# Protection of Personal Data Privacy – Guidance for Property Management Sector

## Summary

**This Guidance covers the following areas:**

- **Collecting personal data of residents or visitors** – In any activities involving the collection of personal data, property management bodies should collect personal data that is necessary, adequate but not excessive in relation to the purpose of such activities; provide the data subject with a "Personal Information Collection Statement", and establish a retention period for the personal data collected during the relevant activity. Property management bodies should also ensure that the use (including disclosure) of the personal data is confined to the purpose for which the data was originally collected or for a directly related purpose, unless the relevant person's consent is obtained or the exemptions under Part 8 of the Personal Data (Privacy) Ordinance are applicable.

- **Recording of Hong Kong Identity (HKID) Card numbers of visitors** – Before collecting the visitors' HKID Card numbers, the property manager must consider other methods of verifying the visitors' identities, and whenever practicable, should give the visitors the option to choose less privacy-intrusive alternatives to verify their identities.

- **Visitors' log book** – The property manager should ensure that the previous entries in the visitors' log book are concealed from visitors or irrelevant parties. The personal data recorded in the log book should be deleted as soon as practicable after the purpose of collection is fulfilled.

- **Handling of complaints from residents** – The property manager should first inform the complainant that his personal data is to be used for handling matters relating to the complaint, and make known to the complainant the persons to whom his personal data may be disclosed. To avoid misunderstanding, the property manager may obtain the complainant's written consent before referring the complaint to a third party.

- **Display of notices containing personal data** – Property management bodies should carefully consider and assess the necessity, extent and duration of publishing a notice containing an individual's personal data. No HKID Card number or contact information of an individual should be displayed in any public place.

- **CCTV located at common areas of buildings** – People should be explicitly notified that they are subject to CCTV surveillance. Such notices should contain details of the data user operating the CCTV system and the specific purpose of surveillance, etc. The property management bodies should also formulate policies on the retention and security of the collected personal data, and handle the recorded images with proper care.

- **Proper storage of personal data** – Property management bodies need to ensure that the personal data stored in traditional paper or electronic form is not affected by unauthorised or accidental access, processing, erasure, loss or use. Access should be confined to a "need-to-know" basis, and practical measures should be taken (e.g. establishing access rights or setting passwords) to control the same.

- **Smart property management** – Property management bodies should exercise extra caution when using smart or electronic means to process personal data of residents (e.g. when communicating with staff or residents through communication apps), to avoid data leakage and inappropriate online disclosure of residents' personal data. If property management bodies wish to use cloud services, they should carefully assess the reliability of the suppliers and relevant contractors/subcontractors, the content of their services, the security measures, and whether the terms and conditions set out in the contracts meet all requirements of data protection. In any event, property management bodies must thoroughly assess the benefits and risks, as well as understand the importance of personal data protection before adopting each smart or electronic measure.

- **Outsourcing of services** – Property management bodies should promulgate clear guidelines and work procedures in relation to the handling of personal data, and effectively monitor the performance of frontline staff.

# Introduction

Protecting and respecting residents' personal data would enable property management bodies (e.g. owners' corporations, owners' committees, mutual aid committees and property management companies) to earn residents' trust and support in fulfilling their management duties. On the other hand, improper handling of personal data may give rise to disputes and even discourage residents from participating in building management.

The scope of the work of property management bodies involves a vast amount of personal data of residents, visitors and employees. This Guidance aims to assist property management bodies to understand the application of the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**) on their daily routine property management works.

# Collecting personal data of residents or visitors

In any activities involving the collection of personal data, property management bodies should collect personal data that is necessary for or directly related to their functions and purposes of such activities, and ensure that the personal data collected is adequate but not excessive in relation to the said purposes.

## Issuance of resident cards

It is common for property managers of private housing estates to install electronic door access card systems at the building entrances. Occupants may use resident cards to enter the buildings or use clubhouse facilities.

For the purpose of issuing resident cards, a property manager usually requires a flat owner to provide, on the resident card application form, information about the authorised users of the resident cards. In this regard,

Data Protection Principle (**DPP**) 1(1) of the PDPO requires a property manager to collect only personal data that is necessary for the purposes for which the data is to be used, and that the data collected is adequate but not excessive for those purposes.

An authorised user named on the application form can be traced or identified with the flat owner concerned. The collection of the authorised user's name and contact telephone number on the resident card application form will therefore generally suffice for such tracing purposes. The HKID Card number of an authorised user is therefore not necessary in the application.

