Transport for London
London Taxi and Private Hire

GUIDELINES FOR CCTV SYSTEMS IN LICENSED LONDON TAXIS & PRIVATE HIRE VEHICLES

Introduction

These guidelines set out to ensure that CCTV systems installed in London Taxis and Private Hire Vehicles (PHVs) licensed by Transport for London (TfL) are properly managed whilst being used to prevent and detect crime; and enhance the health, safety and security of both Taxi/PHV drivers and passengers.

Vehicle owners, who may also be the driver and/or operator, installing CCTV systems must fully comply with the requirements set out in these guidelines.

For the purposes of these guidelines the term "CCTV system" will include any electronic recording device attached to the inside of vehicle having the technical capability of capturing and retaining visual images and audio recording from inside or external to the vehicle. In addition to the standard CCTV camera system these may include for example, such devices as events/incident/accident data recording devices.

The purpose of CCTV

The purpose of the CCTV system shall be to provide a safer environment for the benefit of the Taxi/PHV driver and passengers by:

- Deterring and preventing the occurrence of crime
- Reducing the fear of crime
- Assisting the Police in investigating incidents of crime
- Assisting insurance companies in investigating motor vehicle accidents

General requirements

Any CCTV system to be fitted must, as a minimum, meet the requirements set out in this document. Only CCTV systems meeting these requirements and approved by TfL can be installed into licensed taxi and private hire vehicles.

CCTV systems installed in Taxis and PHVs will be inspected as part of the annual licensing inspection to ensure they do not pose a risk to the safety of the passengers or the driver and are fitted safely and securely.

The installation and operation of CCTV must comply with the requirements of the https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
All equipment must comply with any legislative requirements in respect of Motor Vehicle Construction and Use Regulations.

All equipment must meet all requirements as regards safety, technical acceptability and operational/data integrity.

All equipment must be designed, constructed and installed in such a way and in such materials as to present no danger to passengers or driver, including impact with the equipment in the event of a collision or danger from the electrical integrity being breached through vandalism, misuse, or wear and tear.

Automotive Electromagnetic Compatibility Requirements (EMC)
CCTV equipment must not interfere with any other safety, control, electrical, computer, navigation, satellite, card payment device or radio system in the vehicle.

Any electrical equipment such as an in-vehicle CCTV system fitted after the vehicle has been manufactured and registered, is deemed to be an Electronic Sub Assembly (ESA) under the European Community Automotive Electromagnetic Compatibility Directive and therefore must meet with requirements specified in that Directive.

CCTV equipment should be e-marked or CE-marked. If CE marked confirmation by the equipment manufacturer as being non-immunity related and suitable for use in motor vehicles is required.

Camera Design Requirements
The camera(s) must be fitted safely and securely, should not adversely encroach into the passenger area and must not impact on the safety of the driver, passenger or other road users.

Installation
All equipment must be installed as prescribed by the equipment and/or vehicle manufacturer installation instructions.

Each CCTV installation will be subject to the conditions of vehicle licensing as set out in the private hire vehicle and taxi inspection manuals criteria and sections 5.3 to 5.5 of the Conditions of Fitness document. All three documents can be viewed at the Taxi and Private Hire Licensing web pages.

The installed CCTV system must not weaken the structure or any component part of the vehicle or interfere with the integrity of the manufacturer's original equipment.

All equipment must be installed in such a manner so as not to increase the risk of injury and/or discomfort to the driver and/or passengers. For example, temporary fixing methods such as suction cups will not be permitted, or lighting, such as infra-red, which emits at such a level that may cause distraction or nuisance to the driver and/or passengers.

All equipment must be protected from the elements, secure from tampering and located such as to have the minimum intrusion into any passenger or driver area or impact on the luggage carrying capacity of the vehicle.

It is contrary to the Motor Vehicle (Construction and Use) Regulations, 1986, for equipment to obscure the view of the road through the windscreen.

Equipment must not obscure or interfere with the operation of any of the vehicle's standard and/or mandatory equipment, i.e. not mounted on or adjacent to air bags/air curtains or within proximity of other supplementary safety systems, such as autonomous braking systems, which may cause degradation in performance or functionality of such safety systems.

Viewing screens within the vehicle for the purposes of viewing captured images are not permitted.

