Guidance on the Use of CCTV Surveillance

Introduction

The use of CCTV[1] in public or private areas for security purposes, crime prevention or monitoring of illegal activities[2] (e.g. throwing objects from heights) has become increasingly common. With the advancements in technology, compared with traditional CCTV systems that mainly provide live streaming and recording, CCTV systems powered by artificial intelligence (**"AI"**) often offer enhanced functionalities such as human detection, facial recognition, automatic number plate recognition and object recognition.

As CCTV may capture extensive images of individuals or information relating to individuals, careful consideration should be given to its use to avoid any intrusion into individuals' privacy. This guidance provides recommendations to data users (both organisational and individual data users) on the responsible use of CCTV in compliance with the requirements under the Personal Data (Privacy) Ordinance, Cap. 486 (**"PDPO"**).

Regarding the use of CCTV for monitoring employees' activities in the workplace or domestic helpers at home, specific guidance can be found in *Privacy Guidelines: Monitoring and Personal Data Privacy at Work*[3] and *Monitoring and Personal Data Privacy at Work: Points to Note for Employers of Domestic Helpers*[4] issued by the Office of the Privacy Commissioner for Personal Data (**"PCPD"**).

Is Using CCTV Lawful under the PDPO?

Lawfulness and Fairness

The PDPO is technology-neutral and does not prohibit any individual or organisation from installing or using CCTV. Generally speaking, if a CCTV system is equipped with recording functions that capture and store images and/or videos of individuals for identification purposes, the use of CCTV may involve the collection of "personal data", and the data user must comply with the requirements under the PDPO, including the 6 Data Protection Principles (**"DPP"**).

---

1 CCTV stands for "Closed Circuit Television", which refers to camera surveillance systems or other similar surveillance devices that are capable of capturing images of individuals.

2 Covert surveillance conducted by a law enforcement agency is regulated by the Interception of Communications and Surveillance Ordinance, Cap. 589.

3 See https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf

4 See www.pcpd.org.hk/english/resources_centre/publications/files/points_to_note_15102015_e.pdf

Definition of "Personal Data"

Under section 2(1) of the PDPO, "personal data" means any data —

- relating directly or indirectly to a living individual;
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- in a form in which access to or processing of the data is practicable.

Example 1:

Where a CCTV camera is installed on the rooftop of a building to investigate the dropping of objects from height or other criminal offences, and the footage captured is of sufficiently high resolution to identify individuals appearing in the footage, the data collected would amount to "personal data" under the PDPO.

- DPP 1(1)(a) requires that personal data be collected for a lawful purpose directly related to the function or activity of the data user. **Data users should consider whether the CCTV is installed for a lawful purpose**. One example would be for security purposes to prevent criminal activities.

- DPP 1(2) requires personal data be collected only by lawful and fair means in the circumstances of the case. **Data users should not collect personal data using CCTV under any circumstances which may be considered unfair**, i.e., in places where individuals would have a reasonable expectation of privacy (e.g. changing rooms). Besides, the use of CCTV at home for non-domestic purposes should be properly justified and should not capture images showing activities inside a bathroom or private rest areas. Similarly, the use of pinhole cameras should be avoided, and **covert CCTV surveillance should only be used with strong justification and as a last resort**.

Data users should note that collecting personal data via CCTV for unlawful purposes violates DPP 1 under the PDPO. Surreptitious observation or recording in places where any individual has a reasonable expectation of privacy (e.g. changing rooms or bedrooms), recording or observation of intimate parts (such as "upskirting"), or publishing AI-generated deepfake intimate images may constitute the offence of voyeurism[5] or other criminal offences under the Crimes Ordinance, Cap. 200[6].

[5] Section 159AAB of the Crimes Ordinance, Cap. 200

[6] For example, sections 159AAC, 159AAD and 159AAE of the Crimes Ordinance, Cap. 200

Is It Necessary to Use CCTV?

Necessity and Proportionality, Data Minimisation

When a data user collects personal data, in addition to the above requirement that the collection must be for a lawful purpose directly related to a function or activity of the data user, DPP 1(1) also stipulates that the data collected must be necessary, adequate but not excessive in relation to that lawful purpose[7].

