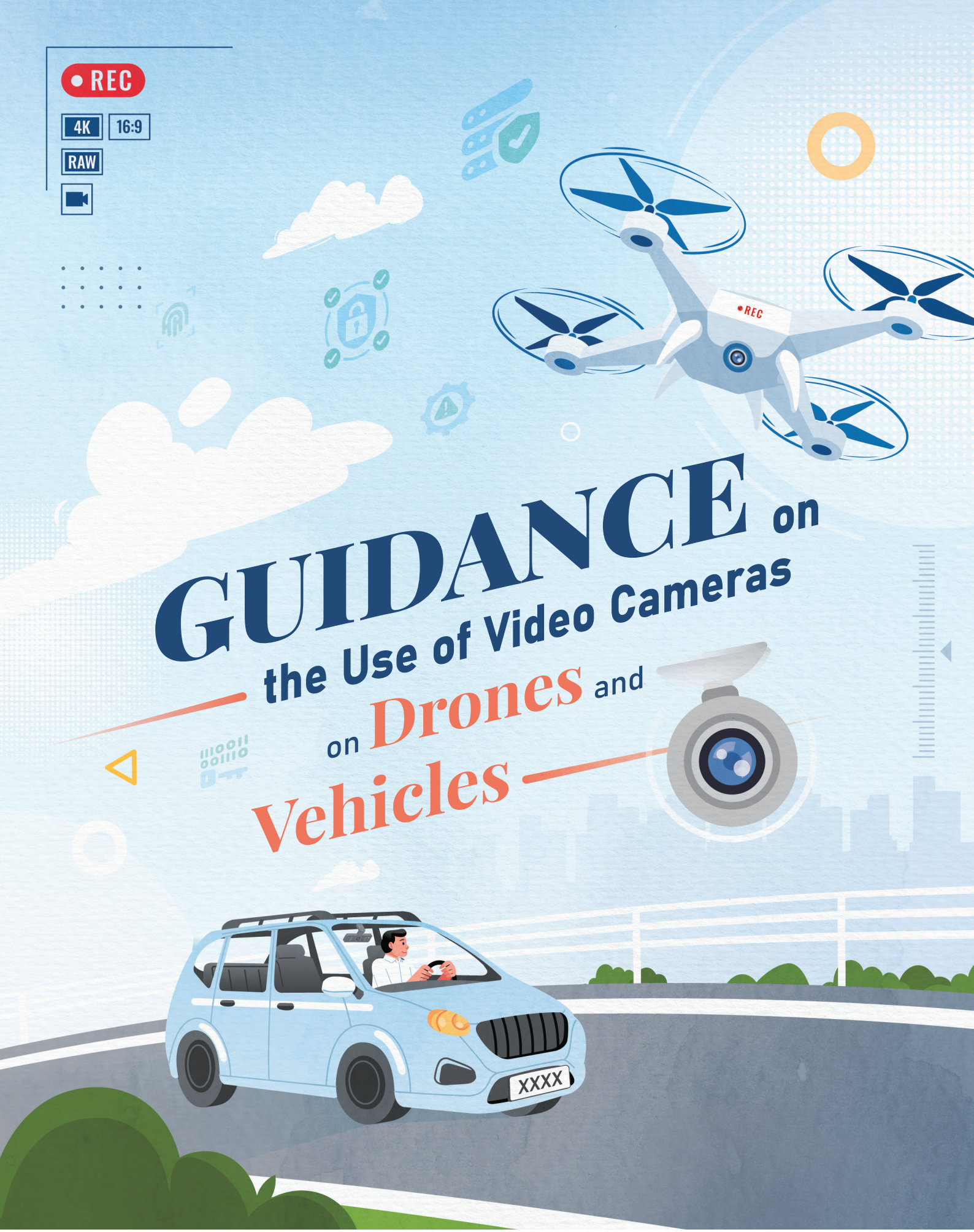


GUIDANCE on the Use of Video Cameras on Drones and Vehicles

PCPD
HK

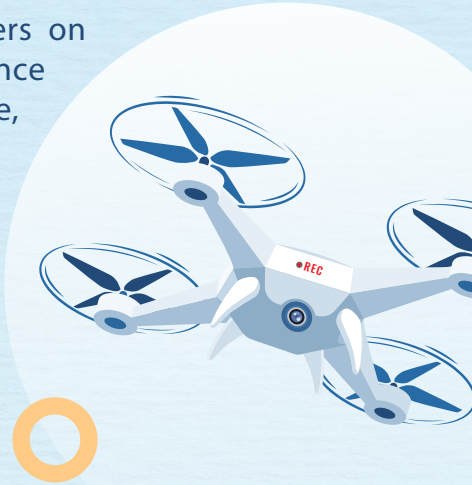
PCPD.org.hk

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

Introduction

With the advancement of technology, the use of various types of surveillance cameras other than closed-circuit television ("CCTV") has become increasingly prevalent in recent years, such as the use of unmanned aircraft systems (commonly known as "drones") for photography, surveying and monitoring, as well as in-vehicle cameras for surveillance and monitoring. While these technologies bring convenience across various sectors, they may involve the collection of personal data, and thus the privacy risks they pose should not be overlooked.

This guidance provides practical recommendations to data users on the responsible use of drones and in-vehicle cameras in compliance with the requirements under the Personal Data (Privacy) Ordinance, Cap. 486 ("PDPO"). Data users using camera-equipped drones or in-vehicle cameras for surveillance and monitoring purposes should also refer to the *Guidance on the Use of CCTV Surveillance*[1] issued by the Office of the Privacy Commissioner for Personal Data to ensure compliance with the PDPO.



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.

1 See https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_cctv_surveillance.pdf

Camera-equipped Drones

Drones can be used in many ways to bring about significant societal and economic benefits, such as land surveying, rescue operations and filmmaking.