All wiring must be fused as set out in the manufacture's technical specification and be appropriately routed.

If more than one camera is being installed their location within the vehicle must be specific for purpose i.e. to provide a safer environment for the benefit of the Taxi/ PHV driver and passengers.

All equipment must be checked regularly and maintained to operational standards, including any repairs after damage.

All system components requiring calibration in situ should be easily accessible.

Camera Activation Methods

Activation of the equipment may be via a number and combination of options, including:

- door switches
- time delay
- drivers' panic button
- or, in the case of an incident/event recorder, predetermined G-Force parameters set on one or more axis (i.e. braking, acceleration, lateral forces)

The CCTV system may be configured to record images for a short period of time before the trigger event, during the related incident and a short period following the related incident.

A direct wired link to the vehicle's taximeter, in the case of a Taxi, will not be acceptable.

Audio Recording

CCTV systems must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified except in very exceptional circumstances. You must choose a system without this facility wherever possible; however, if the system comes equipped with sound recording facility then this functionality should be disabled.

- There are limited circumstances in which audio recording may be justified due to a specific threat to an individual's personal safety, e.g. when a 'panic button' is utilised in response to a threat of physical violence. Where this audio recording facility is utilised a reset function must be installed which automatically disables audio recording and returns the system to normal default operation after a specified time period has elapsed. The time period that audio recording may be active should be the minimum possible and should be declared at the time of submission for approval of the equipment.

In the limited circumstance where audio recording is justified, signs must make it very clear that audio recording is being or may be carried out.

Image Security

Images captured must remain secure at all times.

The captured images must be protected using approved encryption software which is designed to guard against the compromise of the stored data, for example, in the event of the vehicle or equipment being stolen. All SD cards must be secure within the camera device, formatted to the camera device and encrypted. All images may only be reviewed via a secure network, i.e. images should not be available to view via an MP3/MP4 player or equivalent.

The Information Commissioner's Office has published guidance on how to keep personal data secure (including personal data contained in CCTV images), on their website.

Retention of CCTV images

The CCTV equipment selected for installation must have the capability of retaining images either:

- within its own secure, encrypted hard drive;
- using a fully secured and appropriately encrypted detachable mass storage device, for example, a compact flash solid state card;
- or, where a service provider is providing storage facilities, transferred in real time using fully secured and appropriately encrypted GPRS (GSM telephone) signalling to a secure server within the service provider's monitoring centre.

Images must not be downloaded onto any kind of portable media device (e.g. CDs or memory sticks) for the purpose of general storage outside the vehicle.

CCTV equipment selected for installation must include an automatic overwriting function, so that images are only retained within the installed system storage device for a maximum period of 28 days from the date of capture. Where a service provider is used to store images on a secure server, the specified retention period must also only be for a maximum period of 28 days from the date of capture. Data may be retained for longer periods in exceptional circumstances, i.e. insurance claims, criminal investigations etc. However, once a relevant case is concluded all data must be deleted.

Where applicable, these provisions shall also apply to audio recordings.

General compliance with data protection obligations
CCTV footage, still images and audio recordings all constitute personal data under data protection legislation (including the UK General Data Protection Regulation – 'UK GDPR' and the Data Protection Act 2018).

As a result, use of CCTV systems in vehicles needs to comply with the principles found in the legislation and must have a lawful basis. You can find more information about your general obligations in this Guide to Data Protection in the UK

Payment of the data protection fee to the Information Commissioner's Office
The Information Commissioner's Office (ICO) is the official regulatory body responsible for enforcing compliance with privacy and data protection legislation.

The law defines a "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 "controller" is the company, organisation or individual which has decided to have a CCTV system installed and operating within the vehicle.** The controller is ultimately responsible for how the images are stored and used and determines in what circumstances the images should be disclosed and the controller is responsible for ensuring that the CCTV system complies with data protection obligations.

It is a legal requirement for organisations and businesses that process personal information to pay a data protection fee to the ICO every year and it is a criminal offence if you don't. The ICO publishes an online register of the organisations and businesses that have paid the fee.
You can find out more about the process by reading the ICO guide to the data protection fee. The level of fee you have to pay varies according to the turnover of your business and the number of employees you have.

Documentary evidence that the data protection fee has been paid may have to be presented to a TfL official at any time during the term of the TPH vehicle licence.

