS and SCR provide the bases on which the safety assurance framework is built. Although the onus in the framework is on the ASDE and the NUiC Operator, it is intended that the

regulatory authorities will gather and analyse data so it is possible to make judgements that the introduction of AVs provides a significant net reduction in safety risks, over time.

It is important that the Safety Case and SCR are kept ‘in step’ with the evolving system design. However, it would be both onerous and ultimately unproductive to update the SCR for every change, thus guidance is needed on when the SCR needs to be updated and re-submitted to the regulator.

As a rule of thumb, we would expect that the following changes would be considered sufficiently significant to require the production and issuing of a revised SCR:

- Change to priorities between rules in the SEOC which might change the balance of risks between classes of road user
- Extending capability of a particular Automated Driving System (ADS)

The following changes would not be considered sufficiently significant to require the production and issuing of a revised SCR:

- Perfective changes, e.g. change in trajectory generation for path planning that reduces energy use
- Changes to internal labels for object classes used by the perception system, without changing the object classes themselves

The SMS too will evolve, but this will reflect changes in processes, e.g. new training schemes for staff at a NUiC Operator, not changes to the AV itself. Current UNECE regulations typically require review or audit of similar processes, e.g. for managing software updates, every three years. We make no specific recommendations on frequency of audit or update, but suggest that this is an issue which should be kept under review by regulators.

Recommendation	Implementer
7. The ASDE and NUiC Operator shall comply with instructions from the in-use regulator or authorisation authority, e.g. to limit the AV deployment domain or modify the vehicle design, to ensure continued safety of operation. <a href="#">[footnote 17]</a>	ASDE and NUiC Operator
8. ASDEs and NUiC Operator shall keep their SCR up to date and produce it to the authorisation authority when required to gain approval for changes to the vehicle prior to deploying the changes as part of the vehicle’s re-authorisation.	ASDE and NUiC Operator, reporting to the Authorisation authority



9. The ASDE and NUiC Operator shall operate a safety management system (SMS) for the AV governing how they manage safety through the AV lifecycle, and provide periodic independent SMS audit reports to the in-use regulator.	ASDE and NUiC Operator, with oversight from the Authorisation authority and In-use regulator
10. The authorisation authority should assess SMS and safety culture within ASDEs and NUiC Operators as part of the authorisation and licensing decisions respectively, and approve deployments where they meet applicable criteria.	Authorisation authority
11. For authorisation purposes, the authorisation authority shall assess the safety of AV deployments based on:  a) the SCR b) independent SMS audit reports c) notifiable events (cf. LC Rec. 20 - data gathering on safety)  The in-use regulator should assess a), b), and c) on an ongoing basis.	Authorisation authority and In-use regulator
12. The authorisation authority shall define 'notifiable events' in terms of deviation from the ASDE's SEOC. <a href="#">[footnote 18]</a> It will, at a minimum, include traffic infractions as defined by the Law Commissions; an incident that had it been performed by a human driver would have attracted criminal or civil penalties (cf. LC Rec. 20 - data gathering on safety).	Authorisation authority
13. The authorisation authority shall define a scheme for determining what changes to AV performance are significant enough to require re-authorisation prior to ASDEs supplying updates to deployed AVs.	Authorisation authority

## Clarity around responsibility and accountability during handover with the UiC

The AV shall be designed to enable the UiC to take back control of the vehicle in a safe manner, e.g. by being given sufficient time to retain situational awareness, noting that the UiC should respond to the transition demand but that the AV should continue to provide safe operation, should the UiC fail to do so (See Rec. 14). This is important because it will ensure that responsibility and accountability falls in the appropriate place so that, for example, the AV rescinds control to the UiC in a way that they can reasonably take responsibility

and control of the vehicle. This may mean that the AV has to be designed to undertake a Minimum Risk Manoeuvre (MRM) if the UiC doesn't respond to a transition demand.[\[footnote 19\]](#) This is in order to ensure that the vehicle enters a Minimum Risk Condition (MRC) and that appropriate recovery action can be taken. For example, on a motorway, the MRM might involve moving to the leftmost lane and to continue driving at a speed consistent with the surrounding traffic, before entering an Emergency Refuge Area (ERA) and coming to a stop - which is the MRC. It will take significant research and development efforts to ensure there are the human-machine interfaces in place to get these handovers right, and there may be lessons to be learned from other sectors, such as aviation, that have also grappled with handovers between automated systems and human pilots. Ensuring these handovers between the AVs and UiCs work effectively will be crucial for overall safety and trust in AVs as they are deployed more widely.

Recommendation	Implementer
14. The ASDE shall design the AV so that transfers of authority for control of the DDT from the AV to the UiC shall ensure safety, including providing the UiC with sufficient time and information to achieve situational awareness before they engage in the DDT.	ASDE, reporting to the Authorisation authority
The ASDE shall have responsibility and accountability for behaviour of the AV both within and outside the ODD unless it is confirmed that the UiC has authority for control of the DDT. <a href="#">[footnote 20]</a>	

## 2. Data privacy

### Introduction

AVs necessarily collect and process large volumes of data about their surroundings. Many of the privacy and data protection challenges raised by AVs and the services they may enable are therefore similar to other technologies that process large amounts of data about their environments, such as smart speakers, video doorbell cameras and wearable fitness trackers. There are two key characteristics of AVs that suggest particular attention should be paid to the privacy implications of these systems. Firstly, AVs may lead to widespread collection and processing of personal data in order to achieve core functionality such as detecting other road users in situations where explicit consent is not



feasible. Secondly, they require regulatory authorisation for deployment (as discussed in the safety section above) that may be perceived as regulatory endorsement (implicitly or explicitly) about this personal data processing, including how they strike the right balance between what is necessary for safe driving, and sufficient protection of personal data. These challenges merit careful consideration given the potential future scale of AV use in public spaces.

## Personal data of AV occupants

AVs are likely to process several categories of personal data on-board the vehicle, such as time-stamped location data of the vehicle (which carries a high degree of identifiability), 'health and wellbeing' data on the driver (e.g. whether they are awake and alert for the purposes of handing over vehicle control) and personal data collected by non-driving infotainment systems (e.g. choices made on in-vehicle app stores).

In the UK, personal data processing is addressed by Data Protection law, including UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulation (PECR) 2003. Data Protection law requires controllers to have a lawful basis for that processing, which is often consent in the context of goods and services. There are also specific requirements for consent when processing location data<sup>[footnote 21]</sup> under the PECR, where all users (i.e. both UiCs and passengers) must give their [valid consent](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=%E2%80%9Cany%20freely%20given%2C%20specific%2C,relating%20to%20him%20or%20her%E2%80%9D.)) ([https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=%E2%80%9Cany%20freely%20given%2C%20specific%2C,relating%20to%20him%20or%20her%E2%80%9D.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=%E2%80%9Cany%20freely%20given%2C%20specific%2C,relating%20to%20him%20or%20her%E2%80%9D.))) for this processing, unless the data is processed anonymously. It will fall within the duty of the ASDE to provide suitable, clearly worded and easily comprehensible information to owners, UiCs and registered keepers. Where this processing is of sensitive personal data, ASDEs will need to ensure they comply with the requirements of seeking explicit consent. We note that the Law Commissions recommend that the Government establishes a duty on AV data controllers to share relevant data with insurers to provide a legal basis for doing so. Regulators should guard against companies using privacy as an inappropriate reason not to share safety-critical data.

Our interviews with subject matter experts highlighted open questions regarding the intervals for when consent may need to be reviewed - for example, whether the user will need to provide consent every time the vehicle is activated, as there may be new passengers on board who have not previously provided valid consent. This will depend in part on the categories of personal data collected. In particular, there are open questions regarding fleet ownership models using vehicles fitted with a NUiC self-driving feature, and whether the occupants or the NUiC Operator will be responsible for providing consent in these situations.

We recommend that these areas of ambiguity are clarified via joint guidance issued by the ICO and AV regulator(s).

As per Data Protection regulatory requirements, any personal data processed by AVs should not be stored for longer than is strictly necessary. For incident investigation, insurance, and civil enforcement purposes, it will be necessary to store AV location data for a period of time (e.g. for cross-referencing the time and location of reported incidents). However, it would not be acceptable to store such data indefinitely, and future guidance will need to explicitly clarify the retention and deletion schedules required for AV location data. We note that the Law Commissions recommended that location data be stored for 39 months for insurance purposes. We think this is a good guide for parties beyond insurers (e.g. incident investigation and civil enforcement) as similar evidential considerations apply, although they will need to periodically review these to ensure they are appropriate.

## **Personal data of other road users**

AV sensors may also collect personal data from individuals outside the vehicle (for example, of pedestrians and other road users), most notably facial images collected from video feeds. Again, this issue is not unique to AVs, as many conventional vehicles now have dash cams installed that collect the facial images of pedestrians. Although AVs may collect more detailed data from multiple sensors, the legal compliance considerations remain the same, and such collection will likely be necessary for the safe operation of the vehicle, or in the interests of public safety to meet these obligations. If processing this personal data is not necessary, ‘data protection by design and by default’ measures may need to be used (see below). ASDEs will also need to consider how to enable individuals external to the vehicle to assert their data protection rights (in line with ICO guidance)[22].

## **Biometric data**

### **Biometric data**

As defined in UK GDPR, [biometric data](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4) (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4>) is ‘personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person,

which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data’.

Some companies are exploring the use of biometric data of road users outside of the vehicle. One application of this would be to identify the intentions of other road users, for example, by assessing eye contact with the vehicle (‘gaze detection’). If there are instances in which the collection of biometric data could be demonstrated to be necessary for the safe operation of the vehicle, then they may be lawful under the [‘legitimate interests’ basis of UK GDPR](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/) (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>), although this is something of a grey area and would be subject to undertaking a legitimate interests assessment. To provide clarity for companies exploring the use of this technology, the ICO and AV regulator(s) should clearly set out the circumstances (if any) in which the processing of personal data of individuals outside of the vehicle (such as facial images of pedestrians) would be considered lawful and proportionate under Article 6 of UK GDPR. Biometric data is also likely to be special category data and therefore processing will also need to satisfy Article 9 where this is the case.

Recommendation	Implementer
<p>15. The AV regulator(s) should issue guidance for ASDEs and NUiC Operators clarifying how Data Protection obligations<sup><a href="#">[footnote 23]</a></sup> apply to AVs, in consultation with the Information Commissioner’s Office. Issues that could be covered include:</p> <p>a) The requirement to conduct a Data Protection Impact Assessment (DPIA), and to make this document publicly available alongside the vehicle’s safety case report at authorisation<sup><a href="#">[footnote 24]</a></sup>;</p> <p>b) Clarification that an ASDE and/or NUiC Operators should prepare suitable DPIAs and make available for authorisation and licensing decisions;</p> <p>c) A self-assessment checklist to establish whether the ASDE / NUiC Operator is acting as a controller, processor, or joint controller;</p> <p>d) Any requirements to secure valid consent from the UiC or passengers for processing personal data within the vehicle (such as what kinds of data collection would constitute ‘location data’ and ‘cookies or similar’ under PECR) and where additional consent may be required, such as when there are new passengers in the vehicle;</p> <p>e) Proposed retention and deletion schedules for personal data collected by AVs, particularly location data;</p> <p>f) What would be considered necessary and legitimate</p>	<p>ICO; Authorisation authority; In-use regulator</p>

purposes for processing and sharing personal data (e.g. safety improvements, insurance claims etc.);

g) Circumstances under which processing of personal data of other road users outside the vehicle (such as facial images of pedestrians) is likely to be considered lawful and proportionate under Article 6 GDPR (e.g. vital interests, or legitimate interests)<sup>[footnote 25]</sup>;

h) Circumstances under which processing of special category personal data (e.g. biometric data of the UiC) is likely to be considered lawful and proportionate under Article 9 GDPR (e.g. explicit consent, or substantial public interest)<sup>[footnote 26]</sup>;

i) The testing of AI systems for AVs against the requirement ‘to design the AV so that it is possible to construct an explanation of the key decisions made by the AV leading up to the notifiable event, however caused’. See Rec. 29;

j) Which ADS features (if any) could be considered ‘a decision based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or similarly significantly affects [the data subject]’, for the purposes of Article 22 GDPR.

