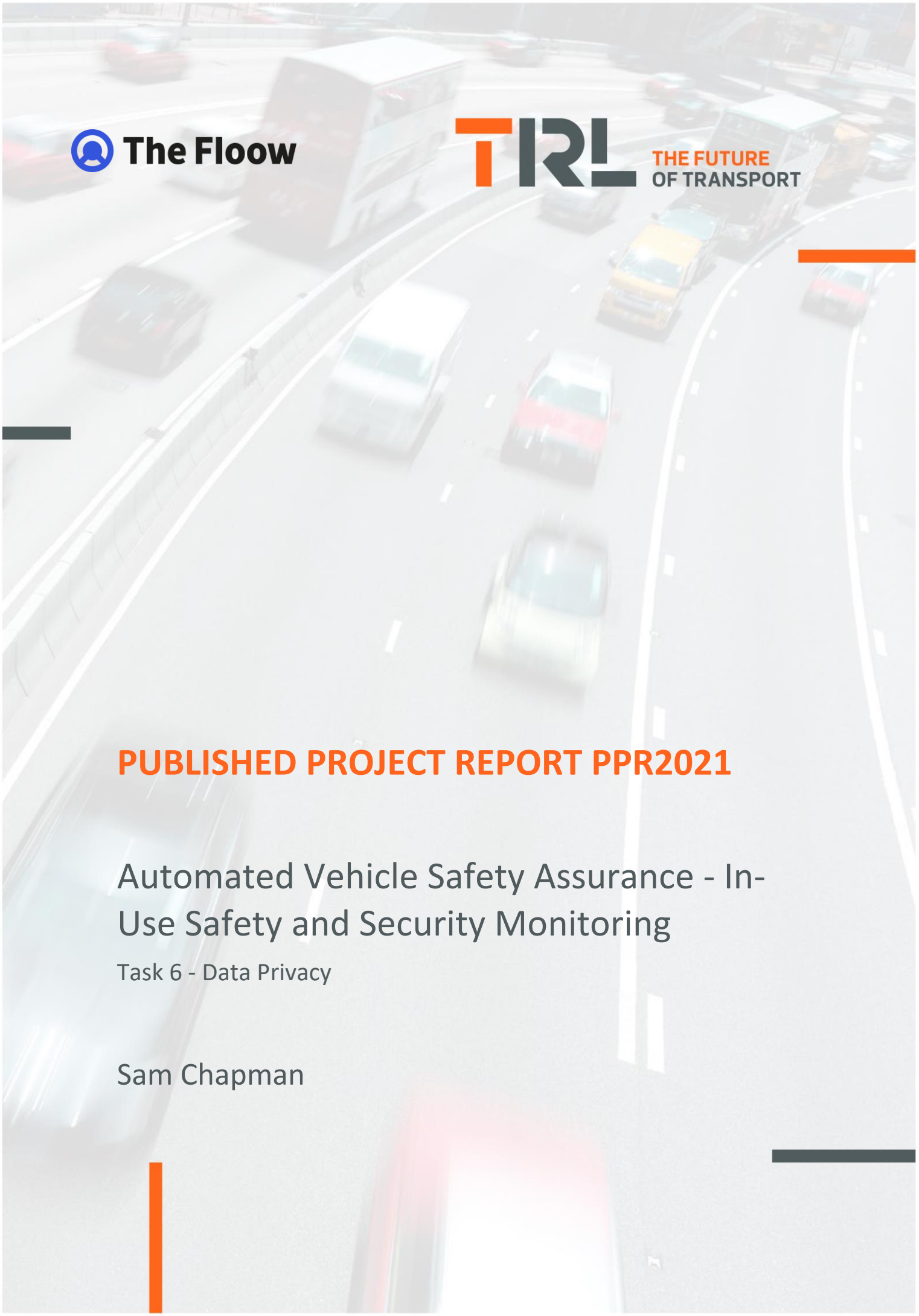

The Floow

TRL THE FUTURE OF TRANSPORT

PUBLISHED PROJECT REPORT PPR2021

Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring

Task 6 - Data Privacy

Sam Chapman

Report details

Report prepared for:	Department for Transport		
Project/customer reference:	TETI0042		
Copyright:	© 2021 The Floow Limited		
Report date:	30/06/2023		
Report status/version:	1.0		
Quality approval:			
Gareth Slocombe (Project Manager)	G. Slocombe	David Hynd (Technical Reviewer)	D. Hynd

Disclaimer

Executive Summary

This report develops data privacy recommendations for Automated Vehicles (AVs). AVs in operation will gather and process significantly more data than traditional human controlled vehicles therefore requiring new regulation and guidance on the data they handle. Each vehicle should have: extensive sensor arrays, advanced processing, object detection, trajectory estimations, data storage and transmissions. Each vehicle primarily gathers and processes data to enable automated mobility however data gathered must also support wider management, monitoring and enforcement (e.g. in-use safety compliance monitoring) and recording data for research and improvement of safe automated services. This data originating from AVs can include personal data related to passengers, other vehicles and also vulnerable road users when within sensor range during operation.

To ensure data protection and privacy it is vital to consider not just vehicle owners and occupants but also third-party vehicle owners and individuals that may feature in gathered data. In these cases, strong data protection consideration is essential. This document reviews:

1. the current legal framework for AVs and data protection
2. the data gathered by AVs and its data protection sensitivity
3. data protection recommendations for AVs

The following recommendations regarding data privacy have been made:

Table 1: Data privacy recommendations for AV safety assurance scheme

No.	Recommendation
1	The AV operator and manufacturer **must** ensure valid open grounds ('lawful basis') for collecting and necessary processing of any personal data. This follows the principles of GDPR Art 5(1) (a) recommending in particular that the operator declare data gathering for: Safety analysis, including in-use data collation and post-incident analysis, to support compliance and regulator-based monitoring.
2a	The AV operator and manufacturer **must** follow GDPR good practice and maintain clear historic and up-to-date records regarding types and classes of gathered data during AV operation.
2b	Such records **must** be provided to the authorised automated vehicle regulator (or other recognised legal authority) upon instruction or request to do so.
2c	This record **must** include as a minimum: • brief data descriptions of gathered data types/classes, • indications if each may contain personal data or if fully anonymised at point of gathering, • descriptions of potential PII within each data type/class, • indication of consent mechanisms and who they apply to for any data type/class of gathered data,

	• indication of any PII that are potentially gathered without explicit consent, i.e. those that are gathered due to necessary and proportionate data gathering needs (e.g. external facing video to maintain safe operation), and • the retention period of each data type.
2d	The Regulator **could** provide guidance to help normalise data within such records to help standardise and understand available data gathered.
3	The LSAV operator and manufacturer **must** make available to the authorised in-use autonomous vehicle regulator upon request its record of data gathered (as detailed above)
4a	The LSAV operator and manufacturer **must** make public and transparent via open publication all data gathering purpose(s) involving 'personal data' to make transparent the purpose(s) and extent of its AV data gathering. (This follows GDPR Article 5(1)(b) to ensure 'purpose limitation' in data gathered.)
4b	A declared purpose **must** contain "data gathering and processing to support in-use and post-incident data provision for regulators and compliance checks".
5	The LSAV **should** (where possible) anonymise external sensor data upon collection to remove PII (following good practice and principles of GDPR article 25). E.g., camera footage blurring faces or number plates. If not possible, AV operators **must** show justified, necessary and proportionate need for gathering such data (i.e., in order to ensure safety or other fundamental needs[1]).
6	The Regulator **should** provide guidance to maintain leading, lagging and continuous 'in-use' data from LSAVs as required with suitable protections and security for a period of 7 years[2].
7a	The LSAV operator (or any other holder of in-use vehicle data) **must** be required to follow industry leading accredited practices for data protection and security. E.g. following ICO guidance on digital service security including compliance with international audited standards like ISO 27001, monitoring and auditing, incident handling and system security to maintain strong data protection.
7b	These approaches **must** maintain a Data Privacy Impact Assessment (DPIA) process and output records which are reviewed via third-party audit annually (or more frequently) covering all the data gathered and processed for LSAV operation.
7c	It is recommended that LSAV operators and manufacturers should have good cybersecurity measures in place, notably third-party penetration (Pen) testing of its systems as part of its process testing.

[1] Gaze detection may be helpful to understand vulnerable road user behaviours and reduce operational risk. In such instances efforts should still be made to remove PII after such analysis and ensure only permitted processing for any such data.

[2] See section 2.1.2.5 for discussion on retention periods and why this period is suggested.