## Organising activities or collecting views

From time to time, property management bodies may organise activities for residents or collect their views, which may involve the collection of residents' personal data. Property management bodies should carefully assess whether the personal data to be collected is necessary and adequate for achieving the purposes of the activity concerned in order to avoid collecting excessive personal data.

In addition, if property management bodies intend to take photos or record a video in the activities, as a matter of good practice, they should notify the participants and provide them with a "Personal Information Collection Statement" (**PICS**) stating the purpose for which the data is collected, regardless of whether such photo taking/video recording involves collection of personal data.

## Providing a PICS

Under DPP1(3), before or during the collection of the personal data of a resident/visitor/another person, property management bodies should take all practicable steps to inform him of the following:

(i) whether it is obligatory or voluntary for him to supply his personal data and, where obligatory, the consequences for failing to supply the data;

(ii) the purpose for which the data is to be used;

(iii) the classes of persons (if any) to whom the data may be transferred; and

(iv) his rights to request access to and correction of the data, and the name or job title, and address of the person to whom such request may be made.

Such notification is usually called a PICS. Apart from posting the relevant PICS in conspicuous places in the lobby of the building, property management bodies should also consider including the PICS in the personal data collection form to ensure that the persons from whose personal data is collected is informed of the matters referred to in the PICS, in order to comply with the requirements of DPP1(3).

Meanwhile, property management bodies should establish a retention period for the personal data collected on each occasion before collecting the residents' personal data, so as to ensure that personal data is not kept longer than necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used, in order to comply with the requirements under DPP2(2). In addition, in accordance with DPP3, property management bodies should only use (including disclose) a resident's personal data for the original or directly related purpose for which the data was collected, unless with the resident's express and voluntary consent or the exemptions under Part 8 of the PDPO are applicable.

**Property management bodies can only collect necessary, adequate but not excessive personal data. They should also provide persons whose personal data are collected with a clear and concise "PICS", establish a retention period for the personal data collected in each activity, and ensure that the collected personal data be used only for the original purpose for which the data was collected.**

# Recording of HKID Card numbers of visitors

## Collecting visitors' HKID Card numbers

For security reasons, a property manager needs to monitor visitors who are permitted to enter the building. If it is not feasible for a property manager to monitor a visitor's activities inside the building, the recording of his HKID Card number by the property manager at the entrance of the building is allowed under paragraph 2.3.4.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers[1] (**PI Code**) issued by the Privacy Commissioner for Personal Data (**Commissioner**). However, pursuant to paragraph 2.2 of the PI Code, the property manager must, wherever practicable, give the visitor the option to adopt less privacy-intrusive alternatives, other than providing his HKID Card number.

Examples of such alternatives include identification of the visitor by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through confirmation with the occupant (e.g. the visitor is picked up by the occupant at the lobby), it is not necessary to record the visitor's HKID Card number as an additional security measure. If a visitor is going to undertake work in the building, the property manager may accept his staff card or work permit as proof of identity. In any event, collection of HKID Card number should be resorted to only after alternative means of verification are duly considered.

Under certain circumstances, the property manager may need to further collect personal data from the visitors; but again, the data collected should also be necessary, adequate but not excessive for the collection purposes. For example, during the COVID-19 pandemic, when requesting visitors to make health declarations, the property manager may simply ask them to confirm whether they have visited or live in a building where the confirmed patient is located, rather than asking them to provide details of their addresses.

## Visitors' log book

A log book containing visitors' personal data such as their HKID Card numbers should be handled by authorised staff with care, as DPP4(1) imposes a duty on a data user to take all reasonably practicable steps to ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use.

A property manager should ensure that the previous entries in the log book are concealed from visitors, and the security staff should access and read these entries only when a need arises (e.g. when an incident of security concern happens).

DPP2(2) imposes a duty on a data user to ensure that there is no excessive retention of personal data.

1 https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/picode_en.pdf

Therefore, the personal data recorded in the log book should be deleted as soon as practicable after the purpose of collection is fulfilled. It is recommended that entries in the log book be deleted regularly and not be retained over one month if no incident of security concern arises.

**A clear PICS and notice of the alternatives to the provision of HKID Card number should be given to visitors. In addition, previous entries in a visitors' log book should be concealed from visitors/irrelevant parties, and visitors' entries should be deleted regularly and not be retained longer than necessary.**

## Handling of complaints from residents

When a property manager receives a complaint from a resident about matters concerning the building or an act of another resident, the complainant's personal data may be collected for handling the complaint. As a matter of good practice, the property manager should first inform the complainant that the data is to be used for handling matters relating to the complaint, and make known to the complainant the persons to whom his personal data may be disclosed (e.g. referral to a government department for follow-up), and act with respect for the complainant's wishes. To avoid misunderstandings, the property manager may obtain the complainant's written consent before referring the complaint to a third party.

