Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

The Information Commissioner's Office (ICO) response to the Department for Transport's call for evidence on the Safe Use of Automated Lane Keeping System (ALKS)

The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law has been broken.

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to this call for evidence on the safe use of automated lane keeping system (ALKS), based on a United Nations Economic Commission for Europe (UNECE) regulation. The UNECE Regulation notes in Article 8.1 that it is "without prejudice to national and regional laws governing access to data, privacy and data protection". Whilst the call for evidence is primarily concerned with the development of a regulatory framework to support the safe use of ALKS, this response focuses on the data protection and privacy considerations that are mentioned in Part 2 of the consultation.

Section 2.20 of this consultation states that "data availability is subject to the requirements of national law" but does not detail these requirements. Where information processed by ALKS constitutes personal data, it must be processed in accordance with data protection legislation.[1] If the personal data of vehicle drivers and users is processed inappropriately, there is a heightened risk of intrusion into individuals' work and private lives. The Government and technology providers should therefore adopt a data protection by design and default approach, ensuring that privacy protections are built into the design and development of ALKS vehicles. Consideration will also need to be given to the application of PECR in the context of the operation of ALKS.

Controller

Controllers are the main decision-makers in relation to any personal data collected – they exercise overall control over the purposes and means of processing the personal data. It is not clear who the controller is for any personal data stored in the Data Storage System for Automated Driving (DSSAD), although both insurers and manufacturers are mentioned at section 2.21 as able to set out conditions on data processing. Given the potential involvement of multiple parties in the processing activities, where such data is personal data, account must be taken of the specific requirements of the data protection legislation as regards controller/processor and/or joint controller arrangements.

[1] The Data Protection Act 2018 and the General Data Protection Regulation

For example, Section 2.19 notes that the DSSAD is required to record a variety of information that may constitute personal data – however it is not clear who is responsible for this processing. Given the importance of the data protection legislation's accountability principle, the roles and responsibilities of controllers, joint controllers and processors must be decided at the outset.

The Information Commissioner has created guidance on controllers and processors that may be of use in determining the controller of the personal data.

Data protection impact assessments (DPIAs)
Section 2.12 details how the driver availability recognition system requires the system to monitor the driver to detect if they are available and section 2.21 states that manufacturers and insurers may set conditions on data processing, including sharing data. The monitoring of individuals has the potential to be particularly intrusive to individuals' personal data so again, the ICO highlights the importance of adopting a data protection by design and default approach to ensure the minimal amount of data is processed.

Any conditions as mentioned in section 2.21 need to be compliant with data protection legislation. A DPIA is a tool to help any controllers involved, be they manufacturers or insurers, ensure that they are processing personal data in a manner that is compliant with the data protection legislation.

Indeed, a DPIA must be carried out before any type of processing that is "likely to result in a high risk" to the rights and freedoms of individuals. As the use of ALKS uses innovative technology and tracks individuals' location or behaviour, and may also involve processing on a large-scale, it will require such an assessment to be completed.

The Information Commissioner has produced guidance that outlines when DPIAs are legally required, and how such assessments should be undertaken. Considering and mitigating the potential privacy risks at the earliest stage of the project's development will help ensure that both individuals and organisations can realise the benefits of ALKS in a way that takes account of privacy risks, integrates appropriate safeguards into the processing and helps controllers fulfil their accountability obligations.

Data minimisation
Article 5(1)(c) of the GDPR states that any personal data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that any data collected by the DSSAD or the driver availability recognition system should be the minimum amount of personal data needed to fulfil the purpose of the processing. The data collected should be periodically reviewed to ensure it is still relevant and adequate for the purposes it is processed. The DPIA process forms an effective means of assisting considerations in this regard.

Data retention
Article 5(1)(e) of the GDPR specifies that data must not be retained for longer than necessary in relation to the purpose for which it is processed. Ensuring that personal data is erased or anonymised when it is no longer needed will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. This also reduces the risk that controllers will use such data in error.

It is also important that retention periods are reviewed regularly as appropriate in the context of the processing, and that ongoing testing of the retention periods is undertaken by using available data to test how useful it has been to keep these records for the specified time. For example, if records haven't been used within two to three years then it is likely to be deemed excessive to retain them for that length of time.

Privacy information
The requirement to provide privacy information to individuals in relation to how their personal data will be processed is a fundamental right under the data protection legislation. This is an obligation that data controllers will need to comply with to ensure that drivers are provided with clear and comprehensive information about how their personal data will be processed including what personal data will be collected, the purpose of the processing, how long it will be processed for, and who it will be shared with. Further, data should not be processed in a way which data subjects would not reasonably expect.

It is often most effective to provide privacy information using a combination of techniques, including layering and dashboards. Careful consideration should be taken regarding what format is the most appropriate under the circumstances and privacy information must be regularly reviewed to ensure that any new use of an individual's personal data is brought to that individual's attention before the processing begins. The Information Commissioner has published guidance on privacy information that provides further information on this requirement.

Data Sharing
The data protection legislation obliges the Information Commissioner to produce a statutory Code of Practice on data sharing. The code is currently being finalised following public consultation. When completed, it will be submitted to the Secretary of State and then laid before Parliament. Organisations involved in processing personal data via ALKS will need to take the Code into account when deciding on any conditions for sharing personal data.

Adhering to the code will help to ensure good practice around data sharing and help to manage risks associated with sharing information, particular regarding any crashes or incident investigation. Following the code and adopting its practical recommendations will help to give organisations confidence to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information is being shared.

Do you foresee any legal barriers to accessing data for incident investigation?
There are often compelling reasons why data sharing is needed for law enforcement purposes, such as incident investigation. The data protection legislation does not prevent appropriate data sharing when it is necessary to protect the public, to support ongoing community policing activities, or in an emergency – it provides a framework in which data sharing can be undertaken in a fair and proportionate way. The Information Commissioner's Data Sharing code as well as other guidance referenced above will assist organisations in this regard.

Incident investigation is not defined in the consultation, but it is worth noting that any sharing of personal data for law enforcement purposes will be subject to Part 3 of the DPA and require those bodies processing the personal data to be competent authorities, as defined in section 30 of the DPA. These competent authorities will need to be clear about their responsibilities, such as the need to consider undertaking a DPIA under s64 of the DPA. The ICO has produced guidance on law enforcement processing under the DPA which may be of use here.

The ICO is happy to provide further input on these matters.

Information Commissioner's Office

October 2020