8	It is recommended that LSAV developers in control of vehicle data gathering **should** (where possible) also apply point of gathering anonymisation to property or household data (if gathered) to the same extent as GDPR personal data. This aims to provide protection for property owners and data about properties ensuring protection beyond GDPR. This follows approaches within California and China that consider such protections and ensure protection related to property and address point information with specific regard to remote vehicle data gathering.
9	The Regulator **could** review "Provisions on the Management of Automobile Data Security"[3] to consider if wider protective controls for gathering data in sensitive regions or data reuse could require wider regulation.
10	The LSAV operator **should** ensure clear separation and processing controls regarding any PII data in relation to data that may classify 'protected characteristics' of individuals. These include object recognition that may for example identify children and wheelchair users separately to other vulnerable road users to help safety analysis and enable road rule compliance checks related to specific protected classes of individuals.
11	The LSAV operators **should** use pseudonymisation where possible to minimise data protection risks (following data protection good practice).
12	The Home Office **should** provide guidance for the application of both RIPA2000 and IPA2016 in regard to LSAVs. This will remove ambiguity about the potential need to supply such data from such vehicles, which is currently uncertain.
13	The Regulator **should** make clear the legal ownership of 'in-use' gathered data and provide guidance for the terms for its access. This may follow the approaches of the Federal Driver Privacy Act 2015 (US), to protect misuse of gathered data. Clear indication of legal owner (as well as who has access) is required and could provide additional protection to the public.
14	The LSAV operator **must** use suitable signage on vehicles to indicate to external individuals that recording may occur – following the latest Surveillance Camera Code of Practice (2022).
15	The LSAV operator **must** provide a clear public-facing contact means for data protection or surveillance recording-related queries or concerns from members of the public.
16	The LSAV operator **must** provide clear public facing indications of data retention related specifically to surveillance camera footage captured internally or externally to the vehicle. 'According to the UK GDPR requirements, any retention of data beyond 31 days must be declared with clear purpose and necessity for the data gathered beyond this period.

[3] Chinese Language version of these provisions are available at http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm

List of Figures and Tables

Tables

List of Abbreviations

ABS:	Anti-Lock Braking System
AEVA:	Automated and Electric Vehicles Act
ANPR:	Automatic Number Plate Recognition
APPI:	Act on the Protection of Personal Information
AV:	Automated Vehicles
CCPA:	California Consumer Privacy Act
CCTV:	Closed Circuit Television
DfT:	Department for Transport
DPA:	Data Protection Act
DPIA:	Data Privacy Impact Assessment
EA:	Equality Act
GDPR:	General Data Protection Regulation
GPS:	Global Positioning System
HRA:	Human Rights Act
ICO:	Information Commissioner's Office
IPA:	Investogatory Powers Act
PIPEDA:	Personal Information Protection and Electronic Documents Act
PIPL:	Personal Information Protection Law
POA:	Public Order Act
PoFA:	Protection of Freedoms Act
RIPA:	Regulation of Investigatory Powers Act
UDHR:	Universal Declaration of Human Rights’
VRU:	Vulnerable Road User

1 Introduction

Low Speed Automated Vehicles (AVs) will commonly be operated in slow mixed-mode urban streets encountering diverse road users. This outline operating environment [4] adds a fundamental requirement for exacting safety practices requiring AVs to gather, process and share pertinent aspects of data to help ensure increasingly safe operation. Differing and conflicting concerns exist, however, for differing stakeholders. These primary concerns are summarised in the following table.

Table 2 - Data protection primary concerns of differing stakeholders

Role	Concerns
AV Passenger	Fundamental rights to privacy being maintained (surveillance and profiling) – especially with increased presence of inward sensors, audio, video and user location tracking and profiling.
AV Manufacturer[5]	Maintaining rights for legal access to necessary and proportional evidential data to handle liability claims. Legitimate needs for usage monitoring to support authorised in-use regulators and internal monitoring of operational risk and any mitigations. To enable support for safety validation and analysis to help inform and improve future safety solutions.
AV owner	Gathering proportionate and minimised usage data to understand, protect and monitor high value commercial assets. This has legitimate interest in a vehicle's: geo-position, usage, and operational state information.
AV operator	Has legitimate need for in use of operational data to support analysis for operational and service improvements, potential maintenance needs.
AV System developer	Proprietary intellectual property protection seeking to minimise exposure of trade secrets and specific sensor and related data concerning its AV system. Rights to gather technical and sensor data to support system checks and enable new improvements.
Regulator	Fundamental rights to safety information to obtain necessary data to support in-use monitoring and operational risk analysis, type approval and incident forensics.
Public	Fundamental rights to privacy for unconsented individuals (surveillance) – especially external video surveillance and object tracking requiring only minimal fair and proportionate gathering or processing of such data.

[4] That may well be formally expressed by a declared ODD (Operational Design Domain).

[5] Please note that AV roles may be combined in a single entity, e.g. owner/operator; these would combine data protection key concerns.

Role	Concerns
Property owner	Interest to adequately protect property privacy that can be influenced via third-party data influencing property value.[6]
Police/court/ legal/governmental	Rights to access specific data to support incident analysis, criminal cases, investigative work or potential national security needs.
Road Authority	Interest to understand road asset usage and environmental data.
Health and Safety Executive	Fundamental rights to safety within physical and remote workplaces that may require exemption from privacy rights to maintain data for safe working.
Information Commissioners Office	Providing guidance to support good practice for data protection and to act as UKs data privacy regulator.
AV Insurer	Interest for data access supporting informed liability determination and incident damage extent.

These concerns regarding safety-pertinent data from AVs are discussed in wider deliverables (WP5 Tasks 2, 3 and 4) but this document focuses upon where data privacy regulation either already applies or requires guidance to its application with AV usage. The regulation is detailed in section 2 and how this applies to both in-use and post-incident data is detailed in Section 3, followed by recommendations in Section 4.

[6] This is not a core protected characteristic in UK legislation unless data is also related to identified individuals related to a property; however, other countries actively regulate and protect the rights of data about legal property separately. Surveillance of property and gathering of data may need guidance for data protection given the ability for mobile sensing to gather data for mass properties.

2 Current legal frameworks relevant to AVs

Legal protection of privacy follows the 1948 United Nations General Assembly adopting the rights and freedoms of human beings. This 'Universal Declaration of Human Rights' (UDHR), although not legally binding, set out guiding principles on fundamental freedoms. Only two years later, in 1950, the Council of Europe drafted their European Convention on Human Rights (ECHR) adding these principles into law. ECHR added new 'privacy' protection (article 8) as a fundamental right such that protections would flow into any new laws that followed. Following this, wider laws incorporated data privacy and protections (e.g. Sweden's 1973 'Data Act', a world first focused data privacy law). In the UK, its similar 'Data Protection Act' of 1984 established UK's first data privacy law but this was later replaced alongside many countries each aligning to a single enhanced framework. This was enacted with an updated Data Protection Act 2018 that supported new UK alignment to the EU's General Data Protection Regulation. Before this general regulation, however, concern had already been raised about privacy related to automated vehicles to understand its implications in new law. In 2016, EU member states signed the Declaration of Amsterdam which agreed specific agendas to protect data privacy in relation to automated vehicles. This consensus to align protections for automated vehicles was adopted later in 2017[7] to ensure adequate protection under generalised data protection regulation.

Despite this protection, the right to data protection is not an absolute right – it requires balancing alongside other intrinsic and fundamental rights and support for wider legal processes. With regard to automated driving, the need to ensure legal investigation and safety can prevail, given specific needs, over the right to data protection. For this reason, several aspects of protection in respect of AVs need careful consideration. The laws, regulation and guidance currently relevant to data protection in respect of AVs in the UK are now detailed.

2.1 Data protection regulations

Data protection regulation globally seeks to provide legal protection to individuals regarding access, consent and extent of personal data processing. Summaries of relevant global regulations are detailed below as well as how they may impact the capture, storage and processing of in-use monitoring data.

2.1.1 Data Protection Act 2018 (UK)

The Data Protection Act 2018 includes the UK implementation of the General Data Protection Regulation (GDPR), see following section. This law defines the core 'data protection principles' of UK's GDPR, ensuring information is:

- used fairly, lawfully and transparently;
- used for specified, explicit purposes;

[7] This Resolution on Data Protection in Automated and Connected Vehicles was adopted in the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong in 2017.

- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary; and
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

This adds explicit legal protection for declared 'sensitive information', such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are also separate safeguards for personal data relating to criminal convictions and offences specifically aligned to related UK legislation. The Act establishes rights for legal persons including rights to:

- be informed about how your data is being used;
- access personal data;
- have incorrect data updated;
- have data erased;
- stop or restrict the processing of your data;
- data portability (allowing you to get and reuse your data for different services); and
- object to how personal data is processed in certain circumstances.

These priciples, protections and rights relate to AV manufacturers and operators. To understand these better, GDPR (and UK's implementation of it) is now discussed when relevant to AVs.

2.1.2 GDPR

The General Data Protection Regulation is a model regulation with wide international alignment. It has inspired and aligned legislation in Argentina, Brazil, California, Canada, Chile, Japan, Kenya, Mauritius, South Africa, South Korea, Turkey and others. This regulation contains provisions on processing and handling of personal data of individuals[8] to provide legal protections for the right to privacy aligned to the ECHR fundamental human rights (see section 2). The law is formed into chapters covering:

- general provisions;
- principles;
- rights of the data subject;
- duties of data controllers or processors;

[8] Sometimes known as 'data subjects'.

- transfers of personal data to third countries;
- supervisory authorities;
- cooperation among member states;
- remedies;
- liability or penalties for breach of rights; and
- miscellaneous final provisions.

Within these, a number of articles define legal rights to gather, process and share data. Some of these articles have particular importance to AVs so are discussed below.

2.1.2.1 Lawfulness, fairness and transparency principle (Art. 5 (1) (a) GDPR)

The AV data controller[9] must ensure valid open grounds ('lawful basis') for collecting and fairly processing personal data.

The AV data controller must ensure that vehicle-gathered data meets the classification of 'personal' or not. This must include positional information of a data subject and imagery of faces or number plates to be considered personal data. It is recommended however that a register should be used to track all gathered data and specify whether it is personal or not. This register should list both personal and non-personal data gathered so that regulators or investigator authorities can easily understand the outline extent of data gathered that may support in-use incident investigation and analysis beyond its applicability to data protection.

If gathered data is personal, it must be supported with a lawful basis to enable data capture or processing. These are:

1. **Explicit granted consent** from the subject of any personal data collection. This cannot apply to third party motorists or vulnerable road users but can apply to passengers if records of consent for data gathering are maintained.
2. **Supporting contractual obligations** entered into by data subjects. This may apply to passengers and operators of a low-speed autonomous vehicle when agreeing contracted mobility services with explicit declaration and agreement of gathering and processing consent for required personal data.
3. **Legal Obligation** for a data controller to apply to any common or statuary law that may require data processing, for instance to support the requested needs of the Investigatory Power Act 2016.
4. **Vital Interest** to make available necessary personal data to help protect life from immediate harm, e.g. to provide emergency data necessary for vital medical care as per GDPR Article 46.
5. **Public Interest** where data gathering and processing would support functions and powers that are set out in law or perform specific tasks in the public interest that are set out in law. Given legislation data gathering and processing could be judged to be in the public interest with regulatory support. For LSAV operation this would however more likely be judged as legitimate interest however (see below).

[9] The manufacturer or operator, for instance.

6. **Legitimate Interest** where data can be processed when meeting three clear checks. 1) having a legitimate interest, i.e. a shared purpose that the data controller and importantly the wider public have in common (such as maintaining fundamental rights to safety and safe operation). 2) where data gathering and processing is necessary and proportionate[10] (processing of external sensor data to enable understanding of risk) and 3) ensuring the legitimate rights of individuals are protected (such as the fundamental right to safety and supporting processing that prevents impacts on the right to privacy). Any data gathering using this lawful reason must be made clear to both consented passengers and the public The AV operator and manufacturers may want to provide clear vehicle signage indicating data gathering is being undertaken transparently and also should each maintain dedicated Legitimate Interest Assessment records (LIA) to record its lawful rights.

2.1.2.2 Purpose limitation (Art. 5 (1) (b) GDPR)

AV vehicles will be enabled by a large extent of data gathering; however, data gathered must be 'proportionate' to the needs and not greater than is required to minimise privacy concerns and risks. Data, however, is required for:

- In-use monitoring, regulatory and safety compliance checks (see Section 3);
- Post-incident forensic analysis;
- Safe operation to enable AV informed decision making; and
- Improving future AV decision making and operations[11].

These aims must be clearly recorded in data impact assessments and expressed in privacy notices before data gathering is undertaken. Any use of data outside of any prior declared purposes would a breach of declared purpose. This point is relevant for LSAVs especially in early development and deployments where data will be required to both refine operation and support in-use monitoring. It is therefore essential that declared purposes include the above declared purposes.

2.1.2.3 Data minimization (Art. 5 (1) (c) GDPR)

AVs should not collect excessive data beyond those that are necessary for the declared purposes (see above). For the purpose of in-use monitoring and post-incident analysis, required data can be declared as detailed in WP5 Tasks 2, 3 and 4, (a review of the minimum dataset is included in Section 3; however, 'by design' they minimise data to factors that are strictly required in order to meet GDPR requirements).

[10] For data to be 'necessary and proportionate' it draws on the fact that data protection is not an absolute right. It requires balancing alongside other intrinsic and fundamental rights (for instance in CCTV law providing protection, safety and legal evidence). With regard to AVs, similar necessity can prevail for data gathering given the specific need to ensure in-use monitoring, road safety and legal operation of vehicles.

[11] This may include input and training data to enhance machine learning and deep learning Artificial Intelligence systems so as to ensure optimal and unbiased operation of algorithms.

For the vehicle operator and developers, however, additional data volumes may need to be declared. Research in the field of AVs being related to machine learning depends upon the collection and availability of large amounts of data to deliver improvements. This data (particularly in the form of 'video surveillance' camera data) may include personal data. The operator must constrain the extent of gathered data to that which is 'adequate, relevant and limited' for undertaking this purpose. In the case of external sensors operators are strongly advised to remove personal data at source where possible (e.g. blur the faces and number plates in recorded and persisted data) to minimise personal data.[12]

2.1.2.4 Accuracy (Art. 5 (1) (d) GDPR)

GDPR requires that data collected must be accurate and kept up to date; however, in the case of AVs, raw sensor data, object detection and machine learning labelling of data may have imperfect accuracy. This may include personal data referring to vehicles or vulnerable road users whereby data could be personal but also be imprecise or incomplete allowing individuals to ask for data corrections. This risk is amplified considering simple traffic scenarios where many individuals may be identified[13] and with occlusions in sensor visibility and raw sensor inaccuracy can present incomplete and potentially inaccurate data about individuals.

AVs are considered to have a 'necessary and proportionate' need to gather such data as it is necessary for their operation, but it is possible to anonymise potentially personal data to avoid vehicle operators being required to correct records.[14] This again places clear requirements upon data gathering to minimise personal data collection where possible at source by design (following the principles of GDPR article 25). Recommendations for this are covered later in Section 2.2.5.

2.1.2.5 Storage limitation (Art. 5 (1) (e) GDPR)

GDPR requires that personal data shall be "kept for no longer than is necessary for the purposes for which the personal data are processed". This may give differing lengths of time for differing purposes and a minimum for each should be selected. Each of these is now detailed with recommended retention periods.

In-use regulator compliance monitoring data, may be used to support leading metric risk analysis without realised risk events. This data by its design (following the principles of GDPR article 25), aims to contain minimal personal data to minimise risk. This allows as needed longer term data storage with minimal impact to data holders so as to enable longer term safety analysis and compliance tracking. This is enabled as it contains information about the ego-vehicle's observed behaviour with its operation in context of the wider surroundings and

[12] More is detailed later in this document regarding camera surveillance data in Section 2.2.5.

[13] For example in a crowd crossing in front of the AV entering into a place of entertainment.

[14] This follows GDPR Article 26 which encourages "data made anonymous in a way that the subject is no longer recognizable".

objects without identifiable data for wider objects. This enables minimal 'necessary' data for compliance checks and road safety analysis without including personal or protected data.