---

## Data protection by design and by default and data minimisation

### Data protection by design

As [defined by the ICO \(https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd3\)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd3), ‘data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle’.

### Data minimisation

Under the [data minimisation principle \(https://www.legislation.gov.uk/eur/2016/679/article/5\)](https://www.legislation.gov.uk/eur/2016/679/article/5) of UK GDPR, [Personal data shall be] ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’.

One way in which AVs could implement a ‘data protection by design and by default’ approach would be to anonymise personal data at the source, where identification is not clearly necessary for any given purpose. In an AV context,

this is likely to be possible because for many of the types of data needed (such as video data), it will not be necessary for individuals to be identifiable. For example, AVs may unavoidably collect facial image data (e.g. via video of their surroundings), which could be considered ‘special category data’ under UK GDPR, but the facial image data itself is not required for safely avoiding obstacles.

Our in-depth consultation with manufacturers and technical experts revealed that it is very likely that all facial image data of other road users could reasonably be anonymised at the point of collection, without any adverse impact on the functioning of the vehicle. This would eliminate the need for the vehicle to process special category data of pedestrians without their consent. For manufacturers that pursue camera-only AV designs (not incorporating Lidar), it is [technically feasible](https://techcrunch.com/2020/10/19/pimloc-gets-1-8m-for-its-ai-based-visual-search-and-redaction-tool/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAND8sOzngN1jk-75fLV_87LaEoT7Dup_aq_A89pB0mMO9IByK6qYyMed_Ql0B4QTiUgHdyx9cvMfa9OwhLuuBsr0XyJhqw0EIVGJCivdbdbtM2XbeNDXx9-nJzgZXq-IKdJAZZIJTp0zpIpOQHBUvHtJvtpEHvZcoBRH0e8zOVFD&guccounter=2) ([https://techcrunch.com/2020/10/19/pimloc-gets-1-8m-for-its-ai-based-visual-search-and-redaction-tool/?guce\\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce\\_referrer\\_sig=AQAAAND8sOzngN1jk-75fLV\\_87LaEoT7Dup\\_aq\\_A89pB0mMO9IByK6qYyMed\\_Ql0B4QTiUgHdyx9cvMfa9OwhLuuBsr0XyJhqw0EIVGJCivdbdbtM2XbeNDXx9-nJzgZXq-IKdJAZZIJTp0zpIpOQHBUvHtJvtpEHvZcoBRH0e8zOVFD&guccounter=2](https://techcrunch.com/2020/10/19/pimloc-gets-1-8m-for-its-ai-based-visual-search-and-redaction-tool/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAND8sOzngN1jk-75fLV_87LaEoT7Dup_aq_A89pB0mMO9IByK6qYyMed_Ql0B4QTiUgHdyx9cvMfa9OwhLuuBsr0XyJhqw0EIVGJCivdbdbtM2XbeNDXx9-nJzgZXq-IKdJAZZIJTp0zpIpOQHBUvHtJvtpEHvZcoBRH0e8zOVFD&guccounter=2)) to detect faces and apply anonymisation techniques to them, to ensure that individuals’ privacy is protected. ASDEs will need to ensure that such techniques fully anonymise faces, otherwise they may be considered ‘pseudonymised’ and therefore still subject to UK GDPR as personal data. This challenge does not arise with Lidar and radar sensor fusion devices as they do not record image data that would include facial images.

Recommendation	Implementer
<p>16. ASDEs and NUiC Operators shall ensure that ‘data protection by design and by default’ measures are incorporated throughout the AV development process. This should include:</p> <ul style="list-style-type: none"> <li>a) Ensuring any personal data collected by AVs or for training AV systems is strictly limited to what is necessary for the purpose for which it is processed<sup>[footnote 27]</sup>;</li> <li>b) Ensuring any personal data that is not necessary to perform the legitimate purposes established by Rec. 15(f) is anonymised at the point of collection or creation (for instance by blurring or pixelating facial image data of pedestrians);</li> <li>c) Ensuring any personal data is only stored for as long as is strictly necessary, and is not transferred from the vehicle except for specific, clearly defined purposes, with reference to the legitimate purposes established by Rec. 15(f);</li> <li>d) Ensuring that any sharing of personal data that is required for one of the legitimate purposes established by Rec. 15(f) is</li> </ul>	<p>Authorisation authority</p>



done in a way that protects individuals privacy, for instance through the use of differential privacy techniques.

---

## **AVs as surveillance cameras and telecommunications devices**

The cameras on AVs have the capacity to function much like surveillance cameras in the sense that they can collect, store and transmit video data of environments, including other road users in public and private spaces.

Given this capability, our recommended approach is that ASDEs should comply with [legal requirements \(https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/\)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/), such as transparency requirements as set out in UK GDPR, and follow established good practice for the responsible adoption of surveillance cameras, such as the [ICO's guidance \(https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/\)](https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/) on surveillance cameras<sup>[footnote 28]</sup>.

Some AVs use video cameras that, while their primary purpose is safe operation, can also function as surveillance cameras by collecting, storing and transmitting video of their environments (in a non-targeted way). This video data could potentially be reused for other purposes such as evidence of crimes unrelated to road safety, and there is some [evidence \(https://www.thetimes.co.uk/article/detective-tesla-videos-itself-being-keyed-cpfq2xgqf\)](https://www.thetimes.co.uk/article/detective-tesla-videos-itself-being-keyed-cpfq2xgqf) that this is already happening in both public and private places. Unlike dash cams, these are now potentially core capabilities of the safe operation of an AV, which would be regulated in the future by DfT agencies. In effect, this is potentially approving a surveillance capability, and DfT should draw on the existing governance frameworks for surveillance cameras.

Beyond the Data Protection legislation and guidance outlined above, the Police and Criminal Evidence Act (PACE) 1984 (s.20) and related Codes of Practice provide the existing legislative framework around the collection of criminal evidence, including the power for police to seize electronic information from vehicles, along with safeguards for the use of these powers, such as requirements for warrants and/or consent. The PACE legislative framework would apply to information collected and stored in AVs, just as it applies to all other electronic devices.

As ASDEs and NUIC Operators provide a service or system that involves facilitating the transmission of communications, they may also fall under the classification of 'telecommunications operators' for the purposes of the Investigatory Powers Act (IPA) 2016. IPA provides the legislative framework for police forces, intelligence agencies and certain regulators to gather information

for intelligence and investigation purposes along with oversight of the use of these powers by the Investigatory Powers Commissioner. As ASDEs may be obliged to comply with the IPA, it will be important to clarify and communicate any obligations to them, especially distinguishing between the categories of AV data that could satisfy definitions in the IPA. For example, if ASDEs are classified as telecommunications operators, they will need to be able to distinguish between ‘communications data’ and ‘the content of a communication’, which has much stricter requirements on being shared, as set out in [s.261 IPA \(https://www.legislation.gov.uk/ukpga/2016/25/section/261/enacted\)](https://www.legislation.gov.uk/ukpga/2016/25/section/261/enacted).

Recommendation	Implementer
17. Where ASDEs are collecting video data of other road users, they should ensure adherence to the relevant ICO guidance on <a href="https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/">video surveillance (https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/)</a> . The authorisation authority should review adherence to the relevant ICO guidance as part of the authorisation decision.	ASDE, Authorisation authority
18. AV cameras that collect personally identifiable information (either within or outside the vehicle) should be clearly indicated. If AVs are collecting camera data of other road users, this should be clearly indicated on the outside of vehicles.	ASDE, Authorisation authority
19. The Home Office should issue guidance clarifying how the Investigatory Powers Act 2016 applies to ASDEs and NUiC Operators.	Home Office

## 3. Fairness

### Introduction

AVs will have implications for the distribution of risks and benefits across groups. Access to the technology will be uneven. The factors that determine who benefits from AVs will include questions of economic development and transport planning that are outside the scope of this report. However, AVs as data-driven technologies have the potential for various forms of algorithmic bias, which may be hard to predict in advance of deployment at scale.

This bias may result in unfair outcomes for particular groups, which may give rise to legally-defined discrimination. Where AVs categorise vulnerable road users (for example, children, adults, wheelchair users), there is a risk of discrimination that could include protected characteristics. As with any algorithmic system, there are risks of bias and error that can be mitigated by diversifying training datasets and by appropriate choice of ML models and hyperparameters. Nonetheless, some systemic injustices may only become apparent once systems are operational. The uncertainties here point to a need for effective collection and sharing of data on how AVs affect different groups.

## Bias in training data

Issues of algorithmic bias have emerged as important and problematic across a range of data-driven technologies. Given the types of data required to perform the AV’s functionality (such as detecting types of road users and their movement), there is reason to believe that these issues, particularly when it comes to protected characteristics such as race, may not be as great with AVs as with, for example, [facial recognition technologies](https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology) (<https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology>). However, the possibility of systemic biases should not be dismissed. Researchers involved in AV testing and development have already spotted potential data gaps caused by a concentration of testing and data collection in some areas.<sup>[footnote 29]</sup> People and objects that are seen less often, such as wheelchairs and wheelchair users, may be underrepresented in training data. Algorithmic bias could also occur with respect to in-vehicle technologies, for example in ‘attention detection’ technologies that use biometric data to judge whether a user in charge is tired or distracted.

Advanced sensing technologies such as gaze detection and intent prediction may, in the future, demand data at a granularity that has implications for bias. Safety cases may, in the future, benefit from identifying, for example, young and old people. Following recent changes to the UK Highway Code, an ethical focus on AVs offering additional protection for vulnerable road users would be justified, which may require more attention to classification of types of road user.<sup>[footnote 30]</sup> The need for AVs to classify road users in terms of whether they are, for example, cyclists, pedestrians, or horse riders and make predictions accordingly, creates a risk if road users are hard to classify.<sup>[footnote 31]</sup>

Recommendation	Implementer
20. To minimise the risk of algorithmic bias, ASDEs’ safety cases and impact assessments <sup>[footnote 32]</sup> should report on the fit between their training data and their ODDs.	ASDE, with oversight from the Authorisation authority



Substantially altered ODDs should require new reports on training data.

---

21. Where training data distinguishes between categories of road users, e.g. between children and adults for reasons of safety, this should be acknowledged as part of the safety case and reported to the authorisation authority. Steps should be taken to anticipate and minimise unfair consequences resulting from data bias, including discrimination.	ASDE, with oversight from the Authorisation authority
--	---

---

## Differentiated treatment between different types of road user

Recommendation	Implementer
22. Where systems distinguish between groups while driving, justified on the grounds of safety, e.g. the identification of children, wheelchair users or other vulnerable road users, ASDEs should have a duty to report in order to allow independent scrutiny (including, but not limited to, reporting this in the safety case). <a href="#">[footnote 33]</a>	ASDE, with oversight from the Authorisation authority and In-use regulator

---

## Risk distribution

AVs will change the balance as well as the magnitude of risk, although the distribution of risk may be unpredictable. Even if AVs enable large improvements in overall safety, some groups may see substantial safety improvements while others see none or even face new hazards. As with other issues involving the rules of road use, perceptions of risk are likely to be important. It will be important to understand whether vulnerable road users feel more or less vulnerable around AVs. Vulnerable road users, who have recently been granted revised attention by the updated Highway Code[\[footnote 34\]](#), are likely to have particular interests in changes of rules of the road that may be made to accommodate AVs. There is a need for meaningful data on how AVs affect different groups. Some of this may be possible through independent scrutiny of risks and risk perceptions around AVs[\[footnote 35\]](#), but it will also require access to ASDEs’ own data on collisions and near misses. ASDEs will need to consider the types of data it is appropriate to collect for understanding

impacts on different groups and how data is stored, in line with data protection requirements. Assessing outcomes of collisions or near misses for discrimination could be a lawful purpose for processing data such as a pedestrian’s detected gender - but would have to take into account ‘data protection by design and by default’ considerations set out above.

