

The Information Commissioner's response to the Department for Transport's consultation on Statutory Guidance for Licensing Authorities; Taxi and Private Hire Vehicle Licensing: Protecting Users.

Overview

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 Commissioner welcomes the Department for Transport's prior engagement with us on the Statutory Guidance for Licensing Authorities; and now the opportunity to provide a response to the formal consultation. We have reviewed the consultation paper and identified that many of the questions do not specifically fall within our remit. It is predominantly the questions regarding in-vehicle visual and audio that are of particular interest to us and so we have set out our answers and any additional appropriate comments below.

General Comments

We welcome the fact that the draft guidance encourages compliance with data protection legislation. As a means of signposting data protection as an important element of the framework in which licensing will be administered, you may wish to consider whether at 2.19 it would be helpful to include 'data protection legislation' alongside 'the Human Rights Act'.

In reviewing the papers that support the statutory guidance, including the Government's response to the report of the Task and Finish Group on Taxi and Private Hire Vehicle Licensing, we noted a number of references to introducing legislation. Whilst we appreciate that this perhaps falls outside of the scope of this consultation, we wanted to highlight a specific requirement in GDPR (Article 36(4)) for Government departments to consult the Commissioner where they are developing proposals for

legislation which concerns, requires or provides for data processing. We trust that the Department will contact us as any proposals are developed and the following [guidance](#) details how you do this and the information we require.

We note that a number of references are made within the statutory guidance to sharing appropriate information with relevant partners, such as the police and neighbouring authorities. Controllers need to be aware of their obligations to data protection law in terms of data sharing: respective responsibilities must be clear, and data that is shared must be necessary and relevant. The Commissioner supports the appropriate use of data sharing to enable better regulation of the taxi and PHV sector. She would reinforce the message that the DPA and GDPR should not be seen as a barrier to justified and proportionate data sharing.

Ensuring that appropriate procedures are in place, such as data sharing agreements, will help to build the necessary relationships with partners to enable the right information to be shared as quickly as possible, whilst meeting good practice. The ICO is currently in the process of updating its statutory data sharing code of practice and will be publishing this for consultation shortly.

The Task and Finish Group on Taxi and Private Hire Vehicle Licensing recommended the formation of a 'mandatory national database' of taxi and PHV licensees. We are aware that plans for this database are now in train, albeit progressed under the banner of the Clean Air Zones programme. Assuming that taxi and PHV licensing bodies will be given access to this database, you may also wish to consider whether the statutory guidance provides a useful vehicle to promote the database as a valuable data sharing tool for licensing authorities.

In relation to paragraph 2.34 and 2.35, whilst we recognise the message intended here in relation to enforced subject access requests, we do feel that there is potential for misinterpretation with how the two paragraphs have been separated. We think it would be helpful if this issue was addressed within the same paragraph and perhaps reworded slightly to make it clearer. We would make the following suggestion:

It should be noted that licensing authorities must not seek to circumvent the legitimate filtering of previous criminal convictions and other information held by the DBS. Whilst data protection legislation gives individuals (or data subjects) a 'right of access' to the personal data that an organisation holds about them. It is a criminal offence for you to require an individual to exercise this right to enable you to gain access to information about their convictions and cautions. This could potentially lead to the

disclosure of information that you wouldn't otherwise be entitled to. The appropriate way of accessing an individual's criminal records is through an enhanced DBS and barred lists check.

In-vehicle visual and audio

Q. 26. The draft statutory guidance recommends that licensing authorities should carefully consider potential public safety benefits and potential privacy issues when considering mandating that taxis and PHVs have CCTV installed (paragraphs 2.104 to 2.109). Do you agree with this recommendation?

The matter of CCTV and audio in taxis has been the subject of lengthy consideration at the ICO and we have engaged closely with relevant stakeholders on this issue. The Commissioner published a [blog](#) back in August 2018 setting out her concerns and view on this issue.