- Data retention is recommended for a period of **seven years** to:
    - Enable long term analysis and change tracking to ensure compliance change is positive over statistically relevant periods of time.
    - Enable required road safety analysis with sufficient evidential data. Instead, if limiting the time period for retention, less data would be available limiting the potential of road safety analysis and validation of leading risk metrics.
    - Fit the needs of insurance, police, regulatory authorities and courts for potential investigation and understanding of either individual or similar incidents. For insurance regulation this has explicit legal timeframes where damage but not personal injury should be maintained 6 years plus 1 year investigation time. It should be noted that DSSAD data retention recommendations from the UK Law Commission[15] recommend 39 months from the date that it is recorded. This is to cover standard three-year limitation periods for personal injury claims and an extended period to process data if occurring at the very end of the claims period. This three-year limitation relates only to personal injury; however, in-use regulators may be concerned with leading metric risk analysis and damage other than personal injury which requires longer storage which is why it is recommended to cover seven years of data retention.
- It should be noted that a regulator may not seek to hold such data for this period but may seek instead to ensure allowable access over such a timeframe given need for road safety or regulator-related processing.

For post-incident analysis monitoring following a realised risk incident, a retention is suggested to match the needs of potential incident liability including any legally enforceable period[16].

- In-use data may have 'required' usage related to vehicle-related insurance claims or legal investigation implying a **seven-year** retention period should be followed to align to the insurance sector.

This suggestion follows that the data could be 'necessary' for handling in-use incidents when related to insurance claims following similar retention periods for similar data. The size and data elements proposed for in-use monitoring are sufficient that longer term storage is practical.

[15] The following review presents a view of the data retention period for DSSAD in-use data "EDR-DSSAD-04-04 Consolidated Review of Contracting Party DSSAD Activities & Way Forward Rev 8" indicating a regulatory need for a minimum of 39 month in-use data retention.

[16] This time period of 7 years matches insurance practices and regulations when gathering in-use data where data can be persisted for a period of 7 years.

In the UK there is no specific statutory limitation period for making claims under an insurance or reinsurance contract. However, insurance contracts are subject to a normal limitation period under the 'Limitation Act 1980'. This suggests that data could be needed for differing periods depending upon the type of legal action possible. These include:

- Simple claims in contract or tort (excluding personal injury): six years.
- Fraud: six years.
- Negligence (in respect of latent damage): three years or six years, subject to a maximum period 15 years from the negligent act or omission.
- Personal injury: three years.

The period of seven years includes a year, to handle claims or investigations plus a period of six years to ensure availability of data to cover: damage, negligence, fraud and full coverage for personal injury.

- **For safe operation to enable decision making**, this data is needed for decision making in an instance therefore may represent data held **ONLY** in the vehicle for the purpose of immediate decision making. Such data has no recognised purpose for retention after the decision is made so by purpose definition must not retain data after needed. This can be set with a minimal retention figure as required by the vehicle operator and available on vehicle storage but is expected to be very short, e.g. **much less than an hour** but can be set following operator needs to enable specific scenario-based data capture to help improve systems (see following).
    - This data may contain proprietary information beyond that shared for in-use compliance monitoring and may well contain Personally Identifiable Information (PII) as the operator may be permitted within its declared and legitimate interest processing.
- **For improving future AV decision making and operations**, this data retention should be set to the minimum period required by the vehicle operator to provide means for enabling system monitoring, enhancement and improvement. This period could extend to **a few years** but should be set as short as possible to enable system enhancements without unneeded data persistence. AV operators should also be aware of the purpose this data is maintained to ensure only clear allowable processing to be performed using this data.

2.1.2.6 Integrity and confidentiality (Art. 5 (1) (f) GDPR)

GDPR requires that personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". This places strong requirements for AV data controllers. This will place requirements on any data holder or recipient of collated data.

It is recommended that strong best practice in data storage and handling is followed with organisational adoption of ISO 27001 policies and tested practices. Such processes and

practices should follow strict DPIA (Data Protection Impact Assessments)[17] and be subject to regular review and third-party accredited auditing.

2.1.3 CCPA (California)

The California Consumer Privacy Act (CCPA) is a US standard for data protection similar, but different, to GDPR. Although only applicable in California, this act has strong adoption across the wider US for products and services deployed nationwide. This includes a growing alignment to Federal Trade Commission guidance.[18] By extension this has implications for automated vehicles which are frequently produced for the global market. One of the key differences for the CCPA compared to GDPR of relevance to AVs is its scope of application. GDPR deals with 'personal data' of an 'individual' whereas CCPA instead extends this scope to include households and data about households independent of the individual. This places potentially added concerns for automated vehicles that may collect data not just about individuals but also properties they pass. It is recommended for AVs that this broader definition also be considered to ensure international interoperability and protections of property owners. This may mean AVs would be required to anonymise or ensure the safe handling of data about the properties that a vehicle passes as well as anonymising personal data linked to individuals.

2.1.4 Personal Information Protection Law - PIPL (China)

In November 2021, China adopted its own privacy law with alignment to GDPR.[19] This law is similar to GDPR in many ways, but it extends the definition of sensitive and protected data to include 'any' information which may cause harm to an individual if it is leaked or illegally used. This wider coverage will then potentially require additional anonymisation (i.e. not just of faces, number plates and obtained personal data but could be extended to any information that could be connected to individuals). For AVs, PIPL provides no specific guidance to automated vehicles. However, a raft of wider legislation is now aimed specifically at automated and connected cars; of note is the "Provisions on the Management of Automobile Data Security"[20]. These new provisions strengthen the data security aspects beyond GDPR and PIPL giving firm guidance to automated vehicle manufacturers and operators into strict handling regarding data protection and security. These terms add not only PIPL "personal data" but also "sensitive personal data" and "important data" definitions in relation to

[17] Following the guidance of GDPR Article 35.

[18] Six other states are adopting similar legislation before 2023, Virginia and Colorado both following the CCPA Act drawing a wider US consensus of data protection and privacy.

[19] A translated version of this law is available via US, Stanford University at: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

[20] Chinese Language version of these provisions are available at: http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm

automated vehicles. These legal extensions aim to support national security, safety and public interest from in-vehicle data.[21] These include specific provisions for data related to:

- Data on the flow of individuals and vehicles in sensitive areas such as military management zones, national defence science and industry units involving state secrets, and party and government agencies at or above the county level;
- Surveying and mapping data higher than the accuracy of the publicly released maps of the state, to mandate sharing of data for public interest when permitted;
- Data on traffic including vehicle type and flow data, such that it can be shared;
- Operating data supporting car charging network optimisations;
- Guidance on the handling of audio and video data including faces, voices, license plates, etc.; and
- Data that may affect national security and public interests as specified by the State Cyberspace Administration.

2.1.5 Personal Information Protection and Electronic Documents Act - PIPEDA (Canada)

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) came into effect in 2001, many years before GDPR. This is highly aligned to GDPR but has distinct differences of relevance to AVs. Protected data is loosely defined as 'data that a reasonable person may consider appropriate'. This gives an approach whereby, like PIPL, added caution is required not just on specific protected features. Current precedent in Canada on PIPEDA embraces particularly strong protection related to any data recording relating to children including, by extension, any video from vehicles. To maintain international alignment, it is especially advised for AVs to consider anonymisation in data concerning children or other protected individuals[22] as a priority.

2.1.6 Act on the Protection of Personal Information - APPI (Japan)

Japan's Act on the Protection of Personal Information (APPI) was established before GDPR in 2003 but with application in 2017 and strong amendment in 2020. This being the first general data protection legislation within Asia, it set a model that other countries in the continent follow. This follows similar approaches to GDPR but has, like other international law, notable differences applicable to AVs. Unlike GDPR, this has no concept of data controllers or processors indicating instead legal protections all must follow when processing 'commercial' data. Also, APPI places little restriction on profiling provided there is informed consent to do so. The recent 2020 amendments to the act place strong emphasis on using pseudonymised data where possible to support machine learning, AI and data exchanges[23]. These additions

[21] An English Language review of these documents and what they contain is available at: https://fpf.org/blog/china-new-draft-car-privacy-and-security-regulation-is-open-for-public-consultation/

[22] Such as the elderly or disabled.

[23] Pseudonymised data is still personal data but mitigates privacy risk by replacing identifying data with artificial identifiers instead – e.g. hashing of observed vehicle registration plates that without the use of additional

provide regulation applicable to AVs where personal data can be protected by pseudonymisation. These changes once again require minimising personal data wherever possible and reinforce the need to undertake this task for international alignment.[24]

2.2 Other Laws (beyond general data protection)

As well as generalised laws for data protection, a large number of other laws are relevant to AVs. These laws are detailed briefly below. The focus remains on the UK legislative landscape, but international examples are used where relevant.

2.2.1 Human Rights Act (HRA 1998) – UK

The Human Rights Act follows Article 8 of the European Charter of Human Rights which encodes fundamental rights into UK law. Article 8 of the UK's human rights act adds legal protection for the right to privacy and family life and relates to GDPR. This legislation, however, also embeds restrictions to these rights to protect, amongst other, things such as 'public safety'. This establishes that exceptions can be made when 'necessary' and 'proportionate' allowing data gathering and sharing for AV in-use monitoring.