While our recommendation on mitigating bias in training data (Rec. 21) will help to give confidence that training data used is representative of the ODD, it will also be important to ensure that the reality of the deployment domain continues to reflect the ODD. Ongoing reporting and independent scrutiny of risks and biases that might emerge as AVs are deployed will be an important way to address this.

Recommendation	Implementer
23. ASDEs and NUiC Operators should facilitate independent scrutiny of emerging risks and biases (in addition to those raised by notifiable events) so that the distribution of risks can be assessed.	ASDE, with oversight from the in-use regulator and Authorisation authority
24. The in-use regulator, advised by CAVES, should collect data on fairness and safety outcomes in order to allow feedback to operators and collective learning. In the event that serious problems are identified and no other means prove effective in mitigation, the regulator should be empowered to impose sanctions, up to and including de-authorisation and product recall (cf. LC Rec. 20 - data gathering on safety).	In-use regulator
The in-use regulator should also compile evidence for where an amendment to the regulatory framework may be necessary (e.g. updates to the RR) to ensure that AVs are acceptably safe, with continual improvements in safety (see also Rec. 8).	

## Fair treatment and access

Some aspects of fairness might be designed into AV systems from the start so that they are more inclusive. For example, there could be new vehicle designs that are more accessible to disabled people. Other questions of accessibility may become clear as systems are tested and deployed, which will demand careful oversight. The safe operation of AVs may make demands on other road users, who could hypothetically be asked to change their behaviour or carry

devices to make them more easily detectable. Our recommendation is that it should be the ASDE's responsibility to ensure the safety of vulnerable road users, and vulnerable road users should never be required to wear or carry devices that would make them more visible to AVs. However, we also note that there may be additional safety benefits to such devices, which should be recognised by ASDEs.

AVs could also have fairness implications resulting from the infrastructures that support them. The Law Commissions were clear that 'one of the UK Government's principles for introducing AVs on GB roads is that they should be able to cope with existing infrastructure'. [\[footnote 36\]](#) However, their report acknowledges that changes to infrastructure may become an important part of ASDEs' safety cases in the near future. AVs may suit some types of roads more than others, they may depend upon Vehicle-to-infrastructure (V2I) connectivity, and demands for their safe operation may create pressure to segregate AV spaces or 'AV-only' lanes.

Some infrastructure changes may be paid for by ASDEs. However, if investments in AV-friendly infrastructure are costly and taxpayer-funded but seen as benefiting a minority of people who travel in AVs, this would change the balance of costs and benefits, jeopardising public trust. AV developers are currently incentivised to downplay the need for changes to infrastructure, as part of asserting the capabilities of their systems. A thorough review of short-term AV infrastructure needs and long-term infrastructure possibilities would allow planners and local authorities to make better-informed decisions.

Recommendation	Implementer
25. AV regulators should assess the potential risks of discrimination, and the adequacy of accessibility features in their authorisation and licensing decisions, in line with their Public Sector Equality Duty (cf. LC Rec. 63 - accessibility advisory panel).	Authorisation authority and licensing authority
26. ASDEs should not, as part of their SEOC, require vulnerable road users to carry or wear anything to make them more easily detectable to AVs. Should vulnerable road users decide to use such devices, however, ASDEs should not ignore their potential additional safety benefits. <a href="#">[footnote 37]</a>	Authorisation authority and In-use regulator
27. If infrastructure upgrades are required that contribute to AV safety, their costs and benefits for other road users should be fully understood and carefully balanced.	Local authorities and other infrastructure bodies; National Infrastructure Commission

# 4. Explainability

## Introduction

Self-driving vehicles are sometimes referred to as ‘autonomous’ vehicles, but it is important to remember that they lack moral autonomy, so cannot be held accountable for their actions. For this reason, the UK Government avoids describing them as ‘autonomous’ and instead uses the term ‘self-driving’. The term ‘self-driving’ also aids public understanding and will become a protected term for the purpose of marketing products to the public. Since a self-driving vehicle lacks agency, any action it performs must be traced back to its designers and operators. The Law Commissions have concluded that it is not reasonable to hold an individual programmer responsible for the actions of the vehicle. Instead, the ASDE as an organisation bears responsibility. This raises a fundamental need for an appropriate degree of explainability for the vehicle’s ‘decisions’. We have seen in the investigation of high-profile self-driving vehicle crashes that perception and classification of some objects might be poor and that complete post hoc explanations might be difficult. [\[footnote 38\]](#) This is a complicated area, and newly emerging. We recommend that CAVES consider this issue in order to give guidance to government on regulating this area (see Recs. 45 and 46).

Explainability (being able to understand why AV systems do what they do, both in real-time and in hindsight) enables improvements in safety and accountability, and provides evidence with which to evaluate the safety and fairness of systems. [\[footnote 39\]](#) It allows regulators to understand the behaviour of AVs and to hold ASDEs and NUIc Operators to account. Some machine learning based systems are challenging to explain, but improving the explainability of AI systems is an active research field and a lot of progress has been made in this area. Some opacity may be expected depending on the AI system used, but what matters is that there is sufficient explainability for accountability similar to the level of explainability currently needed to hold human drivers accountable. Technology companies and regulators need to be able to understand a system’s decisions so that they and others can learn from collisions and near misses. Accordingly, the use of deep learning for safety critical systems represents a substantial governance challenge. There are emerging efforts to build standards for transparency of ML systems. [\[footnote 40\]](#) We recognise there will be further effort required to ensure meaningful explainability and technical feasibility.

Standardising the disclosure of data is also a clear priority. The ethical black box follows the example of ‘black box’ flight recorders on aircraft, devices that are mandated by international regulators with the data they produce shared immediately with investigators. The intent is that it should be possible to generate explanations for notifiable events, not just for collisions, to facilitate

learning as systems grow in maturity. The additional task of explainability during a system's normal operation to aid research and development has been labelled (<https://www.bsigroup.com/en-GB/CAV/cav-resources/safety-benchmarking-report/>) 'digital commentary driving' by the British Standards Institution (BSI). This process would provide assurance that systems' safety-critical sensors and decision making systems are doing what is expected of them, mitigating the possibility of surprises.

The potential hazards of AVs as robots operating in open-ended, uncertain environments, raise the stakes for the interpretability of AI. With other technologies that make use of machine learning systems, performance has been prioritised over interpretability. Growing interest in explainable AI is starting to redress this balance, but there may be some uses of machine learning in AVs, such as computer vision, that remain incompletely interpretable. It may be impossible to know with certainty why an AV image recognition system classified an object or a person according to a particular category. Other parts of AV systems, such as those that determine the speed and direction of the vehicle, are in many cases rules-based and therefore more easily explainable.

Techniques for ensuring explainability will differ across AV systems. An ASDE may need to review logs from a particular event or replay logs through a simulator. Generating explanations for ML-based systems remains an active research area and it is likely that capabilities will advance significantly in the coming years. The recommendations have been framed to be as independent as possible of particular explainable AI methods, and to put the onus on the ASDE to generate explanations, as and when required.

## **Recommendation**

## **Implementer**

28. The ASDE should design the AV so that it is possible to construct an explanation of the key decisions made by the AV when it is undertaking the Dynamic Driving Task (DDT) for a bounded test scenario. These explanations should be made available as required under the duty of disclosure including, as a minimum:

ASDE, reporting to the appropriate regulator

- a) to the authorisation authority as part of the SCR;
- b) to the NUiC Operator where appropriate.

29. For collisions, near misses and other notifiable events, the ASDE should design the AV so that it is possible to construct an explanation of the key decisions made by the AV leading up to the event, however caused. This explanation should be sufficient to identify and rectify causes of undesirable behaviours, and the ASDE should make the

ASDE, reporting to the Authorisation authority; also In-use regulator and collision investigation unit

explanation available to:

- a) a collision investigation unit for the incident being investigated;
  - b) the in-use regulator when investigating a notifiable event to potentially apply a sanction;
  - c) other parties with a legitimate need for the information agreed in advance as part of authorisation (cf. LC Recs. 21, 22, 29 on incident investigation; cf. LC Rec. 74 on data disclosure).
- 

## 5. Data sharing

### Introduction

There are many advanced technologies whose inner workings remain largely opaque to their users and the general public. However, it would be a mistake to presume that there is no public interest in questions of explainability. Expert witnesses and regulators able to translate features for the public will be important intermediaries. We have seen that when prominent crashes have been investigated by the National Transportation Safety Board in the US, the availability and interpretability of data have become important points of contention. A balance will need to be struck between trade secrets and data sharing, particularly when data is safety-critical. UNECE standards for a Data Storage System for Automated Driving (DSSAD) and an Event Data Recorder (EDR) can help to enable sharing of some of the data relating to safety-critical functions, such as establishing who was in control of a vehicle during an incident. However, as a data rich and data-driven technology, there is also potential for data sharing to enable safety improvements across the AV sector.

We note that there are already obligations under vehicle type approval to share data with regulators and third parties, and some similar requirements will be necessary to facilitate the sharing of data with the authorisation and licensing authorities. Beyond these obligations, the wider goal of improving the safety and effectiveness of AVs will require additional data-sharing.

Data-sharing mandates may require standardised formats for data storage and definitions of notifiable events, which currently vary widely between companies.



## Safety cultures

The Law Commissions have discussed the aim of establishing a ‘no-blame safety culture’, which would allow learning between competitors. Similar approaches have led to improvements in safety in medicine and air travel, where learning is prioritised over legal liability in incident investigations. In the airline industry, for example, the US National Transportation Safety Board has sought to encourage the idea that ‘anybody’s accident is everybody’s accident’. Until recently, it was possible to assert that airlines and aircraft manufacturers did not compete on safety. Historically, this system was sustainable because of a tight relationship between regulators and industry. The recent crashes of Boeing 737 Max aircraft reveal that such a model can lead to complacency, regulatory capture and serious harm.<sup>[footnote 41]</sup>

However, there may be benefits to competition based on safety while the technology is new. NCAP and EuroNCAP, the New Car Assessment Programmes, do not only test for regulatory compliance; they also incentivise safety innovation above and beyond the minimum through the use of star ratings.<sup>[footnote 42]</sup> These positive effects of competition should be noted, but we should also recognise that this competition has often benefited the safety of drivers and passengers rather than other road users. In the US, for example, road use has, on average, become increasingly safe for drivers but more dangerous for pedestrians since 2000.<sup>[footnote 43]</sup> We think that a balanced approach that involves aspects of a ‘no blame’ or ‘safety first’ culture - for example, the sharing of safety-relevant data (see Rec. 32), alongside some degree of competition on safety - is optimal.

## Novel data sharing approaches

Regulators and the AV sector should explore the ways in which mechanisms that facilitate responsible sharing of commercially sensitive data, such as data intermediaries, could be used. An example of a data intermediary that facilitates safety improvements while ensuring the protection of commercially sensitive data in the aircraft industry is included below.