She fully appreciates the public safety and safeguarding benefits that can be achieved for mandating the installation of CCTV in taxis and PHV's. However, in order to comply with their obligations under data protection legislation, it is important that licensing authorities understand the need to balance their responsibilities to protect its drivers and the public with the privacy rights of those individuals.

Consideration of individuals' rights and potential privacy implications should be integral to any installation of CCTV/surveillance system. The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is known as '[data protection by design and by default](#)'. Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Data Privacy Impact Assessments (DPIAs) form part of the 'data protection by design and by default' and accountability approach under GDPR. Article 35 requires organisations to carry out a DPIA before carrying out types of processing likely to result in a high risk to the rights and freedoms of individuals in specified circumstances, such as intrusive surveillance systems.

The Commissioner welcomes the detailed references that are made in the statutory guidance in relation to data protection, individual rights, privacy considerations and undertaking robust DPIAs.

The Commissioner expressed in her [blog](#) on this issue that we had concerns in relation to the approaches being adopted by some councils. Our concerns are not so much about the mandated use of CCTV while the vehicle is being used as a licensed taxi/PHV. Our main concern is where

an authorities policy requires that CCTV is operational continuously, meaning the cameras are also operating when the vehicle is being used privately by the driver. The Commissioner's view on this matter is that, in most cases, this is unlikely to be fair and lawful processing of personal data. It would be extremely difficult to evidence the justification and proportionality for this approach and as such is likely to breach data protection and privacy law. We welcome the Department's support of this view which is acknowledged at 2.108 of the guidance.

Q. 27 The draft statutory guidance recommends that CCTV recordings in taxis and PHVs should be encrypted and accessible only by licensing authority officials (if acting a data controller), the police or when subject to a data subject access request (paragraph 2.114). Do you agree with this recommendation?

As highlighted above, the GDPR requires you to implement appropriate technical and organisational measures to ensure you process personal data securely. Article 32 of the GDPR includes encryption as an example of an appropriate technical measure, depending on the nature and risks of your processing activities. The ICO has seen numerous incidents of personal data being subject to unauthorised or unlawful processing, loss, damage or destruction. In many cases, the damage and distress caused by these incidents may have been reduced or even avoided had the personal data been encrypted. It is possible that, where data is lost or destroyed and it was not encrypted, regulatory action may be pursued by the ICO (depending on the context of each incident). Therefore, the Commissioner welcomes the recommendation that the recordings should be encrypted.

In terms of responsibility for the data/footage that is collected (who is the controller), this will depend on who determines the purposes for which the data are processed and the means of processing. The Commissioner has indicated that if a licensing authority has a mandatory policy for the installation of CCTV in taxis, it is likely, in most circumstances, that they would be the data controller, and welcomes the statutory guidance's support for this view at 2.108. From a security and compliance perspective, it is entirely appropriate that the footage can only be accessed by those with legitimate grounds to do so (ie. where the licensing authority is a controller, the driver cannot access/tamper with the footage). The Commissioner also welcomes this recommendation at 2.115.

We are pleased to note the recommendation at 2.116 in relation to making passengers aware that CCTV is operating. This is a key transparency requirement under GDPR, which provides individuals with an individual right to be informed about the use of their personal data. The ICO advises that it is often most effective to provide privacy information

to people using a combination of different techniques such as layering. It is important that the signage in the vehicles inform the individual who the data controller is and where they can go to make a subject access request or find out more information, such as the purposes for their information being processed, retention periods and who the information may be shared with. The guidance does make reference to this kind of layered approach but it may benefit from highlighting that the ICO has further guidance on privacy information and the [right to be informed](#) on its website. We also feel that additional reference to audio could be made here in relation to informing passengers when audio is in operation. There is a brief reference to this at 2.107, but given that audio is considered to be more privacy intrusive, the importance of informing individuals when an audio recording is being made could be further reinforced at 2.116.

Information Commissioner's Office
17 April 2019