2.2.2 Data Reform Bill (DRAFT) - UK

The UK Data Reform Bill proposes changes to UK data protection. This new bill aims to enter consultation in mid-2022 following announcement on 10th May 2022. This new bill is expected to make some changes to UK data protection. These aim to support added powers for the regulator (ICO) but also may change support to encourage AI system developments with increased potential for available training data retention. This may allow UK generalised data protection to differ further from EU's GDPR which could impact data adequacy and rights for international data transfer. As the draft terms of this act are not yet published its impact remains uncertain for AVs so is not considered further in this document.

2.2.3 Regulation of Investigatory Powers Act 2000 (RIPA 2000) – UK

The Regulation of Investigatory Powers Act 2000 provides means for covert surveillance by selected public bodies within the UK. Gathering of data could apply to AVs where data gathered from a vehicle could be required to enable either 'directed surveillance' of individuals or 'intrusive surveillance' to record audio or video within a vehicle. This may require UK Home Office guidance clarifying how this act would apply to AVs. This area is deemed out of scope of this review.

information (kept separate to the pseudonymised data) it cannot by used de-anonymised. This supports machine learning and human tasks but without disclosure of personal details. Pseudonymised data requires strict controls as using additional specific information pseudonymisation can be reversed (hence the legal need to regard data as personal data still).

[24] Similar advice is found in good practice guidance related to GDPR (article 3) and other global standards.

2.2.4 Equality Act 2010 (EA 2010) – UK

The UK Equality Act places equality-based fundamental protections closely linked to GDPR and data protection. These aim to ensure fair and equal treatment across specific protected characteristics, which include:

- age;
- disability;
- gender reassignment;
- pregnancy and maternity;
- race;
- religion or belief;
- sex; and
- sexual orientation

AVs may need to consider this act if and where gathering data could make determination to these protected characteristics. For example, pedestrians may be classed as adult/child or being in a wheelchair. If such data is required (legitimate interest) for LSAV object recognition to support Highway Code rule compliance and analysis it requires strong processes to ensure that this data is not combined with personally identifiable information. Such data will be minimal, if gathered at all, this should if gathered meet the terms of necessary and proportionate for the purpose of maintaining fundamental rights to safety.

2.2.5 Protection of Freedoms Act 2012 (PoFA 2012) – UK

The protection of Freedoms Act 2012 (PoFA2012) covers seven key areas related to data protection and freedoms. These include, amongst other areas, regulation for surveillance covering codes of practice for surveillance technologies. These laws have strong relevance to AVs' use of data in respect of camera usage and automatic number plate recognition technologies and processing. Section 31 of PoFA provides legislation to adhere to a Surveillance Camera Code of Practice. This code of practice was recently updated (in 2022). This includes:

"(a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)"

These terms apply to specific sensors deployed within AVs and data gathered by them, especially visual camera-based systems that are capable of gathering personally identifying information about individuals or number plates of vehicles. This places 12 principles that must be followed by AV operators. These are:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need. (I.e. LSAV declared purposes as detailed in Section 2.1.2.2.)

2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. (I.e. completing DPIA records ensuring that necessity and proportionality is established.)
3. There must be as much transparency in the use of a surveillance camera systems as possible, including a published contact point for access to information and complaints. (I.e. AV operators must use suitable signage on vehicles and must provide transparent information and contact points to enable contact or complaint.)
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. (I.e. AV operators must maintain accountability documentation.)
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them. (I.e. LSAV operators (or manufacturers) must use suitable signage on vehicles as well as making clear to vehicle users the use of camera-based recording.)
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged. (I.e. LSAV operators and manufacturers must indicate required retention as detailed Section 2.1.2.5. LSAV operators and manufacturers may declare a legitimate interest to store information for training and refinement of systems or to maintain records for liability that could have a longer retention. It should be noted that in the case of CCTV data retention is recommended to be limited to 31 days unless 'proportionate' and 'necessary' requirements require longer retention.)
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes. (I.e. AV operators must set approaches to control data access allowing only declared processing on gathered data; this is detailed further in Section 2.1.2.6.)
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards. (I.e. AV data handlers are strongly required to adopt industry best practice and third-party auditing of approaches like those within ISO 27001 accreditation.)
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. (I.e. as above, following best practice approaches and audited processes.)
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published. (I.e. LSAV data handlers are again encouraged to follow audited review approaches like those of ISO 27001.)
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and

information of evidential value. (I.e. supporting the needs for in-use regulation and system safety improvements.)

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date. (If needed by AV operators and manufacturers.)

Further details about the surveillance camera code can be found in the latest version of the guidance[25].

2.2.6 Investigatory Powers Act 2016 (IPA 2016) – UK

Like RIPA (Section 2.2.2), this regulation provides investigatory powers and rights of access to digital data and could be applied to future LSAVs. This again may require Home Office guidance to clarify how this act applies to LSAVs. This area again, as beyond the declared purpose of data gathering, is not considered further in this document as judged out of scope.

2.2.7 Public Order Act 1986 (POA 1986) – UK

The Public Order Act is mostly out of scope for AVs but it does define a "Public place" which includes any highway. As such POA provides the framework related to surveillance camera provisions with rights to record in such settings. This is not detailed any further in this document other than in connection to surveillance law.

2.2.8 Automated and Electric Vehicle Act 2018 – UK

The Automated and Electric Vehicle Act 2018 established law supporting liability handling for automated vehicles. This places a need for any incident involving automated vehicles to make clear determination between machine and human control. In LSAVs, the vehicles are expected to have full automated control and data declared in WP5 Task 2, 3, 4 in-use and post-incident data supports help to support incident liability determination to help support this need.

2.2.9 Vehicle Technology and Aviation Bill (UK DRAFT)

The Vehicle Technology and Aviation Bill is currently only draft proposed legislation[26] in early stages of its review. This seeks to address a number of legal protections related to automated vehicles in places extending various legislation including the Automated and Electric Vehicle Act and Road Traffic Acts. This planned bill introduces new criminal acts for using lasers knowingly to disrupt vehicle operations[27], introduce a registry of automated vehicles and establish law to clarify liability determination. Despite these planned amendments, no additional AV data requirements are known; however, despite this it may become important

[25] https://www.gov.uk/government/publications/update-to-surveillance-camera-code

[26] https://bills.parliament.uk/bills/1960

[27] These clauses target safety impacts for commercial aviation but could have application to similarly impacted automated vehicles. The extent this applies to automated vehicles remains unclear although outline protections against such actions could be supported in this draft text if the scope would cover this area.

for AVs to help inform on criminal interruption of signals that can impact safety. Until this law is clarified no LASV data protection considerations are expected.

2.2.10 2018/858 (EU)

Within Europe, vehicles need conformant 'type approval' before market release. Approval is only granted when a multitude of technical requirements from different regulatory acts are met and post acceptance is subject to market surveillance. UK law retains these principles which form the basis for the planned new national type-approval framework in Great Britain (GB type approval).

Current approval approaches include market surveillance reporting to satisfy regulators' in-use compliance checks; for instance, ALKS includes a need for in-use monitoring. Despite this, no type approval is currently specified for LSAVs via the European directive and its related requirements so is out of scope as it will not currently add additional data protection (beyond GDPR) for privacy needs for LSAVs.

2.2.11 Driver Privacy Act (US) 2015

US specific law would not apply to UK AVs and data protection. However, this regulation (active in 17 states) has strong value to consider alongside post-incident analysis data.

The US Federal 'Driver Privacy Act 2015' is a specific law stating controls on information collected by EDRs within vehicles in relevant US states. This act states that vehicle owners or leasee's hold the ownership of EDR recorded data within a vehicle. This law aims to ensure privacy for the driver allowing access to EDR data only in the event that consent by the vehicle driver is given, subject to certain exceptions (e.g., court orders, vehicle safety research, or to service or repair the vehicle).

This law is of interest to LSAVs as it declares the legal owner of gathered lagging event incident data to address two key risk:

1) risks of data access barriers previously found from manufacturers declaring legal ownership and exhibiting reluctance to share owned data in particular cases,

2) risk of misuse of recorded data for purposes against the interest of passengers and the public.

This law although not applicable to the UK invites consideration of the legal owner of gathered in-use data to ensure best protection for passengers and the public regarding data access and its use. Where possible to assign ownership to LSAV passengers rather than vehicle operators and manufacturers this may minimise the above risks.