### **Case study: Advanced Product Concept Analysis Environment (APROCONE)**

APROCONE is an industrial data platform that facilitates collaborative product design in the airline industry. It involves a range of public and private organisations including Airbus, Rolls-Royce, academic partners, and supply chain companies in the aircraft industry.

The purpose of APROCONE is to improve collaborative product design for aircraft, while protecting participants’ intellectual property through a digital

platform that allows the secure exchange and sharing of product data. The industrial data platform operates between consortium partners who are able to control their intellectual property, allowing other parties access to minimally required information to support their own designs. Partners can choose to add or remove partners and use their existing analysis tools, with the platform performing the required actions that ensure interoperability between partners, overcoming barriers to efficient and cost effective data sharing.

The data sharing facilitated by APROCONE has enabled an innovative approach to initial aircraft and engine sizing that is at least ten times faster and could deliver significant fuel burn savings. The platform has led to manufacturing cost savings and has enhanced design processes by making valuable data available earlier in the design lifecycle.

For full case study, see Centre for Data Ethics and Innovation's [Unlocking the value of data: Exploring the role of data intermediaries](https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries) (<https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries>).

## Privacy-enhancing technologies (PETs)

One example of a privacy-enhancing technology (PET) that could be useful in this context is federated analytics. Federated analytics [refers](https://cdeiuk.github.io/pets-adoption-guide/what-are-pets) (<https://cdeiuk.github.io/pets-adoption-guide/what-are-pets>) to 'a paradigm for executing a computer program against decentralised data'. Federated learning, which is a subset of federated analytics, refers to approaches which train machine learning models on distributed data sets. In the case of self-driving vehicles, it might be useful to explore how these types of techniques could be applied to minimise the amount of data that is uploaded to a centralised server, since it would instead be stored locally in the vehicle itself.

**Case study:** [GBoard](https://cdeiuk.github.io/pets-adoption-guide/repository) (<https://cdeiuk.github.io/pets-adoption-guide/repository>)

GBoard is a keyboard app for Android and iOS devices. It features next-word prediction, driven by a machine learning model. GBoard utilises federated learning where each mobile device downloads an initial model from a central server, which is further trained on the device using user data local to the device. The weights of the resulting model are periodically communicated back to the central server using a secure aggregation protocol (a form of multi-party computation), which aggregates the weights received from all mobile devices into a new common model that reflects



data from each individual user, without sharing any of the underlying data. Devices download this new model, and the cycle repeats, such that the model is [continuously trained \(https://ai.googleblog.com/2017/04/federated-learning-collaborative.html\)](https://ai.googleblog.com/2017/04/federated-learning-collaborative.html) without collecting user data centrally.

Recommendation	Implementer
30. In consultation with the authorisation authority, the ASDE shall publish a summary of the SEOC, which will be made publicly and freely available upon authorisation of the vehicle for self-driving.	ASDE, reporting to the Authorisation authority
31. The ASDE and NUiC Operator should communicate safety-relevant data with other organisations in the AV ecosystem when requested, including other ASDEs, the in-use regulator, the authorisation authority and the collision investigation unit, using agreed data formats, where this contributes to road safety. Data formats should be decided by the authorisation authority and in-use regulator, in consultation with the ICO. <a href="#">[footnote 44]</a>	ASDE and NUiC Operator, with oversight from the In-use regulator
a) The ASDE and NUiC Operator should share core safety-relevant data as stipulated by the in-use regulator and collision investigation unit; (note that there will be some aspects of safety-relevant data that the ASDE and NUiC Operator will be legally required to share for law enforcement purposes. <a href="#">[footnote 45]</a> )	
b) The in-use regulator and collision investigation unit should consult on the agreed scope and format of the core safety-relevant data they will require from ASDEs and NUiC Operators;	
c) The ASDE and NUiC Operator should be encouraged to share data with interested parties, using standards and formats developed via consensus;	
d) Regulators and the AV sector should explore the ways in which mechanisms that facilitate responsible sharing of commercially sensitive data, such as data intermediaries, could be used;	
e) ASDEs and NUiC Operators should explore the use of privacy-enhancing technologies such as <a href="https://cdeiuk.github.io/pets-adoption-guide/what-are-pets">federated learning techniques (https://cdeiuk.github.io/pets-adoption-guide/what-are-pets)</a> , to minimise the volume of personal data that is uploaded to a centralised server.	
32. The ASDE and NUiC Operator shall provide summarised safety performance data to relevant bodies including the in-use regulator to enable the safe, ethical	ASDE and NUiC Operator, reporting to the

and effective operation of the AV marketplace (cf. LC Recs. 20, 74).	Authorisation authority
33. The ASDE and NUiC Operator shall support reasonable access to all relevant proprietary information by a road collision investigation unit and other authorised bodies to enable collision and incident analysis and support the authorities in producing lessons learnt for dissemination to other ASDEs. <a href="#">[footnote 46]</a>	ASDE and NUiC Operator, with oversight from the In-use regulator
34. The in-use regulator shall define formats for safety-relevant data to enable sharing between relevant organisations, including ASDEs, the authorisation authority and the collision investigation unit, to ensure consistency and equity in regulation. This could be achieved via the guidance the Commissions recommend they publish on data sharing.	In-use regulator

## 6. Public trust

### Introduction

Whereas some technologies are developed behind closed doors, important aspects of the development of AVs are taking place in public. Much of the testing and assurance of this technology needs to happen on public roads, which involves complicated relationships with other road users, citizens, local authorities and transport planners. If the purported benefits of AVs are to be realised, the technology will need to be trustworthy and public hopes and fears will need to be well understood. As with other complex sociotechnical systems like air travel, people will decide whether to place their trust not in the technology per se but in the systems that govern the technology and assure its safety and benefits. [Public dialogue exercises](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951094/cav-public-acceptability-dialogue-engagement.pdf) ([https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/951094/cav-public-acceptability-dialogue-engagement.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951094/cav-public-acceptability-dialogue-engagement.pdf)) and surveys have revealed a mix of excitement and concern about the technology among the British public.

A survey of 4,860 members of the British public conducted as part of the Driverless Futures? project provides some insight into early public views [\[footnote 47\]](#).

- Levels of comfort with the idea of using self-driving vehicles or sharing the roads with them have remained similar since 2015. A small majority of respondents would be uncomfortable using self-driving vehicles (58%) or sharing the road with them (55%);
- Respondents demanded transparency: not only that vehicles driving themselves must be identifiable (86% agreeing), 91% agreed that ‘the companies behind [self-driving vehicles] must be able to explain the actions taken by their vehicles, while 68% preferred the statement that self-driving vehicles ‘should be required to make public the full details of how their AI systems work’ to the suggestion that they should be able to ‘keep private the details’ (preferred by 12%). 81% agreed that ‘there should be international standards regulating [self-driving vehicle] technology’ (3% disagreeing);
- 86% of respondents agreed or strongly agreed that ‘it must be clear when a vehicle is driving itself’;
- In the event of a collision, 92% agreed or strongly agreed with the statement ‘all data must be made available to investigators’.

Building public awareness and understanding of self-driving vehicles will be one important element of facilitating public trust. Another important element will be the opportunity for the public to engage in genuine dialogue about this technology. The fact that both the technology itself and the structures that will govern it are still in relatively early stages of development presents an opportunity for an open public conversation on these issues.

## Public information

There is currently public confusion, exacerbated by some claims from industry, about the capabilities and limits of AV systems.<sup>[\[footnote 48\]](#)</sup> All of the issues above, including safety, fairness, privacy and transparency, raise the question of presenting accessible information about the functioning and performance of AVs to the public. The Law Commissions have made recommendations for legislation that clarifies terminology for AVs. Definitions of, for example, ‘self-driving’ also demand clarity on the conditions under which a vehicle can be said to perform those functions. This means clear communication of a vehicle’s Operational Design Domain (ODD), defined by the BSI as the ‘Operating conditions under which a given driving automation system or feature thereof is specifically designed to function’. Companies are currently incentivised to downplay ODD definitions in public communications and overstate the capacity of their technology. When it comes to questions of liability, companies will have the opposite incentives, to claim that their ODDs are narrow. If the technology is going to be trustworthy, technology developers need to be clearer about all aspects of the ODD, including locations, weather conditions, road types, infrastructure requirements and other road users’ behaviour.

Recommendation	Implementer
35. The rules on the use of terminology such as ‘self-driving’ should include requirements to inform the public about the conditions under which self-driving vehicles can operate, e.g. road types, locations, weather, other road users’ behaviour. <a href="#">[footnote 49]</a> <a href="#">[footnote 50]</a>	ASDEs, Authorisation authority and In-use regulator

## Consultation and public engagement

The potential implications of AVs demand wide public consultation. The testing of any technology in public raises ethical questions about safety risks, informed consent, and the ability of people, if they are regarded in some way as test subjects, to opt out if desired. Effective public engagement will be crucial to understanding and mitigating the ethical issues raised in this report. There should be ongoing dialogue with the public that informs the design and regulation of systems. Groups at risk of marginalisation, such as disabled people, should be consulted so the design and regulation of systems can be as inclusive as possible. There is a need for ongoing dialogue and social research to deepen understanding of public views on liability, labelling, the explainability of decisions made by AVs, and possible infrastructure changes as AV systems expand and develop. These are important as they can have a direct impact on safety (infrastructure), acceptability of AVs (labelling, explainability) and on accountability and the requirement to provide recompense (liability).

Recommendation	Implementer
36. An accessible summary of the SCR should be made public and should include clear statements of the functions and limits of an AV within an ODD.	ASDEs, Authorisation authority
37. The in-use regulator shall regularly publish publicly accessible reports on the achieved level of safety of AVs, which should include records of notifiable events and actions taken to improve safety of deployed AVs, including updates to the Road Rules. This should form part of its duty to publish evidence of AV safety, as recommended by the Law Commissions (cf. LC Rec. 19).	In-use regulator
38. Prospective ASDEs and NUiC Operators should engage with local communities, including local authorities, when an AV trial is planned in a particular area. <a href="#">[footnote 51]</a> This engagement should inform testing and/or deployment (e.g. placing conditions on times, places, public information,	ASDE, NUiC Operator, In-use regulator

maximum speeds etc).

Where the vehicle is permitted to carry passengers, the service operator should consult with relevant authorities as proposed under the Law Commissions' passenger permitting scheme.

---

39. Serious incidents in the operation of an AV should be publicly investigated and reported. A road collision investigation unit should have a duty to report publicly on serious incidents. Evidence gathered during the investigation should be published so that others can learn lessons. <a href="#">[footnote 52]</a>	Road collision investigation branch
--	-------------------------------------

---

40. CCAV should commission public dialogue and social research to seek public views on:	CCAV
---	------

---

- a) Balancing the tensions between achieving a 'safety-first culture' and ensuring sufficient accountability for the consequences of AV behaviour;
  - b) The distribution of AV risks and benefits;
  - c) Future changes to infrastructure and rules of the road and any associated costs;
  - d) Explainability of decisions made by AVs;
  - e) Labelling of vehicles.
- 

## **Trials**

It will be particularly important for trialling organisations (or ASDEs where relevant) to engage with local communities in the vicinity of their trials in order to understand opportunities and concerns. In the absence of governance attention, trials of technologies could become de facto deployments. Safety cases that are currently built around the presence of a safety driver (who is understood to have full responsibility) will look very different from safety cases for self-driving systems. Public trials of the technology are opportunities for learning beyond the data collection carried out by the company running the test. Other parties should be encouraged and empowered to engage with and learn from the experiences of AVs on public roads. Local authorities will have interests in the future viability of AV services that might emerge from trials happening in their area, but they may lack the resources to engage with trialling organisations in the co-design of trials or in making sense of trial data.