In assessing whether it is necessary to use CCTV, the key question to ask is – ***Is the use of CCTV in the circumstances of the case justified for achieving the purpose and are there any less privacy-intrusive alternatives?***

For the responsible use of CCTV, data users should conduct an objective pre-installation assessment to ensure that the use of CCTV constitutes a proportionate response, taking into account the severity of the problem at hand and the degree of intrusion into personal data privacy. When considering whether to install CCTV, the following steps should be taken:

- Identify the problem to be addressed and assess whether the use of CCTV can effectively address the problem;
- Gather relevant information to assess whether CCTV can effectively address the problem (e.g. if a property management company intends to use CCTV to tackle the problem of objects being thrown from heights, records of similar incidents and an assessment of the effectiveness of installing CCTV in preventing or detecting the incident);
- Determine whether there are other less privacy-intrusive alternatives to better address the problem or options that could be used together with CCTV to minimise the collection of personal data;
- Before enabling the video recording function, assess whether continuous recording is necessary;
- Assess the quality of the equipment needed for the purpose, e.g. determine whether low resolution or poor quality recordings may be adequate to achieve the purpose, or whether there is genuine need for high-resolution equipment to record detailed facial images of individuals;
- In the absence of a specific problem that needs to be solved by obtaining audio recordings, refrain from enabling audio recording as it is generally considered more privacy-intrusive;
- The use of in-built facial recognition technology and individual tracking functions must be supported by strong justification as facial identification and tracking of individuals are not normally expected by the public;
- Consult, where practicable, with potentially affected individuals to understand their concerns and consider taking steps to address those concerns and minimise the intrusion into privacy; and
- Clearly determine the extent of monitoring required (e.g. avoid permanent use of CCTV to address temporary needs).

---

7 DPP 1(1)(b) and (c)

Should a Privacy Impact Assessment (PIA) be Conducted?

Privacy Impact Assessment

Before installing or using a CCTV system, a privacy impact assessment should be carried out by the data user to identify the key privacy risks, taking into account at least the following factors:

- The data user's functions and activities;
- The nature of the personal data involved;
- The number of data subjects likely to be affected;
- The gravity of harm that may be caused to the data subjects should their personal data be improperly handled; and
- Whether a data processor has been appointed to carry out data processing on behalf of the data user.

After identifying the key privacy risks, the PIA should set out the operational and technical measures to be deployed to prevent or mitigate such risks, insofar as it is practicable to do so. For more information on how to conduct a PIA, data users are recommended to refer to the PCPD's information leaflet on *Privacy Impact Assessments (PIA)*[8].

How to Properly Provide Notices?

Transparency on Collection of Personal Data

DPP 1(3) requires data users to inform data subjects of specified matters on or before collecting their personal data, including the purpose for which the personal data is to be used. Therefore, **potentially affected individuals should be explicitly informed that they are subject to CCTV surveillance**. One of the effective ways to achieve this is to place conspicuous notices in the vicinity of the monitored areas. This is particularly important where the CCTV cameras are discreetly located, or exceptionally located in places where people may not expect to be subject to surveillance.

The notices should contain information about the data user operating the CCTV system (including information about the operator of the system and the point of contact for personal data privacy issues) and the specific purpose of the surveillance.

[8] See https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

Transparency of Policies and Practices

DPP 5 requires data users to take all practicable steps to ensure that a person can ascertain their policies and practices in relation to personal data. To comply with this requirement, data users should establish CCTV monitoring policies and/or practices that are accessible to data subjects. It is recommended that relevant policies and practices cover:

- The types of personal data held by the data user;
- The purposes for which the personal data is collected;
- To whom the recordings may be disclosed or transferred; and
- The data retention policy.

Data users must ensure that relevant staff members are aware of and comply with relevant policies and practices. Appropriate training and guidance should be provided to the staff who operate the CCTV system or have access to the recordings. Effective supervision should also be put in place. Any misuse or abuse of the CCTV system or recordings should be reported to senior staff for follow-up actions, including disciplinary actions.

How to Properly Store the Recordings?

Retention Limitation

DPP 2(2) stipulates that data users shall take all practicable steps to ensure that personal data is not kept longer than is necessary for the purpose (including any directly related purpose) for which the data is or is to be used. **Personal data collected by the CCTV systems should be deleted as soon as practicable once the purpose of collection is fulfilled**. For instance, CCTV footage recorded for security purposes should be regularly and securely deleted if no security incident is discovered or reported.