2.3 Summary of existing regulations relevant to data protection for AVs

Data protection for LSAVs remains guided mostly by generalised data protection regulations (like GDPR) rather than vehicle specific regulation. However, to support legitimate interests for operational, in use and incident purposes requires 'proportional' and 'necessary' data gathering to support public safety. To judge the impact of data gathered, processed and shared, these are each now considered (Section 3).

3 Data gathered by AVs and its data protection sensitivity

This section of the report details the data expected to be gathered from AVs and the protection implications of all data.

Differing stakeholder concerns for data protection[28] must consider any legal breach or exemption carefully according to the law and the legitimate needs for such data. This requires the analysis of data being split into separate considerations of:

- In-use monitoring data
- Public reporting data
- Post-incident response data

Each of these is now considered.

3.1 In-use monitoring data and its data protection

In-use data is required for AVs to ensure safe operation and compliance monitoring. WP5 Task 2 suggested the extent of this data following GDPR Article 5 principles to provide minimal data to support the task. This data was considered to be 'necessary' and 'proportional' to maintain public safety.

The data recommended for in-use monitoring was detailed in three core parts:

- Lagging data
- Leading data
- Continuous data

Each of these is now detailed with analysis on each data field regarding its data privacy implications and considerations.

3.1.1 Lagging Recall Data

Lagging data is that suggested to support the needs of in-use monitoring for a triggered risk event whereby each event having a strong correlation to a realised risk occurrence. These events are rare, and each contains data supporting understanding of the event to support future risk analysis.

[28] As detailed in Table 2, page 3.

Table 3: Data privacy impact review of lagging recall data

Data element	Condition for requirement	Data protection considerations for each data field suggested in WP5 Task 2 – Lagging Data
Delta-V, longitudinal	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Maximum delta-V, longitudinal	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Time, maximum delta-V, longitudinal	Mandatory	This field contains exact time of a likely incident which if in reference to personal data must be protected. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Speed, vehicle	Mandatory	This field contains speed data so can indicate speed limit non-compliance (criminal offence). As such, this data can be sensitive and requires processing controls to maintain data protection. Speed data is, however, necessary to help maintain public safety and compliance checks.
		No barrier to collation given secure storage and processing controls.
Motor Transition Demand	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Service brake Demand	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Ignition/start cycle, crash	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Ignition/start cycle, download	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Occupant protection system deployment, time to deploy, in the case of a single stage air bag, or time to first stage deployment, in the case of a multi-stage air bag(s)	If installed	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Multi-event crash, number of events	If Recorded (strongly recommended)	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.

Data element	Condition for requirement	Data protection considerations for each data field suggested in WP5 Task 2 – Lagging Data
		No barrier to collation given secure storage and processing controls.
Time from event 1 to 2	If Recorded (strongly recommended)	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Complete file recorded	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Lateral acceleration (post-crash)	If recorded	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Longitudinal acceleration (post-crash)	If recorded	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Normal acceleration (post-crash)	If recorded	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Delta-V, lateral	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Maximum delta-V, lateral	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Time maximum delta-V, lateral	Mandatory	This field contains exact time of a likely incident which, if in reference to personal data, must be protected. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Time for maximum delta-V, resultant.	Mandatory	This field contains exact time of a likely incident which, if in reference to personal data, must be protected. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Engine/Motor rpm	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Vehicle roll angle	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.

Data element	Condition for requirement	Data protection considerations for each data field suggested in WP5 Task 2 – Lagging Data
Anti-lock braking system ABS activity	If present in AV vehicle	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Stability control	If present in AV vehicle	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Digital requested Steering input	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Safety belt status	If present, for each seat	This field contains information about seat belt compliance which, given mandates to use fitted seat belts, could hold information about an offence related to individuals in fixed seats. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Occupant protection systems deployment, time to nth stage,	Mandatory if fitted with multi-stage occupant protections. (each)	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Occupant size classification, any passenger	If recorded	This field contains protected information that has concerns under the equality act, i.e. being able to identify weight (linked to gender), and if likely children from seat sensor data. This data must be 'necessary' and 'proportionate' as this is essential in post-incident analysis to understand safety concerns. It therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Automated Driving System Status	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Automated Driving System - Minimal Risk Manoeuvre	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Automated Driving System - Override	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Latitude	Mandatory	Locational data is protected under data privacy as it can inform upon individuals via journey endpoints (privacy), aid profiling related to addresses and can be used statistically to determine journey purpose (which can be linked to individuals). Location data is required, however, for understanding rule compliance and safety. This therefore requires very strong management and strict processing controls to maintain data protection.

Data element	Condition for requirement	Data protection considerations for each data field suggested in WP5 Task 2 – Lagging Data
		No barrier to collation given secure storage and processing controls.
Longitude	Mandatory	Locational data is protected under data privacy as it can inform upon individuals via journey endpoints (privacy), aid profiling related to addresses and can be used statistically to determine journey purpose (which can be linked to individuals). Location data is required, however, for understanding rule compliance and safety. This therefore requires very strong management and strict processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
All trigger status in (Section)	Mandatory	This field does not contain protected information but could be in reference to wider protected data or used alongside. This therefore requires processing controls to maintain data protection.
		No barrier to collation given secure storage and processing controls.
Operating environment static and mobile objects, relative position, longitudinal (nearest 'x' objects infront/behind)	Mandatory	Relative locational data is provided but without personal details (no imagery or identified individuals). This data, however, can be used alongside other sources to enable tracking. This therefore requires strong management and strict processing controls to maintain data protection. Controls should allow for compliance and safety analysis only.
		No barrier to collation given secure storage and processing controls.
Operating environment static and mobile objects, relative position, lateral (nearest 'x' objects left/right)	Mandatory	Relative locational data is provided but without personal details (no imagery or identified individuals). This data, however, can be used alongside other sources to enable tracking. This therefore requires strong management and strict processing controls to maintain data protection. Controls should allow for compliance and safety analysis only.
		No barrier to collation given secure storage and processing controls.
Operating environment static and mobile objects, speeds, (nearest 'x' objects)	Mandatory	Relative speed data is provided but without personal details (no imagery or identified individuals). This data, however, can be used alongside other sources to enable tracking. This therefore requires strong management and strict processing controls to maintain data protection. Controls should allow for compliance and safety analysis only.
		No barrier to collation given secure storage and processing controls.
Operating environment static and mobile objects, trajectory, (nearest 'x' objects)	Mandatory	Relative trajectory data is provided but without personal details (no imagery or identified individuals). This data, however, can be used alongside other sources to enable tracking. This therefore requires strong management and strict processing controls to maintain data protection. Controls should allow for compliance and safety analysis only.
		No barrier to collation given secure storage and processing controls.
Operating environment static and mobile objects, classification, (nearest 'x' objects)	Mandatory	Object classification is provided but without identifying personal data just broad classification to allow analysis without impact to personal details (no imagery or identified individuals). This data, however, can be used alongside other sources to enable tracking. This therefore requires strong management and strict processing controls to maintain data protection. Controls should allow for compliance and safety analysis only.
		No barrier to collation given secure storage and processing controls.

Across all lagging data recommended, no barrier to data collation is found given that lagging data followed privacy by design principles. Despite this, data protection and privacy concerns remain as data could be used alongside external data sources (with personal data included).

This could enable profiling and enable additional data about individuals being obtained. As individuals or registered vehicles in gathered data may not have given consent for data gathering, strict controls are required to ensure compliance. Data gathered must be:

- Held in secure repositories with auditing of these (e.g. ISO 27001)
- Follow a DPIA process to review and audit data privacy
- Have processing controls to ensure only purpose declared processing can be undertaken

These approaches must be ensured for any processors of such data.

3.1.2 Leading Recall Data

Leading data aims to provide additional data about safety-related operations that may not result in risk occurrence, e.g. atypical events that may support safety and compliance analysis.