As trials of the technology are in many cases happening in public, there may be a slippery slope from trials to de facto deployments of the technology as numbers of vehicles scale up and ODDs expand. Large-scale, highly

concentrated deployments, measured by number of vehicles within a particular area, for example, may have different ethical implications from smaller deployments. The line between testing and deployment may be hard to draw. Systems that are deployed may (and in many cases should) be used to gather ongoing data to improve safety, service design etc.

Recommendation	Implementer
41. Where AVs are being trialled, the safety driver should not be removed unless the vehicle is authorised <sup><a href="#">footnote 53]</a></sup> , and AVs should only carry passengers where the appropriate passenger licence has been issued.	CCAV, in-use regulator and Authorisation authority
CCAV should support local authorities to monitor trials in their area (e.g. to identify significant increases in the number of vehicles involved in a trial) and to make passenger licencing decisions, for example via guidance.	
42. Where an ASDE is given a limited authorisation to trial an ADS feature, the vehicle must be re-authorised should the ASDE wish to deploy the feature in a wider context.	Authorisation authority and In-use regulator

## Labelling

The labelling of vehicles is ethically complex. Self-driving vehicles should be considered a new class of road user when operating in mixed traffic. They will not always behave in the same way as human drivers do (recognising that there is a wide range of ‘normal’ driving behaviour) and while there may be some external signs of novelty (e.g. large Lidar sensors on a vehicle’s roof), people may not know what these mean or if a vehicle is being driven by a human or by software. Sensors are likely to become smaller over time and in some cases would be essentially invisible, making some AVs indistinguishable from conventional cars. The novelty of AVs creates an argument based on the principle of human autonomy that people have a right to know what sort of agents they are sharing the road with. With some of the low-speed crashes in which human drivers have been blamed for collisions with some types of self-driving vehicles, we can assume that uncertainty about the often ultra-cautious manoeuvres of those vehicles was a contributory factor.

One of the Engineering and Physical Sciences Research Council principles for robotics [states](#) (<https://www.tandfonline.com/doi/full/10.1080/09540091.2016.1271400>), ‘Robots are



manufactured artefacts. They should not be designed in a deceptive way to exploit vulnerable users; instead their machine nature should be transparent'. The range of possible interactions on the road make labelling complicated in practice, but this principle represents a good starting point.

However, labelling could change the distribution of responsibilities in profound ways. An expectation that other road users will understand and adapt (as with emergency vehicle warning lights and sirens or L-plates for learner drivers) could be interpreted as an abdication of AV developers' responsibility. Additionally, self-driving vehicle companies may be concerned that clear labelling will lead other road users to behave differently around their vehicles, affecting their data collection, or to take advantage of their vehicles' assumed greater caution. The emergence of AVs onto roads will shift the responsibilities of all road users, as previous technologies have done. On balance, it is better that this is done in a deliberate and informed way rather than under conditions in which road users are uncertain. This should be seen as part of the debate on wider changes to rules of the road. The ethics of on-road communication with other road users should not be overlooked as systems develop. The practicalities of labelling would need careful research and discussion, but there is clear [public support \(https://driverless-futures.com/2022/05/09/survey-reports/\)](https://driverless-futures.com/2022/05/09/survey-reports/) for the principle; 86% of UK survey respondents agreed or strongly agreed that 'it must be clear when a vehicle is driving itself'.

External Human-Machine Interfaces (e.g. lights or display panels that clarify when an AV has detected a pedestrian and deemed it safe to cross) may be deemed necessary by some ASDEs, in shared spaces or to break deadlocks at crossings. Such innovations would need to be developed with care, as they may be used as an excuse for unsafe practices by creating expectations that vulnerable road users should understand and know how to respond to signals.

## Recommendation

## Implementer

43. AVs should be clearly labelled. Where vehicles can drive themselves or be driven conventionally at different times, signals should indicate the status of operation. This external labelling should be in addition to information inside the vehicle that clearly indicates mode of operation. AV tests and deployments should be clearly publicised within and near the relevant location.

ASDEs, with oversight from the authorisation authority<sup>[[footnote 54](#)]</sup>

44. CAVES should review and advise on the practicalities of labelling and the questions of liability raised by External Human-Machine Interfaces on AVs.

Committee on AV Ethics and Safety (CAVES)

# 7. Governance

## Introduction

Refining and implementing this framework will take time because the introduction of more sophisticated ADSs and AVs will take place over years and decades. Also, implementing the framework will involve judgements by individual ASDEs and NUiC Operators which can have an impact on the safety and wellbeing of all road users and other stakeholders. Whilst some of these are rightly the province of such organisations, there are areas where there is a need for consistent standards between ASDEs and NUiC Operators, both to uphold societal norms and to avoid risks that might arise due to inconsistency in behaviour between different AVs. It is not possible to be prescriptive about such issues - certainly not with sufficient foresight - hence we recommend the establishment of a joint Committee on AV Ethics and Safety (CAVES) to advise the relevant authorities and to seek consensus on those issues which need to be managed and agreed centrally, to support the safe and ethical introduction of AVs on UK roads.

## Committee on AV Ethics and Safety

The purpose of the Committee should be to provide contestable advice and recommendations - as opposed to decisions - on policy and ethical issues regarding the safety of AVs. The scope of the advice and recommendations is likely to include issues relevant to policy, authorisation, and in-use regulation and therefore should be issued to the Department for Transport, including its motoring agencies. The Committee should assess the benefits of AVs alongside the risks to provide a balanced governance approach. We would expect the committee to sit within the Department for Transport and be managed by CCAV.

In line with the government's code of practice on scientific advisory committees and councils, the purpose of CAVES would be 'to access, interpret and understand the full range of relevant scientific information, and to make judgements about its relevance, potential and application'. The scientific expertise should be broad and [lay members](#)

<https://www.gov.uk/government/publications/scientific-advisory-committees-code-of-practice/code-of-practice-for-scientific-advisory-committees-and-councils-copsac-2021>) 'may act as a critical friend, contribute experience from outside the professional membership, or provide an external non-expert perspective to the decision-making process'. We see the Food Standard Agency's [scientific advisory committees](#) (<https://www.food.gov.uk/about-us/scientific-advisory-committees>) (e.g.



The Advisory Committee on Novel Foods and Processes) as a useful model that CAVES could follow.

## Recommendation

## Implementer

45. The authorisation authority and in-use regulator should establish a **joint Committee on AV Ethics and Safety (CAVES)** composed of experts and lay members with a diverse range of perspectives (cf. LC Rec. 30 - in-use regulator's duty to consult).

Authorisation authority; In-use Regulator.

a) CAVES should report to the Secretary of State for Transport (DfT). Since the SoS's powers will likely be delegated to the motoring agencies, in practice CAVES will advise the motoring agencies (which are themselves part of DfT).

b) CAVES' recommendations and policy advice should be issued to DfT and the regulators in parallel for full visibility. Its reports and minutes should be public by default (recognising that some discussions will need to be held in private). CAVES should provide advice and constructive challenge to DfT. It should not make policy decisions or overrule the Secretary of State.

c) CAVES should have a standing Road Rules Subcommittee that includes stakeholders representing different groups of road users, to provide advice on the definition of the RR, including consistency with published specifications for Automated Driving Systems (ADS), especially on ethical rules and priorities. [\[footnote 55\]](#)

d) CAVES should be constituted as a non-statutory, Scientific Advisory Committee, with diverse membership, including lay member representation (e.g. vulnerable road users). Expertise should include engineering, artificial intelligence, human factors, transport planning and policy, road safety, ethics and public engagement. The committee should pay particular attention to questions of accessibility, and should include a member with expertise in disability issues (See LC Rec. 63 - accessibility advisory panel).

e) CAVES should draw on the views of a wide range of stakeholders and undertake stakeholder engagement to ensure that the needs of all classes of road users (including vulnerable road users) are considered in defining the RR and in assuring the overall governance of AVs, including authorisation and temporary restrictions of AV operations.

46. CAVES should have responsibility for assessing regulatory decisions, and should advise on complex issues

Authorisation authority; In-

related to the regulation and governance of AVs, such as labelling, differentiated treatment towards vulnerable road users, and explainability.

use Regulator.

- a) CAVES should assess regulatory decisions, and provide DfT with assurance that the authorisation decision and forms of restrictions on AVs imposed by the regulators provide an appropriate alignment between innovation and safety;
  - b) CAVES should review and advise on the practicalities of labelling and the questions of responsibility raised by External Human-Machine Interfaces on AVs;
  - c) CAVES should review the desirability of appropriately differentiated treatment towards vulnerable road users, and what additional reporting duties may be required;
  - d) CAVES should review the degree of explainability needed for regulatory oversight.
- 

## Next steps

The recommendations in this report will support and guide the Department for Transport as they deliver 'Connected & Automated Mobility 2025: realising the benefits of self-driving vehicles' ([link](#)), a roadmap that commits to developing a new legislative framework that builds trust in self-driving vehicles while enabling innovation.

After laying primary legislation before Parliament in 2022, the Department for Transport will develop and consult on secondary legislation that will set out the details of the requirements and processes of the new legislative framework for self-driving vehicles in 2023. This report will closely inform the development of that secondary legislation.

In particular, our recommendations will inform the design of the new safety framework for self-driving vehicles, and will shape the requirements for what constitutes a sufficient safety case by ASDE and NUiC Operators. Following consultation, the Department for Transport expects to publish further guidance on this issue, closely informed by the recommendations of this report.

## Annex A: Safe and Ethical Operational Concept and Safety Management Systems

# Safe and Ethical Operational Concept (SEOC)

The intent of this brief note is to sketch out what (part of) a Safe and Ethical Operational Concept (SEOC) might look like. As identified above, the SEOC would be a set of constraints on vehicle behaviour, including motion, signalling to other road users, and actions to preserve their own safety.

The SEOC would be defined as a set of Self-Driving Constraints (SDCs) and precedence between these constraints, as they can conflict in certain circumstances. The constraints would also cover signalling as appropriate signalling can reduce concern (and misleading signalling might increase concern). We illustrate part of a SEOC that relates to motion. These are intended to be illustrative and an ASDE’s SEOC would need to be thought through from their perspective on safe and ethical behaviour, e.g. the extent to which they prioritise safety of vulnerable road users. The intent here is to identify some example SDCs, some clear precedence rules, and some situation-dependent precedences so the concept is clear.

**Table 1: Example SDCs**

SDC	Description
-----	-------------

- |   |   |
|---|---|
| 1 | Avoid collision with all other objects  |
| 2 | Maintain safe distance to other objects (given predicted trajectories)                              |
| 3 | Remain on the road, except at an access point to the roadside (e.g. house drive, car park entrance) |
| 4 | Avoid movement that can cause discomfort or harm to passengers                                      |
| 5 | Leave the road away from an access point where this reduces overall risk                            |
| 6 | Avoid movements that cause other vehicles to violate any other SDC                                  |
| 7 | Avoid movements that cause individuals concern about their safety                                   |

8 Follow directions given by authorised persons

---

Table 2: Example SDC Precedences

SDC Precedence

---

SDC 1 takes precedence over SDC 4 (e.g. an emergency stop for an unanticipated object in a vehicle path)

---

SDC 5 takes precedence over SDC 3 (if doing so satisfies SDC 1)

---

Table 3: Example SDC Situation Dependent Precedences

Initiator	Possible Constraint Conflict	Constraint Honoured
Response to Authorised Person (Constraint 8)	Response leads to conflict with constraint 1	1
	Response leads to conflict with constraint 2	8
	Response leads to conflict with constraint 3	3
	Response leads to conflict with constraint 7	8

---

This is intended to be simple enough to communicate the concept. Specific road rules, e.g. clauses from the Highway Code, would be organised under these top-level SDCs, where appropriate. It would be expected that the notifiable events would include items from Table 3 where active (dynamic) choices have to be made between the SDCs; they would probably also include the ‘triggering’ of the precedences from Table 2.