In view of the Small Unmanned Aircraft Order, Cap. 448G ("SUA Order"), drone operators must comply with the corresponding regulatory requirements regarding registration of drones and remote pilots, training and assessment, equipment, operating requirements, insurance and other matters[2]. Depending on the risks involved in the use of drones, prior approval of the use of drones from the Civil Aviation Department may be required.

In view of their unique attributes, camera-equipped drones may be used to collect personal data:

- ☑ Being small, portable, mobile and cheap, drones of any size may be improperly used to track individuals' activities persistently over time and over a wide area;
- ☑ They are generally controlled remotely and it would be difficult for the public to predict where drones may be operating and to find out who the operators are; and
- ☑ When equipped with advanced surveillance technologies such as telephoto lenses and infrared sensors, they possess sophisticated capabilities such as capturing data from a distance with a fine level of detail.

Example 1:

- Camera-equipped drones may be deployed for purposes such as building inspection or product delivery. When operated near residential areas, the drones may inadvertently capture facial images of individuals in the area. If collection of personal data is involved, data users should observe the relevant requirements under the PDPO.
- However, if the facial images captured by the cameras would be automatically detected and blurred/masked such that no individual could be identified from the resulting footage, the footage may not fall within the meaning of "personal data" under the PDPO.

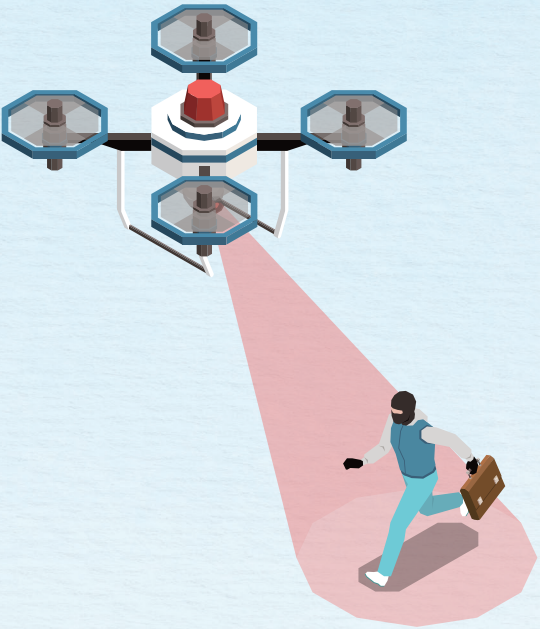
2 See https://www.cad.gov.hk/english/sua.html