Table 4: Data privacy impact review of leading recall data

Data element	Condition for requirement	Data protection considerations for each data field suggested in WP5 Task 2 – Leading Data
Delta-V, longitudinal	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Speed	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Delta-V, lateral	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Automated Driving System Status	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Automated Driving System - Minimal Risk Maneuver	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Automated Driving System - Override	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Latitude	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Longitude	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Satellite UTC time	Mandatory	This field is a timestamp taken from satellite GPS connections in UTC time. This data field by itself is not protected but if used in combination with other data can be utilised to profile individuals. Its use is no barrier to collation given secure storage and data processing controls.
Operating environment static and mobile objects, relative position, longitudinal (nearest 'x' objects)	If using proximity leading measures	This data is a subset of data in lagging measures so is discussed above.
Bearing (gyroscope)	Mandatory	This data is a subset of data in lagging measures so is discussed above.
Operating environment static and mobile objects, relative position,	If using proximity leading measures	This data is a subset of data in lagging measures so is discussed above.

lateral (nearest 'x' objects)		
Operating environment static and mobile objects, speeds, (nearest 'x' objects)	If using proximity leading measures	This data is a subset of data in lagging measures so is discussed above.
Operating environment static and mobile objects, trajectory, (nearest 'x' objects)	If using proximity leading measures	This data is a subset of data in lagging measures so is discussed above.
Operating environment static and mobile objects, classification, (nearest 'x' objects)	If using proximity leading measures	This data is a subset of data in lagging measures so is discussed above.

Although data in leading measures can be gathered more often, the resolution of the data can be reduced to still represent a minimal-data-required approach to data collation for the purpose of declared usage (it minimises data fields from those of lagging data gathering and the frequency of gathering). As such, this is compliant with GDPR assuming strong controls are followed supporting only allowable processing of the data restricted to the declared purposes of data gathering.

3.1.3 Continuous Data

Continuous data gathering is required to support liability determination and post-incident handling should a lagging or leading approach fail to trigger specific data gathering around an incident. Also, continuous data is required for in-use compliance checks to road rules. By design, this data having continuous data gathering is vastly minimised to reduce risk to privacy and practicalities for data gathering. These data protection concerns are covered now in two parts (continuous data and data only provided upon state changes) detailing for each area any data privacy concerns:

Continuous data:

- Vehicle telemetry – GPS, speed, gyroscopes, accelerometers, telemetry accuracy and quality measurement (as undertaken in commercial telematics vehicle tracking)
    - This data being continuous has data privacy risk in that it has a potential to reveal entire journey routes and movements – including from distinct address endpoints that could separately (in combination with external data) be associated with an individual or household.
    - Specific controls are therefore required to minimise access to such data as well as restricting usage to only allowable processing for the declared purpose.
    - This data, despite its risks, is 'necessary' to enable rule compliance analysis and is 'proportionate' given a need to protect public safety.
- Proximity data for nearby objects – data derived from object detection, distance, object classification (vehicle, static obstacle, VRU), object direction, object trajectory,

object state (brake lights, traffic signal lights, indicator lights, hazard lights, blue flashing lights)
    - This data may (like in lagging and leading data) enable the tracking of movements of wider individuals and vehicles. By design, however, this data does not contain personal data unless combined with external data sources.
    - Specific controls are therefore required to minimise access to such data as well as restricting usage to only allowable processing for the declared purpose.
    - This data, despite its risks, is 'necessary' to enable rule compliance analysis using scene reconstruction and is 'proportionate' given a need to protect public safety.
- Event-based change data (only upon state change, not continuously transmitted)
    - Automated systems – operating status change and override events.
    - Door, boot, window and bonnet status – open/closed/locked/position/status
    - Horn and light operations
    - On/off/low-beam/high-beam/flash/fog/hazard/etc/accuracy and quality measurement
    - Vehicle dynamics and safety systems – ABS pre-charge, forward collision warning, stability and traction control, etc.
    - Crash restraint and seat sensors – status, occupancy, accuracy and quality measurements
    - Wipers – speed/state/front/rear/accuracy and quality measurement
    - [if fitted] Trailer / wheelchair ramp / assistive systems – status/detection
    - Ignition control – interaction and operation of ignition and auto/start-stop technologies or in the case of EVs engine on and off.
        - These data in themselves present little data protection concern as they relate to the vehicle operation; however, some aspects are related to user protected characteristics (e.g. a wheelchair ramp) or personal preferences (e.g. window positions). By design, however, this data does not contain personal data unless combined with external data sources or processed incorrectly in connection with location data.
        - Specific controls are required to minimise access to such data as well as restricting usage to only allowable processing for the declared purpose (in-use monitoring and risk-analysis).
        - This data is 'necessary' to enable rule compliance analysis using scene reconstruction and is 'proportionate' given a need to protect public safety.

Overall, no major barriers for data protection are observed. This does, however, stem from a privacy by design principle which has omitted camera footage from in-use data[29] and ensured that fields do not contain in themselves personal data. Controls are still required to prevent

[29] Omitted also due to practicalities of automated reuse and its data size making capture prohibitive for the operator.

unwanted disclosure or unwanted processing upon such data. In cases where such data is required, anonymisation of data should be prioritised at source.

3.2 Public reporting data and its protection

Task 3 "Safety Monitoring Framework" details potential mechanisms for reporting of concerns related to AV operation. Such mechanisms can originate from AV operators, the public or wider authorities. Any such mechanism, however, will be reported by a submitting individual thus holding personal information about the report originator. Also, details provided may contain sensitive and personal data due to the potential open format allowing wide information capture. These details are required to ensure validity of the person(s) submiting a report as well as the flexibility needed to capture wide concerns that could be reported. This allows inclusion of additional personal data as may be required. Such information presented must be treated with respect to applicable regulations and stored securely for only agreed purpose based processing. This information is provided in support of public safety so is 'necessary' and 'proportional' to the need to provide open communication of concerns. Data gathered in this manner, however, must follow strict controls to be securely stored, processed only by allowable and declared processing.

3.3 Post-incident response data

Reporting after an incident could include a range of reporting pathways[30] such as from:

- members of the public
- enforcement agencies
- road authorities[31]
- manufacturers
- operators
- automated in-use trigger event reporting (Section 3).

Reporting can also include many differing event scenarios, for example:

- Road rule violations
- Road collisions
- Near miss or proximity events
- ODD exits
- Minimal Risk Manoeuvres
- Remote operator overrides

[30] As detailed in the WP5 Task 4 Post Incident Framework report.

[31] Including IoT and smart infrastructure recording of events.

- Passenger or public emergency stop overrides
- Vehicle detected safety critical events
- Emergency safety system initialisations.

Such varied pathways and event scenarios present highly varied potential data and its need for transmissions, sharing, processing and persistence. Regarding data protection for these reporting channels and the data within such reports they are very likely to contain personal information. Personal information may include information about the submitter[32] or other individuals[33] related to the event. Reports may also include data in a variety of formats that can include not just numeric and textual reporting but also sensor, camera (or dashcam) data that could include again potential personal information.

For such reports and the data within them, it can strongly be argued as necessary to gather this information given its clear proportional need for maintaining public safety. However, this does indicate, given the potential sensitivity of data, that very strict controls and security are required. These need to ensure data is gathered and held for only the permitted purpose of safety reviews and analysis. Upon receipt, pseudo-anonymisation approaches should be used (where possible[34]) to minimise risk in processing.

[32] To ensure validity of submitted events and means to obtain additional information involved parties.

[33] These may be directly impacted individuals or witnesses to a reported event who may be needed to understand a complex event.

[34] This may not be possible in all cases as contact details for witnesses or those involved in an event may be needed for safety analysis. This, however, should be exposed only when needed for agreed processing of safety analysis.

4 Data protection recommendations for AVs

The recommendations for AVs in relation to data protection follow in the most part existing generalised data protection law; however, some specific recommendations are made on top of existing law or where it provides specific guidance to AV regulators or operators. These are recommended in the list below.

Table 5: Summary recommendations table

No.	Recommendation
1	The AV operator and manufacturer **must** ensure valid open grounds ('lawful basis') for collecting and necessary processing of any personal data. This follows the principles of GDPR Art 5(1) (a) recommending in particular that the operator declare data gathering for: Safety analysis, including in-use data collation and post-incident analysis, to support compliance and regulator-based monitoring.
2a	The AV operator and man ufacturer **must** follow ICO and industry good practice and maintain clear historic and up-to-date records regarding types and classes of gathered data during AV operation including both those including personal data and those not.
2b	Such records **must** be provided to the authorised in-use regulator (or other recognised legal authority) upon instruction or request to do so.
2c	This record **must** include as a minimum: • brief data descriptions of gathered data types/classes, • indications if each may contain personal data or if fully anonymised at point of gathering, • descriptions of potential PII within each data type/class, • indication of consent mechanisms and who they apply to for any data type/class of gathered data, • indication of any PII that are potentially gathered without explicit consent, i.e. those that are gathered due to necessary and proportionate data gathering needs (e.g. external facing video to maintain safe operation), and • the retention period of each data type.
2d	The Regulator **could** provide guidance to help normalise data within such records to help standardise and understand available data gathered.
3	The LSAV operator and manufacturer **must** make available to the authorised in-use regulator upon request its record of data types gathered (as detailed above)
4a	The LSAV operator and manufacturer **must** make public and transparent via open publication all data gathering purpose(s) involving 'personal data' to make transparent the purpose(s) and extent of its AV data gathering. (This follows GDPR Article 5(1)(b) to ensure 'purpose limitation' in data gathered.)
4b	A declared purpose **must** contain "data gathering and processing to support in-use and post-incident data provision for regulators and compliance checks".

5	The LSAV **should** (where possible) anonymise external sensor data upon collection to remove PII (following good practice and principles of GDPR article 25). E.g., camera footage blurring faces or number plates. If not possible, AV operators **must** show justified, necessary and proportionate need for gathering such data (i.e., in order to ensure safety or other fundamental needs[35]).
6	The Regulator **should** provide guidance to maintain LSAVs: leading, lagging and continuous 'in-use' data as required with suitable protections and security for a period of 7 years[36].
7a	The LSAV operator (or any other holder of in-use vehicle data) **must** be required to follow industry leading accredited practices for data protection and security. E.g. following ICO guidance on digital service security including compliance with international audited standards like ISO 27001, monitoring and auditing, incident handling and system security to maintain strong data protection.
7b	These approaches **must** maintain DPIA process and output records which are reviewed via third-party audit annually (or more frequently) covering all the data gathered and processed for LSAV operation.
7c	It is recommended that LSAV operators and manufacturers **should** have good cybersecurity measures in place, notably third-party penetration (Pen) testing of its systems as part of its process testing.
8	It is recommended that LSAV developers in control of vehicle data gathering **should** (where possible) also apply point of gathering anonymisation to property or household data (if gathered) to the same extent as GDPR personal data. This aims to provide protection for property owners and data about properties ensuring protection beyond GDPR. This follows approaches within California and China that consider such protections and ensure protection related to property and address point information with specific regard to remote vehicle data gathering.
9	The Regulator **could** review "Provisions on the Management of Automobile Data Security"[37] to consider if wider protective controls for gathering data in sensitive regions or data reuse could require wider regulation.
10	The LSAV operator **should** ensure clear separation and processing controls regarding any PII data in relation to data that may classify 'protected characteristics' of individuals. These include object recognition that may for example identify children and wheelchair users separately to other vulnerable road users to help safety

[35] Gaze detection may be helpful to understand vulnerable road user behaviours and reduce operational risk. In such instances efforts should still be made to remove PII after such analysis and ensure only permitted processing for any such data.

[36] See section 2.1.2.5 for discussion on retention periods and why this period is suggested.

[37] Chinese Language version of these provisions are available at http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm

	analysis and enable road rule compliance checks related to specific protected classes of individuals.
11	The LSAV operators **should** use pseudonymisation where possible to minimise data protection risks (following data protection good practice).
12	The Home Office **should** provide guidance for the application of both RIPA2000 and IPA2016 in regard to LSAVs. This will remove ambiguity about the potential need to supply such data from such vehicles, which is currently uncertain.
13	The Regulator **should** make clear the legal ownership of 'in-use' gathered data and provide guidance for the terms for its access. This may follow the approaches of the Federal Driver Privacy Act 2015 (US), to protect miss use of gathered data. Clear indication of legal owner (as well as who has access) is required and could provide additional protection to the public.
14	The LSAV operator **must** use suitable signage on vehicles to indicate to external individuals that recording may occur – following the latest Surveillance Camera Code of Practice (2022).
15	The LSAV operator **must** provide a clear public-facing contact means for data protection or surveillance recording-related queries or concerns from members of the public.
16	The LSAV operator **must** provide clear public facing indications of data retention related specifically to surveillance camera footage captured internally or externally to the vehicle. Any retention of data beyond 31 days must be declared with clear purpose and necessity for data gathered beyond this period.

5 References

39th International Conference of Data Protection and Privacy Commissioners. (2017). *'Resolution on Data Protection in Automated and Connected Vehicles'.*

ALTUNYALDIZ, M. Z. (2022, Jnne 1st). *Council of Europe Committee on Legal Affairs and Human Rights Legal aspects of "automated" vehicles Report**. Retrieved from assembly.coe.int: https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-20-EN.pdf

British Standards Institute. (2021). *A review of CAV safety benchmarking and a proposal for a "Digital Commentary Driving" technique.* BSI.

British Standards Institute. (2021). *PAS 1882:2021. Data collection and management for automated vehicle trials - Specification.* BSI.

Commission Nationale Informatique & Libertés (French Data Protection Agency). (2017). *Report on Connected vehicles and personal data: 'Compliance Package - Connected Vehicles and Personal Data'.* Commission Nationale Informatique & Libertés .

European Commission. (2016). *'A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility'.* European Commission.

European Data Protection Board ("EDPB"). (2022, June 2nd). *draft guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.* Retrieved from edpb.europa.eu: https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

fpf. (2022, June 1st). *China new draft car privacy and security regulation is open for public consultation.* Retrieved from fpf.org: https://fpf.org/blog/china-new-draft-car-privacy-and-security-regulation-is-open-for-public-consultation/

Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). (2020). *Ethics of Connected and Automated Vehicles : Recommendations on Road Safety, Privacy, Fairness, Explainability and Responsibility.* Luxembourg. doi: 10.2777/035239.

ICO. (2022, May 27th). *The Information Commissioner's Office (ICO) response to the joint consultation from the Law Commission and Scottish Law Commission entitled 'Automated Vehicles: Consultation Paper 3 – a regulatory framework for automated vehicles'*. Retrieved from ico.org.uk: https://ico.org.uk/media/about-the-ico/consultation-responses/2619706/ico-response-law-commission-automated-vehicles-202103.pdf

International Working Group on Data Protection in Telecommunications. (2022, May 12th). *Connected Vehicles 63rd meeting, 9-10 April 2018, Budapest, HUNGARY.* Retrieved from www.datenschutz-berlin.de: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Connected_Vehicles.pdf

Joint Research Centre (JRC). (2022, May 27th). *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Automated Driving*. Retrieved from www.enisa.europa.eu: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-automated-driving/

Nister, D. L. (2019). *"The Safety Force Field," NVIDIA Technical Report.* NVIDIA.

UK Government. (2022, June 7th). *UK's 2022 revised "Surveillance camera code of practice" (related to Protection of Freedoms Act 2012).* Retrieved from gov.uk: https://www.gov.uk/government/publications/update-to-surveillance-camera-code

WP.29 180th session. (March 2020). *revised Framework Document ECE/TRANS/WP.29/2019/34/Rev.2. Consolidated EDR-DSSAD review 'EDR-DSSAD-04-04 Consolidated Review of Contracting Party DSSAD Activities & Way Forward Rev 8'.* https://wiki.unece.org/download/attachments/92014028/EDR-DSSAD-04-04%20Consolidated%20Review%20of%20Contracting%20Party%20DSSAD%20Activities%20%26%20Way%20Forward%20Rev%208.docx?api=v2 [LAST ACCESSED 7th JUNE 2022].

Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring

Abstract

This report assesses the data privacy considerations associated with proposals for an in-use safety and security monitoring scheme. This work presents the current legal framework of data privacy in the UK as well as internationally. Based on this the proposals for data capture are assessed against the regulatory requirements to identify any issues. This work finds that the benefits of in-use monitoring to ensuring public safety can justify the capture of data provided that privacy concerns are managed appropriately.

Relevant Reports

- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 1 – Road Incident Taxonomy; https://doi.org/10.58446/mvuc1823
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 2 - Minimum Dataset Specification; https://doi.org/10.58446/nksn4732
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 3 - Safety Monitoring Framework; https://doi.org/10.58446/sgxq7004
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 4 - Post Event Investigation Process; https://doi.org/10.58446/egfa6491
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 5 - Outcome Reporting; https://doi.org/10.58446/qlpq9096
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 7 - Change Control; https://doi.org/10.58446/bpdl3309

TRL
Crowthorne House, Nine Mile Ride,
Wokingham, Berkshire, RG40 3GA,
United Kingdom
T: +44 (0) 1344 773131
F: +44 (0) 1344 770356
E: enquiries@trl.co.uk
W: www.trl.co.uk

ISSN: 2514-9652

DOI: https://doi.org/10.58446/dwll8689

PPR2021