Safety Management Systems (SMS)

## **For ASDEs:**

The SMS should include, at a minimum:

1. A process for safety assessment of design, verification and change relating to the vehicle, covering software, hardware, subsystems and data.
2. Procedures and mechanisms for responding to test failures, incidents, collisions and hazardous failures.
3. Processes, procedures, competencies, certifications and training for vehicle design, manufacture, maintenance and upgrade activities.
4. Processes for responding to directives from regulators, including making design changes and communicating to users/operators of the vehicle.
5. Processes for updating the safety documentation to allow for regular review and re-issue as appropriate.

## **For NUiC Operators:**

The SMS should include, at a minimum:

1. A process for safety assessment of changes relating to the vehicle and its safety case, deployment routes and infrastructure.
2. Procedures and mechanisms for responding to incidents, collisions and hazardous failures.
3. A process for management of specific restrictions, deviations and waivers covering the vehicle, infrastructure and routes, arising from the in-use regulator and other authorities.
4. Processes, procedures, competencies, certifications and training for vehicle operation, maintenance and upgrades.
5. Processes for updating the safety documentation to allow for regular review and re-issue as appropriate.

# **Annex B: List of recommendations**

## **Road safety**

### **Recommendation**

### **Implementer**

---

---

1. The ASDE shall define the AV ODD to be consistent with the relevant Road Rules (RR) and to cover all classes of road users including vulnerable road users that can reasonably be expected in the ODD.	ASDE, reporting to the Authorisation authority
---	--

The ODD definition should include all relevant features defined to an appropriate level of detail. The definition should cover the parameter ranges for fixed scenery elements, attributes of dynamic elements and environmental elements. It should also include all ethically salient features relating to other road users.

Further guidance will be needed from DfT to define these ethically salient features.

---

2. The ASDE shall ensure that the deployment domain is compatible with the ODD prior to operational use of the AV.	ASDE reporting to the In-use regulator
--	--

---

3. The authorisation authority, in concert with the in-use regulator, shall develop and publish guidance on RR in the context of self-driving vehicles, with input from the CAVES Road Rules Subcommittee, to inform the development of SEOCs that:	Authorisation authority
---	-------------------------

- a) give complete coverage of situations that an AV could reasonably be anticipated to encounter in the ODD;
- b) reflect rules of behaviour that are ethical and broadly acceptable across different types of AV; and
- c) identify precedence between the rules.

---

4. The ASDE shall define a SEOC, including Self-Driving Constraints (SDCs) (see <a href="#">Annex A</a> for more detail), for inclusion within its SCR submitted as part of authorisation, for the behaviour of the AV in its ODD, that:	ASDE, reporting to the Authorisation authority
--	--

- a) complies with road rules (RR);
- b) complies with any applicable regulations for automated driving system (ADS);
- c) minimises occurrence of 'at-fault' collisions in its defined ODD;
- d) mitigates risk of 'non-fault' collisions in its defined ODD;
- e) manages entry to and exit from the ODD, ensuring a transition to safe control of the AV by the UiC where there is one, or a safe transition to a minimal risk

condition (MRC) on exiting the deployment domain;  
 f) does not unfairly discriminate against road users or otherwise unfairly treat vulnerable road users;  
 g) does not require other road users to violate applicable rules or SDCs;  
 h) defines the priority of rules and SDCs where they can conflict in particular circumstances;  
 i) does not cause individuals in the vicinity of the AV unjustified concern about their safety;  
 appropriately balances the need to make progress with the need to ensure safety.

5. The ASDE shall demonstrate to the authorisation authority that they have designed the AV to be consistent with the SEOC, and provide supporting arguments and links to evidence in a SCR to gain authorisation for self-driving. The SEOC shall be made publicly available once authorisation is granted.

ASDE, reporting to the Authorisation authority

6. The ASDE shall monitor the operation of the AV to identify situations where it fails to implement the SEOC, inform the in-use regulator of 'notifiable events' and take action to resolve deviations from the SEOC that are not notifiable. Government will need to consider how this interacts with NUiC Operators and what their obligations in relation to the SEOC will be.

ASDE and NUiC Operator, with oversight from the In-use regulator

7. The ASDE and NUiC Operator shall comply with instructions from the in-use regulator or authorisation authority, e.g. to limit the AV deployment domain or modify the vehicle design, to ensure continued safety of operation.

ASDE and NUiC Operator

8. ASDEs and NUiC Operator shall keep their SCR up to date and produce it to the authorisation authority when required to gain approval for changes to the vehicle prior to deploying the changes as part of the vehicle's re-authorisation.

ASDE and NUiC Operator, reporting to the Authorisation authority

9. The ASDE and NUiC Operator shall operate a safety management system (SMS) for the AV governing how they manage safety through the AV lifecycle, and provide periodic independent SMS audit reports to the in-use regulator.

ASDE and NUiC Operator, with oversight from the Authorisation authority and In-use regulator

10. The authorisation authority should assess SMS and safety culture within ASDEs and NUiC Operators as

Authorisation authority

part of the authorisation and licensing decisions respectively, and approve deployments where they meet applicable criteria.

---

11. For authorisation purposes, the authorisation authority shall assess the safety of AV deployments based on:

Authorisation authority and In-use regulator

- a) the SCR
- b) independent SMS audit reports
- c) notifiable events (cf. LC Rec. 20 - data gathering on safety)

The in-use regulator should assess a), b), and c) on an ongoing basis.

---

12. The authorisation authority shall define ‘notifiable events’ in terms of deviation from the ASDE’s SEOC. It will, at a minimum, include traffic infractions as defined by the Law Commissions; an incident that had it been performed by a human driver would have attracted criminal or civil penalties (cf. LC Rec. 20 - data gathering on safety).

Authorisation authority

---

13. The authorisation authority shall define a scheme for determining what changes to AV performance are significant enough to require re-authorisation prior to ASDEs supplying updates to deployed AVs.

Authorisation authority

---

14. The ASDE shall design the AV so that transfers of authority for control of the DDT from the AV to the UiC shall ensure safety, including providing the UiC with sufficient time and information to achieve situational awareness before they engage in the DDT.

ASDE, reporting to the Authorisation authority

The ASDE shall have responsibility and accountability for behaviour of the AV both within and outside the ODD unless it is confirmed that the UiC has authority for control of the DDT.

---

## Data privacy

---

**Recommendation**

**Implementer**

---



---

15. The AV regulator(s) should issue guidance for ASDEs and NUiC Operators clarifying how Data Protection obligations apply to AVs, in consultation with the Information Commissioner's Office. Issues that could be covered include:

ICO;  
Authorisation  
authority; In-use  
regulator

- a) The requirement to conduct a Data Protection Impact Assessment (DPIA), and to make this document publicly available alongside the vehicle's safety case report at authorisation;
  - b) Clarification that an ASDE and/or NUiC Operators should prepare suitable DPIAs and make available for authorisation and licensing decisions;
  - c) A self-assessment checklist to establish whether the ASDE / NUiC Operator is acting as a controller, processor, or joint controller;
  - d) Any requirements to secure valid consent from the UiC or passengers for processing personal data within the vehicle (such as what kinds of data collection would constitute 'location data' and 'cookies or similar' under PECR) and where additional consent may be required, such as when there are new passengers in the vehicle;
  - e) Proposed retention and deletion schedules for personal data collected by AVs, particularly location data;
  - f) What would be considered necessary and legitimate purposes for processing and sharing personal data (e.g. safety improvements, insurance claims etc.);
  - g) Circumstances under which processing of personal data of other road users outside the vehicle (such as facial images of pedestrians) is likely to be considered lawful and proportionate under Article 6 GDPR (e.g. vital interests, or legitimate interests);
  - h) Circumstances under which processing of special category personal data (e.g. biometric data of the UiC) is likely to be considered lawful and proportionate under Article 9 GDPR (e.g. explicit consent, or substantial public interest);
  - i) The testing of AI systems for AVs against the requirement 'to design the AV so that it is possible to construct an explanation of the key decisions made by the AV leading up to the notifiable event, however caused'. See Rec. 29;
  - j) Which ADS features (if any) could be considered 'a decision based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or similarly significantly affects [the data subject]', for the purposes of Article 22 GDPR.
-

<p>16. ASDEs and NUIC Operators shall ensure that ‘data protection by design and by default’ measures are incorporated throughout the AV development process. This should include:</p> <p>a) Ensuring any personal data collected by AVs or for training AV systems is strictly limited to what is necessary for the purpose for which it is processed;</p> <p>b) Ensuring any personal data that is not necessary to perform the legitimate purposes established by Rec. 15(f) is anonymised at the point of collection or creation (for instance by blurring or pixelating facial image data of pedestrians);</p> <p>c) Ensuring any personal data is only stored for as long as is strictly necessary, and is not transferred from the vehicle except for specific, clearly defined purposes, with reference to the legitimate purposes established by Rec. 15(f);</p> <p>d) Ensuring that any sharing of personal data that is required for one of the legitimate purposes established by Rec. 15(f) is done in a way that protects individuals privacy, for instance through the use of differential privacy techniques.</p>	<p>Authorisation authority</p>
<p>17. Where ASDEs are collecting video data of other road users, they should ensure adherence to the relevant ICO guidance on <a href="https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/">video surveillance (https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/)</a>. The authorisation authority should review adherence to the relevant ICO guidance as part of the authorisation decision.</p>	<p>ASDE, Authorisation authority</p>
<p>18. AV cameras that collect personally identifiable information (either within or outside the vehicle) should be clearly indicated. If AVs are collecting camera data of other road users, this should be clearly indicated on the outside of vehicles.</p>	<p>ASDE, Authorisation authority</p>
<p>19. The Home Office should issue guidance clarifying how the Investigatory Powers Act 2016 applies to ASDEs and NUIC Operators.</p>	<p>Home Office</p>

## Fairness

Recommendation	Implementer
<p>20. To minimise the risk of algorithmic bias, ASDEs' safety cases and impact assessments should report on the fit between their training data and their ODDs. Substantially altered ODDs should require new reports on training data.</p>	<p>ASDE, with oversight from the Authorisation authority</p>
<p>21. Where training data distinguishes between categories of road users, e.g. between children and adults for reasons of safety, this should be acknowledged as part of the safety case and reported to the authorisation authority. Steps should be taken to anticipate and minimise unfair consequences resulting from data bias, including discrimination.</p>	<p>ASDE, with oversight from the Authorisation authority</p>
<p>22. Where systems distinguish between groups while driving, justified on the grounds of safety, e.g. the identification of children, wheelchair users or other vulnerable road users, ASDEs should have a duty to report in order to allow independent scrutiny (including, but not limited to, reporting this in the safety case).</p>	<p>ASDE, with oversight from the Authorisation authority and In-use regulator</p>
<p>23. ASDEs and NUiC Operators should facilitate independent scrutiny of emerging risks and biases (in addition to those raised by notifiable events) so that the distribution of risks can be assessed.</p>	<p>ASDE, with oversight from the in-use regulator and Authorisation authority</p>
<p>24. The in-use regulator, advised by CAVES, should collect data on fairness and safety outcomes in order to allow feedback to operators and collective learning. In the event that serious problems are identified and no other means prove effective in mitigation, the regulator should be empowered to impose sanctions, up to and including de-authorisation and product recall (cf. LC Rec. 20 - data gathering on safety).</p>	<p>In-use regulator</p>
<p>The in-use regulator should also compile evidence for where an amendment to the regulatory framework may be necessary (e.g. updates to the RR) to ensure that AVs are acceptably safe, with continual improvements in safety (see also Rec. 8).</p>	
<p>25. AV regulators should assess the potential risks of discrimination, and the adequacy of accessibility features in their authorisation and licensing decisions, in line with</p>	<p>Authorisation authority and licensing authority</p>

their Public Sector Equality Duty (cf. LC Rec. 63 - accessibility advisory panel).