Example 2:

Where camera-equipped drones operate at a high altitude or adopt low-resolution cameras such that it would not be reasonably practicable to ascertain the identity of any individual from the footage captured, the collected data may not amount to "personal data" and the PDPO would not apply.

Example 3:

In cases where camera-equipped drones are deployed for aerial patrols for investigation and enforcement purposes, the recorded footage may be used to gather evidence of criminal activities and help identify suspects. The collected data would likely include "personal data", so the relevant data user must pay heed to the requirements and relevant exemptions under the PDPO.



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, data users may use personal data for new purposes without obtaining the prescribed consent (i.e. express consent given voluntarily) of the data subject. For example, if the footage recorded by a camera-equipped drone captures criminal activities or the appearance of suspects, and the footage may assist law enforcement agencies in conducting further investigation or making an arrest, 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.

In light of the potential intrusion on privacy, drone operators should be particularly mindful of the need to respect people's privacy and ensure compliance with the requirements under the PDPO. **Strong justification is needed for using camera-equipped drones to conduct surveillance, and alternative use of less privacy-intrusive means should be seriously considered.** Drone operators should assess whether the intrusion on privacy is proportional to the benefits to be derived, as otherwise it could amount to excessive and/or unfair collection of personal data under Data Protection Principle 1(1) and/or (2).

Below are some tips on the responsible use of drones:

Flight path

Flight paths should be carefully planned to avoid flying close to individuals or private premises. For example, drones should take off at a location as close as possible to the area they need to cover. The flight paths must also comply with the operating requirements stipulated in the SUA Order.

Recording and retention

Drone operators should consider whether video recording and/or audio recording is necessary during the operation of drones. **If recording is intended, the recording criteria (including what, where and when to record as well as the quality and resolution of the footage captured) should be pre-defined to avoid excessive collection of data, especially personal data.** Depending on the purpose of the drone operation, drone operators may consider leveraging technology that automatically detects and applies blurring or masking to any facial images captured to avoid unnecessary collection of personal data. Drones may go off course by accident and record scenes unintentionally. Hence, policy regarding the erasure of irrelevant recordings and personal data retention policy should be established.

Security

Use encryption for wireless transmission of images to avoid interception or unauthorised access. If the drones have a recording function, the storage of the footage captured, whether on physical portable storage devices or in cloud storage, should be safeguarded with robust security measures. Furthermore, access control should be considered to prevent the recordings from falling into the wrong hands in the event that the drones are accidentally lost or stolen.

Notice

Transparency about drone operations is essential for building trust with the affected individuals, which **includes clearly communicating the purposes and operational details of drone usage.** However, informing these individuals via notices may pose challenges in practice, making it necessary to explore alternative creative approaches, such as the following:

- Before operating drones on or in close proximity to private premises, notifying potentially affected individuals (such as occupants of the premises) of the intended drone operation in advance;
- Before operating drones in public areas, pre-announcing the drone operation by putting up conspicuous notices in the vicinity of the areas concerned and/or via public channels;
- Attaching QR codes on relevant notices to link to the Personal Information Collection Statement and/or privacy policy;
- Using flashing lights to indicate the operation of drones and that recording is taking place;
- Putting corporate logos on the drones;
- Requiring crew members to wear clothing that identifies the organisation; and
- Putting up notices or large banners with the Personal Information Collection Statement and contact details at launch sites.