If third-party contractors are engaged to maintain or enhance the CCTV systems, and have access to CCTV footage containing personal data, DPP 2(3) requires data users to adopt contractual or other means to prevent any personal data transferred to contractors from being kept longer than is necessary for processing of the data. For example, if a data user receives a data access request to obtain a data subject's personal data from CCTV footage and a contractor is engaged to extract the relevant footage, the data user must take steps to ensure that the contractor will not retain the footage longer than necessary. Data users may refer to the PCPD's information leaflet on *Outsourcing the Processing of Personal Data to Data Processors*[9] for details.

[9] See www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf

Data Security

DPP 4(1) stipulates that data users shall take all practicable steps to ensure that the personal data held by them is protected against unauthorised or accidental access, processing, erasure, loss or use. **Adequate security measures must be in place to prevent unauthorised and accidental access (both physically and remotely via the network) to, processing, erasure, loss or use of the CCTV systems and the recordings**. For instance:

- CCTV recordings should be stored in encrypted formats, both at rest and in transit;
- If recordings are stored in the cloud, data users are responsible for ensuring that cloud service providers are able to provide sufficient security. For details, data users may refer to the PCPD's *Guidance on Cloud Computing*[10];
- Data users should also ensure that adequate security measures are in place to safeguard the physical security of CCTV recording storage devices. For example, hard drives containing CCTV footage should be kept in locked facilities, with access restricted to authorised staff; and
- Data users should maintain a log to document access to the CCTV system and storage devices, as well as transfers and movements of recordings.

If a data user engages contractors that would have access to recorded images, DPP 4(2) requires the data user to adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the contractors.

Can CCTV Recordings be Transferred to Third Parties?

Purpose Limitation

DPP 3 stipulates that personal data shall only be used (including "transfer" and "disclose") for the purposes for which it was collected or for a directly related purpose. In other words, unless the data subject gives prescribed consent (which means express consent given voluntarily) or an exemption under Part 8 of the PDPO applies (see Example 4), personal data should not be used for a new purpose.

Example 2:
A door-to-door salesperson visited a customer's home to sell products. The process was recorded by the CCTV camera installed by the customer for security purposes. Dissatisfied with the salesperson's service, the customer subsequently shared the recording of the visit on a social media platform. As the publication of the recording constitutes a new purpose and consent from the salesperson (being the data subject) was not obtained, the customer contravenes the requirements of DPP 3.

[10] See https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf

Example 3:
If a person discloses personal data collected through a CCTV system (e.g. by uploading the footage to online social media platforms) without the relevant consent of the data subject with the intent to cause, or being reckless as to whether such disclosure would cause or would likely cause, any specified harm[11] to the data subject or his/her family member, the discloser may commit a "doxxing" offence under section 64(3A) or (3C) of the PDPO. Doxxing is a serious offence and the offender may be liable on conviction to a fine of up to HK$1,000,000 and imprisonment for up to five years.

Exemptions

Pursuant to the exemption provisions under section 58(2) of the PDPO, in certain specific circumstances, such as for the prevention or detection of crime, or the prevention or remedying of unlawful or seriously improper conduct or dishonesty, if a data user has reasonable grounds for believing that failure to use the data would likely prejudice the aforementioned matters, the data user may use the personal data for a new purpose without obtaining the prescribed consent of the data subject.

Example 4:
It is not uncommon for a data user (e.g. building management company) to be asked by a law enforcement agency (e.g. the police) to provide CCTV recordings for criminal investigations. In such cases, the data user may consider invoking the exemption under section 58(2) of the PDPO to use (including transfer or disclose) the relevant footage containing personal data without obtaining the data subject's prescribed consent.

Regular Reviews

Regular compliance checks and audits are recommended for data users to review the effectiveness of the safeguards implemented for CCTV systems.

Regular reviews should also be conducted to consider whether the continuous use of CCTV systems still serves the initial purpose of installation. If the use of CCTV is no longer necessary or if less privacy-intrusive alternatives are available to achieve the same purpose, the data user should discontinue the use of CCTV systems.

[11] Pursuant to section 64(6) of the PDPO, "specified harm", in relation to a person, means harassment, molestation, pestering, threat or intimidation to the person; bodily harm or psychological harm to the person; harm causing the person reasonably to be concerned for the person's safety or well-being; or damage to the property of the person.

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

PCPD.org.hk

政府資助機構
Government-funded organisation

Tel : **2827 2827**
Fax : **2877 7026**
Address : **Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

PCPD website
pcpd.org.hk

Download this publication

Disclaimer
The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

October 2025 (Third Revision)