---

26. ASDEs should not, as part of their SEOC, require vulnerable road users to carry or wear anything to make them more easily detectable to AVs. Should vulnerable road users decide to use such devices, however, ASDEs should not ignore their potential additional safety benefits.	Authorisation authority and In-use regulator
27. If infrastructure upgrades are required that contribute to AV safety, their costs and benefits for other road users should be fully understood and carefully balanced.	Local authorities and other infrastructure bodies; National Infrastructure Commission

---

## Explainability

Recommendation	Implementer
28. The ASDE should design the AV so that it is possible to construct an explanation of the key decisions made by the AV when it is undertaking the Dynamic Driving Task (DDT) for a bounded test scenario. These explanations should be made available as required under the duty of disclosure including, as a minimum:  a) to the authorisation authority as part of the SCR; b) to the NUiC Operator where appropriate.	ASDE, reporting to the appropriate regulator
29. For collisions, near misses and other notifiable events, the ASDE should design the AV so that it is possible to construct an explanation of the key decisions made by the AV leading up to the event, however caused. This explanation should be sufficient to identify and rectify causes of undesirable behaviours, and the ASDE should make the explanation available to:  a) a collision investigation unit for the incident being investigated; b) the in-use regulator when investigating a notifiable	ASDE, reporting to the Authorisation authority; also In-use regulator and collision investigation unit

event to potentially apply a sanction;  
c) other parties with a legitimate need for the information agreed in advance as part of authorisation (cf. LC Recs. 21, 22, 29 on incident investigation; cf. LC Rec. 74 on data disclosure).

---

## Data sharing

Recommendation	Implementer
30. In consultation with the authorisation authority, the ASDE shall publish a summary of the SEOC, which will be made publicly and freely available upon authorisation of the vehicle for self-driving.	ASDE, reporting to the Authorisation authority
31. The ASDE and NUiC Operator should communicate safety-relevant data with other organisations in the AV ecosystem when requested, including other ASDEs, the in-use regulator, the authorisation authority and the collision investigation unit, using agreed data formats, where this contributes to road safety. Data formats should be decided by the authorisation authority and in-use regulator, in consultation with the ICO.	ASDE and NUiC Operator, with oversight from the In-use regulator
a) The ASDE and NUiC Operator should share core safety-relevant data as stipulated by the in-use regulator and collision investigation unit; (note that there will be some aspects of safety-relevant data that the ASDE and NUiC Operator will be legally required to share for law enforcement purposes.) b) The in-use regulator and collision investigation unit should consult on the agreed scope and format of the core safety-relevant data they will require from ASDEs and NUiC Operators; c) The ASDE and NUiC Operator should be encouraged to share data with interested parties, using standards and formats developed via consensus; d) Regulators and the AV sector should explore the ways in which mechanisms that facilitate responsible sharing of commercially sensitive data, such as data intermediaries, could be used; e) ASDEs and NUiC Operators should explore the use of privacy-enhancing technologies such as <a href="https://cdeiuk.github.io/pets-adoption-guide/what-federated-learning-techniques">federated learning techniques</a> ( <a href="https://cdeiuk.github.io/pets-adoption-guide/what-federated-learning-techniques">https://cdeiuk.github.io/pets-adoption-guide/what-federated-learning-techniques</a> )	

[are-pets](#)), to minimise the volume of personal data that is uploaded to a centralised server.

32. The ASDE and NUiC Operator shall provide summarised safety performance data to relevant bodies including the in-use regulator to enable the safe, ethical and effective operation of the AV marketplace (cf. LC Recs. 20, 74).	ASDE and NUiC Operator, reporting to the Authorisation authority
33. The ASDE and NUiC Operator shall support reasonable access to all relevant proprietary information by a road collision investigation unit and other authorised bodies to enable collision and incident analysis and support the authorities in producing lessons learnt for dissemination to other ASDEs.	ASDE and NUiC Operator, with oversight from the In-use regulator
34. The in-use regulator shall define formats for safety-relevant data to enable sharing between relevant organisations, including ASDEs, the authorisation authority and the collision investigation unit, to ensure consistency and equity in regulation. This could be achieved via the guidance the Commissions recommend they publish on data sharing.	In-use regulator

## Public trust

Recommendation	Implementer
35. The rules on the use of terminology such as ‘self-driving’ should include requirements to inform the public about the conditions under which self-driving vehicles can operate, e.g. road types, locations, weather, other road users’ behaviour.	ASDEs, Authorisation authority and In-use regulator
36. An accessible summary of the SCR should be made public and should include clear statements of the functions and limits of an AV within an ODD.	ASDEs, Authorisation authority
37. The in-use regulator shall regularly publish publicly accessible reports on the achieved level of safety of AVs, which should include records of notifiable events and actions taken to improve safety of deployed AVs, including updates to the Road Rules. This should form part of its	In-use regulator

duty to publish evidence of AV safety, as recommended by the Law Commissions (cf. LC Rec. 19).

38. Prospective ASDEs and NUiC Operators should engage with local communities, including local authorities, when an AV trial is planned in a particular area. This engagement should inform testing and/or deployment (e.g. placing conditions on times, places, public information, maximum speeds etc).

ASDE, NUiC Operator, In-use regulator

Where the vehicle is permitted to carry passengers, the service operator should consult with relevant authorities as proposed under the Law Commissions' passenger permitting scheme.

39. Serious incidents in the operation of an AV should be publicly investigated and reported. A road collision investigation unit should have a duty to report publicly on serious incidents. Evidence gathered during the investigation should be published so that others can learn lessons.

Road collision investigation branch

40. CCAV should commission public dialogue and social research to seek public views on:

CCAV

- a) Balancing the tensions between achieving a 'safety-first culture' and ensuring sufficient accountability for the consequences of AV behaviour;
- b) The distribution of AV risks and benefits;
- c) Future changes to infrastructure and rules of the road and any associated costs;
- d) Explainability of decisions made by AVs;
- e) Labelling of vehicles.

41. Where AVs are being trialled, the safety driver should not be removed unless the vehicle is authorised, and AVs should only carry passengers where the appropriate passenger licence has been issued.

CCAV, in-use regulator and Authorisation authority

CCAV should support local authorities to monitor trials in their area (e.g. to identify significant increases in the number of vehicles involved in a trial) and to make passenger licencing decisions, for example via guidance.

42. Where an ASDE is given a limited authorisation to trial an ADS feature, the vehicle must be re-authorised should the ASDE wish to deploy the feature in a wider context.

Authorisation authority and In-use regulator



43. AVs should be clearly labelled. Where vehicles can drive themselves or be driven conventionally at different times, signals should indicate the status of operation. This external labelling should be in addition to information inside the vehicle that clearly indicates mode of operation. AV tests and deployments should be clearly publicised within and near the relevant location.	ASDEs, with oversight from the authorisation authority
44. CAVES should review and advise on the practicalities of labelling and the questions of liability raised by External Human-Machine Interfaces on AVs.	Committee on AV Ethics and Safety (CAVES)

## Governance

Recommendation	Implementer
<p>45. The authorisation authority and in-use regulator should establish a <b>joint Committee on AV Ethics and Safety (CAVES)</b> composed of experts and lay members with a diverse range of perspectives (cf. LC Rec. 30 - in-use regulator's duty to consult).</p> <p>a) CAVES should report to the Secretary of State for Transport (DfT). Since the SoS's powers will likely be delegated to the motoring agencies, in practice CAVES will advise the motoring agencies (which are themselves part of DfT).</p> <p>b) CAVES' recommendations and policy advice should be issued to DfT and the regulators in parallel for full visibility. Its reports and minutes should be public by default (recognising that some discussions will need to be held in private). CAVES should provide advice and constructive challenge to DfT. It should not make policy decisions or overrule the Secretary of State.</p> <p>c) CAVES should have a standing Road Rules Subcommittee that includes stakeholders representing different groups of road users, to provide advice on the definition of the RR, including consistency with published specifications for Automated Driving Systems (ADS), especially on ethical rules and priorities.</p> <p>d) CAVES should be constituted as a non-statutory, Scientific Advisory Committee, with diverse membership, including lay member representation (e.g. vulnerable road users).</p>	<p>Authorisation authority; In-use Regulator.</p>

Expertise should include engineering, artificial intelligence, human factors, transport planning and policy, road safety, ethics and public engagement. The committee should pay particular attention to questions of accessibility, and should include a member with expertise in disability issues (See LC Rec. 63 - accessibility advisory panel).

e) CAVES should draw on the views of a wide range of stakeholders and undertake stakeholder engagement to ensure that the needs of all classes of road users (including vulnerable road users) are considered in defining the RR and in assuring the overall governance of AVs, including authorisation and temporary restrictions of AV operations.

---

46. CAVES should have responsibility for assessing regulatory decisions, and should advise on complex issues related to the regulation and governance of AVs, such as labelling, differentiated treatment towards vulnerable road users, and explainability.

Authorisation  
authority; In-  
use Regulator.

a) CAVES should assess regulatory decisions, and provide DfT with assurance that the authorisation decision and forms of restrictions on AVs imposed by the regulators provide an appropriate alignment between innovation and safety;

b) CAVES should review and advise on the practicalities of labelling and the questions of responsibility raised by External Human-Machine Interfaces on AVs;

c) CAVES should review the desirability of appropriately differentiated treatment towards vulnerable road users, and what additional reporting duties may be required;

d) CAVES should review the degree of explainability needed for regulatory oversight.

---

## List of Abbreviations

ADS: Automated Driving System(s)

ASDE: Authorised Self-Driving Entity

AV: Automated Vehicle (in this report we use the abbreviation 'AV' to refer to self-driving vehicles)

CAVES: Committee on AV Ethics and Safety

CCAV: Centre for Connected and Autonomous Vehicles

CONOPS: Concept of Operations

DDT: Dynamic Driving Task

DfT: Department for Transport

DPIA: Data Protection Impact Assessment

DSSAD: Data Storage System for Automated Driving

DVSA: Driver and Vehicle Standards Agency

EDR: Event Data Recorder

ERA: Emergency Refuge Area

GDPR: General Data Protection Regulation

ICO: Information Commissioner's Office

LC: Law Commission(s) (here refers to the Law Commission of England and Wales and the Scottish Law Commission who are joint authors of the proposals on the regulation of Automated Vehicles)

MRC: Minimal Risk Condition

MRM: Minimum Risk Manoeuvre

NCAP: New Car Assessment Programmes

NUiC: No User-in-Charge

NUiC Operator: No User-in-Charge vehicle Operator

ODD: Operational Design Domain

PECR: Privacy and Electronic Communications Regulations

PETs: Privacy-Enhancing Technologies

RR: Road Rules

SCR: Safety Case Report

SDV: Self-Driving Vehicle

SEOC: Safe and Ethical Operational Concept

SMS: Safety Management System

UiC: User-in-Charge

UNECE: United Nations Economic Commission for Europe

VCA: Vehicle Certification Agency

VSCR: Vehicle Safety Case Report

V2I: Vehicle-to-Infrastructure

## Acknowledgments

Professor John McDermid OBE FREng (Professor of Software Engineering, University of York)

Professor Jack Stilgoe (Professor of Science and Technology Policy, University College London and Turing Fellow)

Centre for Connected and Autonomous Vehicles (CCAV)