In-Vehicle Cameras

In-vehicle cameras, or “dash cams” or “car cams”, are typically inward- and/or outward-facing cameras mounted or pre-installed in vehicles to record the vehicle compartment, the journeys and safety or traffic incidents. In-vehicle cameras can enhance both driving safety and road safety in general as the footage recorded by in-vehicle cameras may be used as evidence in the event of disputes or incidents.

Inward-facing Cameras

Inward-facing cameras are often used for monitoring the vehicle compartment and may come with an audio recording function. These cameras may serve as a deterrent against improper conduct. Additionally, where inward-facing cameras are equipped with more advanced functions such as automated detection of signs of drowsiness or distraction from the driver, they may help to mitigate the risk of accidents caused by driver fatigue or inattentiveness.

Video recordings made by such cameras are likely to capture the faces of the driver and passengers, and audio recordings are likely to record conversations taking place in the vehicle. Continuous recording of the driver and/or passengers inside the compartment without notifying the individuals concerned may be considered intrusive to individuals’ privacy. If such recordings are misused, e.g. disclosed to the public without passengers’ consent, the passenger(s) concerned may suffer harm or become victims of doxxing, harassment or bullying.

Outward-facing Cameras

Outward-facing cameras can capture footage of accidents or dangerous driving behaviour. They may record identifiable images of other road users, such as vehicle registration marks of other vehicles and images of surrounding pedestrians. Similar to drones, outward-facing cameras are small, portable and covert. Therefore, care must be taken to avoid intruding upon personal privacy.

Responsible Use of In-Vehicle Cameras

Below are some tips on the responsible use of in-vehicle cameras for data users (including drivers who have installed in-vehicle cameras in their vehicles and organisations that have instructed their employees to use in-vehicle cameras):

Providing adequate justification

Consider activating the recording functions of inward-facing cameras only when the vehicle is in motion. Data users should provide adequate justifications for continuous recording, especially if both video and audio are recorded.

Notice and transparency

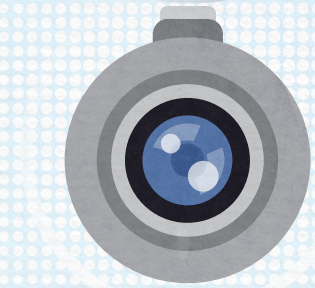
Compared to passengers travelling on high-capacity public transportation (such as trains and buses), passengers travelling in private vehicles (such as taxis), who are situated in an exclusive space, generally have a higher expectation of privacy during the ride. Therefore, **data users should take all practicable steps to notify passengers of the existence and functions of in-vehicle cameras and collect personal data by lawful and fair means.** For example, where a taxi is installed with an inward-facing camera, the taxi driver may consider putting up notices on the exterior of the taxi or at conspicuous locations inside the compartment, such as on the dashboard and on the back of the headrests facing the passenger seats.

Handling and retention of recordings

To reduce the risk of misuse of any recordings by in-vehicle cameras, **data users should establish a personal data retention policy that stipulates a reasonable retention period**, and delete recordings containing personal data, in which no incidents have arisen or been reported, in a timely manner. Data users should not disclose recordings containing personal data to third parties for purposes other than the original intended use, e.g. to record a journey in case of occurrence of any safety or traffic incident, unless the explicit and voluntary consent of the passenger concerned has been obtained, or an exemption under Part 8 of the PDPO applies.

Data security

The recordings stored in the in-vehicle cameras should be properly secured through physical and technical measures to prevent unauthorised or accidental access or copying. Where possible, non-removable solid-state storage media should be preferred for the storage of recordings over removable storage media such as memory sticks or cards. Other recommended security measures include storing recordings in encrypted form, implementing appropriate access control, adopting measures to prevent direct replay of recordings on the device, and attaching the camera securely to minimise the risk of loss or theft.



PCPD.org.hk

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

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**

E-mail : **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