Data Protection Impact Assessments
Before installing a CCTV system in a Taxi or Private Hire Vehicle it is good practice (and sometimes mandatory) to complete a Data Protection Impact Assessment (DPIA) to ensure that you have identified all the relevant privacy issues and taken steps to resolve or mitigate them where necessary. You should also regularly review (ie annually) whether the CCTV system in the vehicle remains useful and fit for purpose.

The ICO has published guidance on Data Protection Impact Assessments.

Using a third-party service provider (processor)
Where a service provider is used for the remote storage and/or management of CCTV data they will act as a 'processor'.

A processor, in relation to personal data, means any person (other than an employee of the controller) who processes data on behalf of the controller, in response to specific instructions. With a few exceptions, the controller retains full responsibility for the actions of the processor, so it is important that care is taken when selecting a third-party service provider and adequate assurances should sought on issues such as data protection and data security.

There must be a formal written contract between the controller and processor (service provider). The contract must contain provisions covering security arrangements, retention/deletion instructions, access requests and termination arrangements.

Documentary evidence of the contractual arrangements may be required to be presented to a TfL official at any time during the term of the TPH vehicle licence.

Using recorded CCTV images
The controller is responsible for complying with all relevant data protection legislation, as well as being legally responsible for the use of all images including any breaches of privacy and data protection legislation.

Any images and/or audio recordings should only be used for the purposes described earlier in these guidelines

Requests to view captured images may be submitted to the controller by the Police or other statutory law enforcement agencies; TfL; insurance companies/brokers/loss adjusters; or exceptionally other appropriate bodies. The controller is responsible for responding to these requests in accordance with the law. Police or other law enforcement agencies should produce a standard template request form, setting out the reasons why the disclosure is required. Alternatively, a signed statement may be accepted.

All requests should only be accepted where they are in writing and specify the reasons why disclosure is required.

Under the data protection legislation, members of the public may also make a request for the disclosure of images, but only where they have been the subject of a recording. This is known as a 'Subject Access request'. Such requests can be made verbally or in writing and must include sufficient proof of identity (which may include a photograph to confirm they are in fact the person in the recording). Controllers are not entitled to charge a fee for a subject access request and must process it for free. More guidance on handling Subject Access requests can be found in the ICO's Guide to the right of access.

Signage

All Taxis and PHVs fitted with a CCTV system must display the sign shown below in a prominent position. The driver may also verbally bring to the attention of the passengers that CCTV equipment is in operation within the vehicle, if it is felt necessary or appropriate.

The signage must be displayed in such positions so as to minimise obstruction of vision and to make it as visible as possible to passengers, before and after entering the vehicle (please refer to the document: Guidelines for Advertising on Licensed London Taxis and Signs on Licensed London Private Hire Vehicles.)

Signs are available for collection from all vehicle inspection centres.

The name and contact details of the Controller must be provided in the blank space included on the sign template. The contact details can be in the form of either telephone number, email address or website URL.

Signage for external facing CCTV systems

Where a CCTV system is installed in order to record incidents *outside* the vehicle (eg a dashcam or similar), you should also display a warning sign wherever practical. In addition, when the CCTV is activated in response to an incident, the driver of the vehicle must inform the person(s) recorded that their personal data was captured - as soon as practicable after the incident. They should also be informed the purpose for which the device has been installed, for example to facilitate their insurance company's investigation of insurance claims.

To assist individual drivers, owners, and operators who are considering the installation of a CCTV system, TfL has produced the summary checklist below to help ensure that all of the relevant approval requirements/standards are complied with.

Please tick

[ ] Data Protection fee paid to the Information Commissioner's Office (ICO). www.ico.org.uk and has the ICO provided you with documentation to evidence payment of the data protection fee as the "controller" associated with your system?

[ ] Have you completed a Data Protection Impact Assessment in relation to your proposed system (or conducted a recent review to ensure it is still fit for purpose)?

[ ] Do you have a process for handling requests to access CCTV footage?

[ ] Do you have documentary evidence regarding contractual arrangements with any data processor or service provider associated with the operation or management of

the CCTV system? (where applicable)

[ ] Have you displayed the required signage, including the relevant contact details?

[ ] Does the CCTV system meet the installation standards as set out in the relevant TPH inspection manual? Please see Taxi and Private Hire Licensing