Centre for Data Ethics and Innovation Advisory Board

Home Office

The Driver and Vehicle Standards Agency

The Information Commissioner's Office

The Law Commission of England and Wales and the Scottish Law Commission

The Office of the Biometrics and Surveillance Camera Commissioner

The Vehicle Certification Agency

- 
1. Law Commission of England and Wales and the Scottish Law Commission. [Automated Vehicles: joint report \(https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf\)](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf), January 2022. p.XVII
  2. Law Commission of England and Wales and the Scottish Law Commission. [Automated Vehicles: joint report \(https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf\)](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf), January 2022. p.XVII
  3. See Article 5(1)(c) of [UK GDPR \(https://www.legislation.gov.uk/eur/2016/679/article/5\)](https://www.legislation.gov.uk/eur/2016/679/article/5)

4. Law Commission of England and Wales and the Scottish Law Commission. [Automated Vehicles: joint report \(https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf\)](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf), January 2022. p.XVIII
5. See Law Commission of England and Wales and the Scottish Law Commission. [Automated Vehicles: joint report \(https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf\)](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf), January 2022. p.XIX
6. See Article 4(1) of [UK GDPR \(https://www.legislation.gov.uk/eur/2016/679/article/4\)](https://www.legislation.gov.uk/eur/2016/679/article/4)
7. Law Commission of England and Wales and the Scottish Law Commission. [Automated Vehicles: joint report \(https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf\)](https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf), January 2022. p.XXI
8. See Rule 204, [The Highway Code \(https://www.gov.uk/guidance/the-highway-code/road-users-requiring-extra-care-204-to-225\)](https://www.gov.uk/guidance/the-highway-code/road-users-requiring-extra-care-204-to-225), Updated 2022. Note that vulnerable road users are referred to as ‘road users requiring extra care’ in the Highway Code.
9. This supplements LC Rec. 30 - in-use regulator’s duty to engage with those with an interest in the safety of automated vehicles
10. Slovic, Paul. [Perception of risk \(https://www.science.org/doi/10.1126/science.3563507\)](https://www.science.org/doi/10.1126/science.3563507), Science, 236(4799), 280–285, 1987.
11. Liu, Peng., et al. [How safe is safe enough for self-driving vehicles? \(https://doi.org/10.1111/risa.13116\)](https://doi.org/10.1111/risa.13116), Risk Analysis, 39(2), 315–325, 2019. Note that this was a small public survey.
12. Stilgoe, Jack. [How can we know a self-driving car is safe? \(https://link.springer.com/article/10.1007/s10676-021-09602-1\)](https://link.springer.com/article/10.1007/s10676-021-09602-1), Ethics and Information Technology, 23(4), 635-647, 2021.
13. We propose that this be defined in terms of behaviours such as: keeping a safe distance from the individual or infrastructure, decelerating well in advance of stopping (as opposed to an emergency brake), mounting the pavement slowly if it is necessary and permissible to do so.
14. cf. LC Recs. 6 and 7 - safety standard; cf. LC Rec. 15 - safety case and EIA; cf. LC Rec. 20 - data gathering on safety
15. Note that we expect DfT to publish good practice on how the SMS contents should be defined in due course.
16. This implements and strengthens the LC Rec. 13 to ‘cooperate’ with the in-use regulator; it requires the ASDE and NUiC Operator to comply with any changes in operation required by the in-use regulator - for example, to change a valet parking system or to avoid routes with level crossings.

17. This is intended, with the authority as having control, to be flexible. However, it would include things like records of when rules are broken/priorities are applied as these will indicate points where there are decisions that are potentially ethically significant.
18. And minimum risk manoeuvre (MRM) should lead to a minimum risk condition (MRC); the combination is often referred to as MRX.
19. This is in line with LC Rec. 49, and the discussion of inability to respond to a transition demand due to medical emergencies, but goes further in making clear that responsibility for behaviours of the AV remains with the ASDE unless the handover to the UiC is confirmed.
20. 'Location data' under the PECR has a specific meaning, and does not include general use of network-agnostic location services such as GPS signals (although more general GDPR requirements still apply). How location data is collected and processed will affect their data protection obligations, and this is an important area for greater regulatory clarity.
21. Note that the UK government is consulting on reforms to the data protection regime: See Department for Digital, Culture, Media and Sport, [Data: a new direction](https://www.gov.uk/government/consultations/data-a-new-direction) (<https://www.gov.uk/government/consultations/data-a-new-direction>), September 2021.
22. Note that there is no explicit obligation in UK GDPR requiring the publication of DPIAs, but we consider it would be appropriate here.
23. It may not be practical for such a list to be exhaustive but would assist organisations in undertaking DPIAs, which will be needed to assess what is necessary, proportionate and appropriate in each given circumstance.
24. As above, it may not be practical for such a list to be exhaustive but would assist organisations in undertaking DPIAs, which will be needed to assess what is necessary, proportionate and appropriate in each given circumstance.
25. The 'necessary purposes' here could include, for example: responding fairly to the needs of other road users, safe operation of the vehicle and incident investigation.
26. As part of the consultation for the Data Protection and Digital Information Bill, the government consulted on proposals to simplify the oversight framework for the regulation of surveillance cameras. Following the government response to this consultation, there are now legislative proposals in parliament which, if approved, will repeal the Surveillance Camera Code and role of the Surveillance Camera Commissioner. The government is currently looking at options for continuing some of the Surveillance Camera Commissioner's ancillary functions, such as the third party certification scheme.
27. One example from Philip Koopman is of a AV system that failed to identify people in high-visibility clothing because it was unused to construction zones, which had been avoided in testing, see IEEE Computer Society, Roundtable discussion on ['Ethics, Safety, and Autonomous Vehicles'](#)



([http://users.ece.cmu.edu/~koopman/pubs/koopman21\\_Ethics\\_Safety\\_AVs\\_IEEE\\_Roundtable.pdf](http://users.ece.cmu.edu/~koopman/pubs/koopman21_Ethics_Safety_AVs_IEEE_Roundtable.pdf)), 2021.

28. A recent European Commission report on the ethics of AVs argued for appropriately differentiated treatment towards vulnerable road users. See European Commission, [Ethics of Connected and Automated Vehicles](https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search) (<https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search>), 2020.
29. It is notable, for example, that Uber ATG's fatal collision in Arizona in March 2018 was in part due to a classification problem caused by a pedestrian, outside a pedestrian crossing, pushing a bicycle across a road. See National Transportation Safety Board, [Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian](https://www.nts.gov/investigations/accidentreports/reports/har1903.pdf) (<https://www.nts.gov/investigations/accidentreports/reports/har1903.pdf>), Accident Report NTSB/HAR-19/03, 2019.
30. Note that these impact assessments should consider impacts on relevant protected characteristics as set out in equality law, but the assessments should also cover impacts on vulnerable road users.
31. Note that in recommendation 49 on CAVES, we recommend that CAVES should review the desirability of appropriately differentiated treatment towards vulnerable road users, and what additional reporting duties may be required.
32. See Rule 204, [The Highway Code](https://www.gov.uk/guidance/the-highway-code/road-users-requiring-extra-care-204-to-225) (<https://www.gov.uk/guidance/the-highway-code/road-users-requiring-extra-care-204-to-225>), Updated 2022.
33. The case for independent scrutiny to evaluate AI systems is in: Falco, Gregory., et al. [Governing AI safety through independent audits](https://www.nature.com/articles/s42256-021-00370-7) (<https://www.nature.com/articles/s42256-021-00370-7>). Nature Machine Intelligence 3, 566–571, 2021.
34. LC paragraph 3.44
35. This follows a recommendation from the European Commission expert group report on the ethics of connected and automated vehicles. See European Commission, [Ethics of Connected and Automated Vehicles](https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search) (<https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search>), 2020.
36. Macrae, Carl. [Learning from the failure of autonomous and intelligent systems: accidents, safety, and sociotechnical sources of risk](https://onlinelibrary.wiley.com/doi/10.1111/risa.13850) (<https://onlinelibrary.wiley.com/doi/10.1111/risa.13850>). Risk analysis, 2021.
37. Note that another aspect of explainability is that of explaining what is likely to happen in the future. This is covered in Rec. 5 which requires ASDEs to define a SEOC that would set out how the AV is intended to achieve safe and ethical behaviour.
38. See for example the forthcoming IEEE standard on transparency (Winfield, Alan FT, Serena Booth, Louise A. Dennis, Takashi Egawa, Helen Hastie, Naomi Jacobs, Roderick I. Muttram et al. [IEEE P7001: a proposed standard](#)



on transparency (<https://www.frontiersin.org/articles/10.3389/frobt.2021.665729/full>), Frontiers in Robotics and AI, Volume 8, 225. 2021) and ISO/IEC NP TS 6254 (<https://standardsdevelopment.bsigroup.com/projects/9020-04875#/section>)

39. Herkert, Joseph, et al. [The Boeing 737 MAX: Lessons for engineering ethics](https://link.springer.com/article/10.1007/s11948-020-00252-y) (<https://link.springer.com/article/10.1007/s11948-020-00252-y>). Science and engineering ethics, 26(6), 2957-2974. 2020.
40. Any framework for certification should acknowledge the possibility of incentives towards cheating, as revealed by the VW 'dieselgate' controversy.
41. Tyndall, Justin. [Pedestrian deaths and large vehicles](https://www.sciencedirect.com/science/article/abs/pii/S2212012221000241) (<https://www.sciencedirect.com/science/article/abs/pii/S2212012221000241>). Economics of Transportation, 26, 100219. 2021.
42. Note: this recommendation is broader than the requirements set out in LC Recs. 20 and 57.
43. See for example, LC Rec. 74, which establishes a legal basis for data disclosure on AV data controllers.
44. Note that this aligns with the Law Commissions' recommendation that the ASDE must cooperate with an investigation unit as much as the regulator.
45. Tennant, Chris et al. [Driverless Futures? A Survey of the British Public](https://driverless-futures.com/2022/05/09/survey-reports/) (<https://driverless-futures.com/2022/05/09/survey-reports/>), (2022). Driverless Futures? was a three-year social science project (2019-2022) funded by the Economic and Social Research Council, with researchers from University College London, UWE Bristol and City, University of London. See also Department for Transport, [Transport and transport technology: public attitudes tracker](https://www.gov.uk/government/publications/transport-and-transport-technology-public-attitudes-tracker) (<https://www.gov.uk/government/publications/transport-and-transport-technology-public-attitudes-tracker>), 2021 (seven iterations since 2018).
46. A recent US survey from J.D. Power found that 19% of people thought fully self-driving vehicles were already available to buy. When prompted for more information, 'Tesla' was the most commonly used word by survey respondents. See J.D. Power, MIT Advanced Vehicle Technology Consortium, Partners for Automated Vehicle Education (PAVE), [Mobility Confidence Index Study](https://www.jdpower.com/business/press-releases/2021-mobility-confidence-index-mci-study) (<https://www.jdpower.com/business/press-releases/2021-mobility-confidence-index-mci-study>), 2021.
47. This expands on LC Rec. 23 - info to owners and UIC and LC Rec. 34 - criminal offence on terminology
48. This could be addressed by the Government led AV-DRiVE group.
49. This supplements LC Rec. 30 - in-use regulator's duty to engage with those with an interest in the safety of automated vehicles
50. Note: Recommendation 33 states that the ASDE and NUiC Operator shall support reasonable access to all relevant proprietary information by a road collision investigation unit and other authorised bodies to enable collision and incident analysis and support the authorities in producing lessons learnt for dissemination to other ASDEs.

51. Prior to the commencement of the future framework, listing under AEVA 2018 would be the appropriate alternative.
52. Where AVs are being trialled only, and have not been authorised, trialling organisations should implement this.
53. This would implement the Law Commissions' recommendation for a 'Road Rules Forum' (LC Rec. 31).

[↑ Back to top](#)

---

## **OGL**

All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright