Appendix F

Privacy Impact Assessment (PIA) for CCTV within licensed Hackney Carriage & Private Hire Vehicles.

1. Introduction to Privacy

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

This assessment is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about;
- not kept securely.

2. Identifying the need for a PIA

Worthing Borough Council, as the Licensing Authority, currently requires Hackney Carriages and Private Hire Vehicles are fitted with CCTV. As part of a review of it's Hackney Carriage & Private Hire Handbook the Licensing Authority is undertaking a review of it's Privacy Impact Assessment (PIA) to ensure the initiative is lawful, proportionate, and to ensure that privacy risks are minimised while allowing the aims of the CCTV in licenced Hackney Carriage & Private Hire Vehicles to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice.

As part of the assessment it is necessary to determine who is the 'data controller. The recording and storage of CCTV images is personal data and falls within the Data

Protection Act 2018 (DPA). The DPA defines a “data controller” as the individual or organisation which has ultimate responsibility for how personal data is collected and processed. For the purpose of the installation and operation of in-vehicle CCTV, the council considers that the “data controller” is the Council as it has decided to have a CCTV system installed and operating within the vehicle. The ‘data controller’ is responsible for processing and exercising control over personal information together with how images are stored and how they should be disclosed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the DPA. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

It is important to recognise the purpose for requiring mandatory CCTV installation in Worthing Borough Council licensed Private Hire and Hackney Carriage vehicles and the policy is made in accordance with evidence and local requirements.

3. Describing the information flows

Purpose

The implementation of CCTV within licensed vehicles will serve multiple purposes which ultimately will enable the prevention and detection of crime and promote a safe experience for both drivers and the travelling public

The purposes include:-

- The protection of licensed drivers
- The protection of the travelling public
- The protection of contracted support
- To ensure that licensed drivers continue to be ‘fit and proper’ in line with the licensing conditions

The protection of licensed drivers

Information obtained from the last 2 years have terminated 4 taxi licenses being reviewed as a consequence of hearsay evidence. CCTV footage would have allowed the hearing to consider the CCTV evidence and make a more informed assessment before reaching their decision.

Drivers work alone, often at antisocial hours, visiting areas that may be poorly lit or away from safe routes, and could be carrying any amount of cash within the taxi cab. These factors could increase the risk posed to the driver.

Since the implementation of the CCTV in licensed vehicles in 2017 we have been required to access CCTV footage to provide evidence for:-

- Racial abuse of drivers
- Physical assaults
- Passengers making off without payment
- Investigation on inappropriate behaviour
- Rape allegations

- Investigation on passenger stealing property found in taxi

The protection of taxi passengers

Licensed vehicles are used extensively to service the late night economy, the period of which extends well beyond the availability of other forms of public transport. Patrons often have little choice but to use licensed vehicles. Some customers may be vulnerable if they have consumed excessive amounts of alcohol, and or, become separated from their friends. Licensed vehicles are often the only option for vulnerable people who have no direct transport links, or who have special transportation requirements.

Without the benefit of CCTV an example of risks identified are evident in the following case studies:-

1. Police often have insufficient information to take a prosecution.
2. Victims do not receive appropriate restitution.
3. Drivers may continue to trade for extended periods; whilst any appeal is determined, potentially placing other vulnerable people at risk.
4. The availability of a more robust evidence base would have, in all likelihood secured a more timely resolution in both cases

The introduction of CCTV allows the Licensing Authority with strategic partners to work with the trade, taxi marshals and street pastors to signpost people towards vehicles which operate to the highest standards of public safety. The availability of CCTV would increase the fear of sanction and reduce the likelihood of an incident occurring. In the event that a serious incident was to occur, or an allegation be made, then the availability of CCTV would enable an evidence based decision to be made, as to whether a crime has been committed, and increase the likelihood of securing an appropriate sanction.

An alternative is to rely on existing controls to safeguard the public and to protect drivers and not to use CCTV.

As the local authority has a statutory requirement to ensure that hackney carriage and private hire driver licences are issued to fit & proper persons and rely on existing control measures which include the requirement for Disclosure & Barring Service (DBS) checks for drivers upon application and then every three years. However, incidents continue to be reported to Sussex Police despite these DBS checks.

The DBS check provides a snapshot at that time of categories such as unspent convictions, depending on whether a basic or enhanced check is undertaken. If an incident occurs after a successful check has been undertaken, this would not necessarily be picked up unless the organisation requested another DBS check to be undertaken.

Where the Licensing Authority receives a complaint or allegation, it currently has no option but to suspend the driver pending an investigation. The implementation of CCTV would provide the Licensing Authority with the means to have a quicker overview of any alleged incident.

What enforcement activity is there?

The Council's Licensing Team carry out periodic enforcement operations in conjunction with other partner agencies e.g. Sussex and Surrey Road Policing Unit,, Fraud Officers,, VOSA Vehicle Examiners, Immigration, and other Licensing Authorities. These enforcement operations include, vehicle maintenance checks, airport checks on vehicles, benefit fraud, road fund and fuel tax evasion, Rights to live and work in the UK.
What these activities cannot take into consideration is the exploitation and trafficking of people, money laundering, inappropriate behaviour and other offences.

Case Studies

Study 1: Driver A was the subject a serious allegation of rape and was arrested, an interview under police caution and the licensed vehicle was seized and impounded for DNA analysis. A police investigation was undertaken and Driver A was unable to work, he returned to work after a 10 week investigation and the charges were dropped by the police. If CCTV had been installed at the time in Driver A licensed vehicle, it would have eliminated the driver earlier and he could have returned to work. The driver has since had CCTV installed immediately to ensure his own safety and the protection to his income and business.

Case 2: Driver B was reported to the licensing office for failing to carry 2 wheelchair passengers in a correct and safe manner. Investigating officers had to rely on the statements from the passengers that had travelled with the 2 wheelchairs unsecured in the licensed vehicle. The Licensing Committee determined that Driver B to have CCTV installed in the vehicle and to attend additional disability access training.

Case 3: Driver C was involved in a collision in his/her licensed vehicle. It was a non-fault collision. CCTV proved that it was a non-fault accident to his insurance company which entitled the licence holder to a temporary vehicle whilst repairs were carried out, this enabled him to carry on working

Case 4: Driver D Complaint made by passenger, accusing the driver of asking for sex, no CCTV available to corroborate the passengers accusation and the councils licensing office was unable to verify the claim or prove that the driver was innocent. The complaint was dealt with based on the balance of probability without CCTV any offence(s) remain unproven and the driver remains a holder of a driver licence.

Case 5: Driver E had CCTV running whilst the licensed vehicle was parked with no one in the vehicle. The vehicle was hit by a hit and run driver and was recorded by the CCTV installed within the vehicle. The footage confirmed the identity of the offender and allowed the driver to make a non-fault claim on his insurance.

Case 6: Driver F of a small Private Hire Operator company allowed his Private Hire Vehicle licence to expire which would have made the licence holder's insurance invalid if the vehicle was used for hire & reward. Without CCTV the Licensing Authority was unable to prove whether the vehicle continued to be used for private hire work without a licence and therefore no insurance. If it had this would be putting the public at risk.

Other Cases: There have been various incidents where CCTV installation has provided evidence for investigating officers including incidents where:

- Passenger being racially abusive to the driver
- Aggressive passenger refusing to pay
- Assault on driver
- Misuse of taxi ranks outside of the district

Consultation

Existing licensing trade: The Taxi Licensing Team has recently carried out 2 handbook consultations in 2016 and 2018. All licence holders in the hackney carriage and private hire trades within the Borough were written to. The Consultation included an outline of the Licensing Authority's proposed policy, which included the implementation of CCTV.

All responses to a Licensing Consultation are considered and evaluated by the Licensing Authority before a handbook is adopted.

Elected Members: The Taxi Licensing Team has carried out 2 handbook consultations in 2016 and 2018 with all members consulted.

Internal stakeholder: The Taxi Licensing Team has carried out 2 handbook consultations in 2016 and 2018 and relevant officers and the council's legal team were consulted.

External stakeholders: The Taxi Licensing Team has carried out 2 handbook consultations in 2016 and 2018 with external stakeholders and the general public consulted.

Police: The Taxi Licensing Team has carried out 2 handbook consultations in 2016 and 2018. A detailed representation was received supporting the implementation of CCTV on Crime & Disorder and Public Safety Grounds.

4. Identifying the privacy and related risks

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.

- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.
- Not recording at all times of a journey could impact on the comfort and safety of the passenger

Corporate risks

- Non-compliance DPA or other legislation can lead to sanctions, fines and reputational damage.
- Not recording and an incident occurring could have reputational damage and impact on internal and external investigations
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the Data Protection Act 2018
- Non-compliance with human rights legislation.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.

5. Identifying privacy solutions.

Privacy issue	Risk(s)	Solution(s)	Evaluation
Excessive recording of members of the public in the vehicle	New surveillance methods may be an unjustified intrusion on their privacy. People may be concerned about the risks of identification or disclosure of information. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. Public distrust about how information is used can damage an organisation's reputation.	The system will automatically overwrite data after 28 days. Public are using a commercial vehicle which is used for public transport and would be expected to abide by the terms and conditions governing the use of the vehicle. Appropriate signage displayed advising of the use of CCTV.	The individual will be aware that they are using a commercial vehicle which is used for public transport and that they must abide by the terms and conditions governing the use of the vehicle. Signage will advise of the use of CCTV. The system to be installed is to protect the public and as such the recording of the data is not considered to be excessive.
Intrusion from recording of members of the public outside the vehicle.	New surveillance methods may be an unjustified intrusion on their privacy.	There will be limited collateral intrusion outside of the vehicle as the camera will be positioned accordingly. Signage will be displayed on the vehicle which will be visible from the outside.	The cameras will be installed in a way that ensures that there will be minimal 'over spill outside of the vehicle. The risk is considered to be minimal. The measure is considered to be justified, compliant and proportionate on this basis..
Intrusion of recording of taxi drivers whilst working.	New surveillance methods may be an unjustified intrusion on their privacy. If a retention period is not established information might be used for longer than necessary. Non-compliance with the DPA or other legislation. can lead to sanctions, fines and reputational damage	The system has been installed to protect drivers who are using a commercial vehicle. The driver should be operating the vehicle in accordance with the terms and conditions of the Licence. Data is encrypted. Data will only be accessed securely in the event of an incident by approved and restricted staff	Drivers are operating a commercial vehicle, which is used for public transport and must already abide by the terms and conditions of their licence. The data is encrypted and will be overwritten after xx days. The CCTV system is designed to help to protect the welfare and integrity of the drivers.
Intrusion of taxi drivers whilst not working	New surveillance methods may be an unjustified intrusion on their privacy.	A licensed vehicle remains a commercial vehicle, used for public transport 24 hours a day. Data is encrypted. Data will be overwritten	A licensed vehicle remains a commercial vehicle to be used for public transport 24 hours a day. The data is fully encrypted and data would only be accessed in the event of an incident. Only those images related to the incident will be

		after 28 days.	accessed. All other data would be overwritten. There is no commercially available option to switch the system on and off as this would leave it open to abuse, which would result in uncontrollable risks
Storage of data within the vehicle	Should the data be accessed it will display video images of passengers and driver for the previous 28 days(+). Data could be accessed and/or destroyed illegally to inhibit prevention/detection of crime. Data losses which damage individuals could lead to claims for compensation.	The data is stored within a secure unit. The data is encrypted	The data is stored within a secure, encrypted device, that only an appropriate and authorised licensee can access via the CCTV provider where there is a clear and defined purpose
Disposal of data	Unsecure disposal of data could lead to a DPA Breach. If a retention period is not established information might be used for longer than necessary. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.	Data will be automatically overwritten after 28 days. Any data accessed and stored for the purposes of detecting crime and disorder will be kept in accordance with existing policies of retention.	The Council and the service have appropriate data retention policies in place. Any data that has not been accessed for the purposes of detecting crime and disorder will be automatically be overwritten within 28 days.
Wilful destruction of The data/unlawful access.	Inadequate disclosure controls increase the likelihood of information being shared inappropriately. Wilful destruction may prevent the detection of Crime.	The data is held securely and cannot be accessed directly by the driver. Action can be taken under the conditions of the licence in the event that anyone attempts to	The system is held securely and the data is encrypted. . Action can be taken under the terms and conditions of the licence.

	Data not stored or disposed of in line with the Data Protection Act 2018 Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.	interfere with the system. The council has disciplinary arrangements in the event of any misconduct by a licensee of member or member of staff	

Background papers

ICO : A data protection code of practice for surveillance cameras and personal information version 1.2 (2017) (0609)
ICO Conducting privacy impact assessments code of practice (Draft November 2013)
SCC : Surveillance Camera Code of Practice (2013)