Any use or disclosure of the personal data of the complainant should be confined to the handling of the complaint, or directly related matters, in compliance with DPP3(1), which requires that personal data shall not, without the prescribed consent[2] of the data subject, be used for a new purpose[3].

There may be occasions where a complainant does not wish his identity to be disclosed to other parties. If non-disclosure of the complainant's identity does not affect the handling of the complaint, the property manager should accommodate the complainant's wish. If non-disclosure of the complainant's personal data makes it impracticable for the property manager to deal with the subject matter(s), then the property manager should explain this difficulty to the complainant.

**Inform a complainant in the first place that his personal data is to be used for dealing with the complaint and the person to whom his personal data may be disclosed.**

## Display of notices containing personal data

Property management bodies may have to inform owners of building management affairs by the public display of notices[4]. In doing so, property management bodies should carefully consider and assess the necessity and extent of publishing information containing an individual's personal data. An individual's personal data not necessary for the purpose of posting the notice must be edited out (e.g. during the pandemic, when any occupant tests positive for COVID-19, there is no need for the property management bodies to disclose the personal data of that occupant in its notice when updating other residents about the positive case. In most circumstances, the disclosure of the names and personal data of confirmed patients in the notice would be deemed unnecessary or disproportionate).

2 "Prescribed consent" means an express consent given voluntarily which has not been withdrawn in writing.

3 "A new purpose" means any purpose other than the purpose for which the data was to be used at the time of the collection of the data or a directly related purpose.

4 For example, the Building Management Ordinance (**BMO**) requires the display of the notices and minutes of the general meeting of an owners' corporation and the meeting of the management committee in a prominent place in the building for a prescribed period of time.

While an owners' corporation is obliged to display in a prominent place in the building a notice[5] containing particulars of the legal proceedings to which the owners' corporation is a party, it will generally be sufficient for the capacity of the other parties, the case number, the forum of the case, the nature of the case and the amount claimed or remedies sought under the action to be disclosed in such notice. No HKID Card number or contact information (e.g. phone number and email address) of an individual should be displayed in any public place.

Excessive disclosure of personal data (e.g. a complaint letter against an owners' corporation with the telephone number of the complainant) or displaying personal data with ulterior motives (e.g. a name list of owners who have unpaid management fees) may therefore contravene the requirements under DPP3.

**An individual's personal data is not to be published in management notices unnecessarily, and in particular, the HKID Card number or contact information of an individual is not to be displayed in public.**

## CCTV located at common areas of buildings

The use of CCTV for security reasons has become increasingly common. Since CCTV may capture extensive images of individuals, its use should be properly handled and arranged to avoid intrusion into the personal data privacy of individuals.

### Informing passers-by about CCTV in operation

CCTV cameras should be positioned in a way that will not unnecessarily intrude into the personal data privacy. Property management bodies should explicitly inform the public that the relevant area is subject to CCTV surveillance. An effective way is to post conspicuous notices at the entrance to the monitored area as well as inside the area as reinforcement. The notices should contain details of the data user operating the CCTV system, the specific purpose of surveillance, and the person to whom matters relating to the handling of personal data can be raised.

### Identifying and managing privacy risks

If a property management body has installed a CCTV with an intent to identify individuals (e.g. adopts artificial intelligence technology or camera with high resolution), this may constitute a collection of personal data and the requirements under the PDPO must be complied with. The requirements cover the need to inform data subjects of the matters under DPP1(3) as mentioned above, and the restrictions on use of data under DPP3. Depending on the specific operational circumstances, a data user may consider whether the exemptions under Part 8 of the PDPO (e.g. section 58(1)(a) for the prevention or detection of crime) are applicable.

The Office of the Privacy Commissioner for Personal Data (**PCPD**) recommends property management bodies intending to install CCTV systems to conduct a Privacy Impact Assessment to understand the operation and functions of the CCTV system, define the purpose of the CCTV system, and identify privacy issues arising from the installation, in order to assess whether there is a genuine need for the installation of the CCTV system and whether there are less privacy-intrusive alternatives. For details, please refer to the

5 Section 26A of the BMO

information leaflet on "Privacy Impact Assessment"[6] issued by the PCPD.

### Storage and security of CCTV recordings

Property management bodies should formulate policies on the retention and security of the collected data and handle the CCTV recorded images properly. Property management bodies should decide the retention period of the recorded images according to their operational needs, and destroy the recorded images regularly in a reliable manner to comply with the requirements under DPP2(2). Moreover, in order to prevent unauthorised access to the CCTV system, property management bodies must take all practicable security measures (e.g. to implement appropriate access control, to specify who may access the recorded images under what circumstances), to protect the personal privacy of residents. Furthermore, access to areas used by the property management bodies for viewing, storing or processing CCTV images should be restricted to authorised persons only.

The document titled the "Guideline on CCTV Surveillance and Use of Drones"[7] issued by the PCPD provides guidance on whether CCTV should be used and how they can be used responsibly.

**Property management bodies must define the purpose of installing CCTV systems and identify the privacy issues arising from the installation. After installation, they must also handle video recordings properly, establish retention and security policies, and use CCTV responsibly.**

## Proper storage of personal data

To comply with the security requirements under DPP4(1), property management bodies should take all practicable steps, including adopting appropriate privacy enhancement systems and measures, to protect personal data from unauthorised or accidental access, processing, erasure, loss or use.

### Take practicable steps to protect personal data

Property management bodies should define the types of personal data to be collected from residents, identify the persons who have authorisation or operational needs to handle and access such data, include such access rights in the policy for handling personal data, and clearly communicate such information to relevant management staff or members, to ensure that they do not disclose residents' personal data to persons who have not been authorised to handle such data.

Property management bodies collecting personal data in traditional paper form (e.g. resident registration forms, complaint letters, etc.) should have physical security measures in place to prevent unauthorised access to and use of personal data. Such measures include using access control systems to limit staff entry to the storage room and storing personal data in locked file cabinets carefully. When accessing data, the person responsible for data storage should make a proper record for trail audit purposes in the future, and only allow access by key-keepers to retrieve the personal data on a "need-to-know" basis. The person accessing the data should also return the data as soon as possible after completing his duties to reduce the risk of data leakage.

6 https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

7 https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf

For personal data stored electronically, property management bodies should make use of proper encryption programmes and system access management, and adopt measures such as identity authentication management to restrict and monitor people who have access to personal data in IT systems. The relevant electronic devices should be password-controlled, and the password and access to such data should be granted to staff members on a "need-to-know" basis. For an electronic device that requires login, avoid sharing a single password among multiple users, and ensure that the device is logged out every time after use or upon departure. In addition, property management bodies should regularly monitor and review the access record of personal data, to check where its staff members have abnormal access to residents' personal information. Property management bodies should also develop a comprehensive data security policy, supplemented by regular training, to enhance staff awareness of protecting personal data privacy.

Meanwhile, property management bodies should ensure that all electronic devices are installed with the latest security patches and anti-virus software, protected by firewalls, and that network connections are secure and reliable to prevent intrusion of hackers and computer viruses, and theft of personal data stored therein. Property management bodies should also ensure that work-related personal data stored in electronic devices has been encrypted, use strong passwords (e.g. a combination of letters, numbers and symbols), limit the number of failed login attempts, and prevent the transfer of data from company devices to personal electronic devices. Property management bodies should also use encrypted communication channels when transmitting documents containing personal data electronically. Regarding the use of portable devices (e.g. USB flash drive, tablet/notebook, mobile/smartphone) to store personal data of residents, on top of the above security measures, property management bodies should also refer to the "Guidance on the Use of Portable Storage Devices"[8] issued by the PCPD.

### Use of mobile electronic devices for work purposes

In recent years, it has become increasingly popular for property managers to use mobile electronic devices to communicate with residents and to conduct official business (e.g. contacting residents, taking photos and recording events in the estate, sending documents). An ideal way is for property management bodies to provide mobile electronic devices (e.g. cameras, smartphones and laptops) for their staff and formulate relevant policies and guidelines, in order to restrict the use of and access to the information stored in the devices. In addition, property management bodies should adopt the security measures described above for electronic devices to ensure the security of the personal data stored in the electronic devices.

**Property management bodies are required to take all practicable steps to protect residents' personal data, limit access of such data to "need-to-know" persons, and establish guidelines and practices for the use of electronic devices for work purposes to ensure the security of the data stored in the devices.**

## Smart property management

Property management has become smarter. In early years, property management bodies collected and processed personal data through the Internet[9]. Nowadays, property management mobile applications are getting more and more popular. The application of management measures such as electronic resident

8 https://www.pcpd.org.hk/english/publications/files/portable_storage_e.pdf

9 please refer to "Guidance for Data Users on the Collection and Use of Personal Data through the Internet" published by the PCPD : https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_internet_e.pdf

cards, electronic notices and QR code visitor cards inevitably involves the collection and storage of personal data through electronic means (e.g. collecting personal data of residents/visitors through online forms or electronic applications).

## Popularisation of property management applications

In recent years, some property management bodies have launched their own mobile applications for housing estates, allowing residents to read notices issued by the property management company, make appointments for domestic services such as housekeeping and laundry, ordering food, booking clubhouse services, and even settling management fees by mobile payment. This type of applications can also store electronic resident cards and support visitor registration by QR code.

Meanwhile, some property management bodies have also introduced an intelligent mobile patrol system, in which security guards are provided with smartphones. When they arrive at patrol points with sensors, they need to scan the sensors with their phones, and the phones will then pop up a to-do-list. The security guards can also upload photos and videos to the system, and the control centre can then be informed of the pending follow-ups through the corresponding mobile application.

The above example shows that property management bodies can collect and process a wide range of personal data through mobile applications. In designing such applications, property management bodies should incorporate privacy protection into the design, and assess the impact on personal data privacy arising from the introduction of the applications.

The document titled "The Best Practice Guide for Mobile App Development"[10] issued by the PCPD provides a clear and concise overview of the requirements of the PDPO and how to develop products and services in a manner consistent with the concept of privacy by design.

## Use of messaging groups and social media platforms

Members of the property management bodies may use messaging applications to communicate with one another on estate matters, and groups may be set up to facilitate communication. Disclosure and discussion of resident information at the time of communication should be avoided. If personal data of residents or staff must be involved, due consideration should be given to the list of recipients on "need-to-know" basis. For example, the property management bodies should opt for sending information to members individually (instead of posting in the group), and should not disclose the data to persons whose access to such data is not authorised.

Furthermore, when collecting and sharing information about the estate through social media platforms, property management bodies must comply with the requirements under the PDPO. For example, when collecting personal data from residents, they should provide a PICS; when uploading a post containing notices or photos, they should refrain from disclosing any personal data unless they have obtained the consent of the person concerned.

Property management bodies must be aware that information shared on messaging applications and social media platforms can be easily copied or permanently stored, and further disseminated. Therefore,

10 https://www.pcpd.org.hk//english/resources_centre/publications/files/Best_Practice_Guide_for_Mobile_App_Development_20151103.pdf

property management bodies should exercise extra caution when using messaging applications and social media platforms, especially if the instances involve disclosure of personal data, to avoid inappropriate and irreversible disclosure of such data in the group, or on the platforms.

### Privacy risks of cloud computing

As property management bodies move towards digitalisation or intelligentisation, there is a growing trend for organisations to fully adopt cloud services to replace in-house servers.

Personal data privacy concerns arising from the use of cloud computing are primarily related to the lack of control over the retention and security of personal data entrusted to a cloud service provider by an organisation. Therefore, generally speaking, organisations are required to adopt contractual or other methods to prevent the retention of personal data transferred to cloud service providers for a period of time longer than necessary to process the data, and to prevent unauthorised or accidental access, processing, deletion, loss or use of the personal data. When considering using cloud services, property management bodies should carefully assess the reliability of those providers or relevant contractors, contents of their services, and whether the terms and conditions set out in the contracts do meet all requirements of data protection.

In this regard, please refer to the information leaflet "Cloud Computing"[11] issued by the PCPD.

**Property management bodies should exercise extra caution when handling residents' personal data by smart and electronic means. Due consideration should be given to who will receive the data in accordance with the "need-to-know" basis, so as to avoid data leakage and improper disclosure. In addition, property management bodies must thoroughly assess the benefits, risks and importance of personal data protection before adopting each smart or electronic measure.**

## Outsourcing of services

Property management bodies usually employ temporary agents or engage service contractors to assist in their routine property management work, develop mobile applications or handle the maintenance of IT systems. Under section 65(1) and 65(2) of the PDPO, any act done, or practice engaged in, by an employee in the course of his employment or by an agent with the authority of the principal shall be treated as done or engaged in by his employer or principal (as the case may be) as well as by him.

For example, an owners' corporation may be held liable for the acts done or practices engaged in by the property management company in the course of managing the building on behalf of the owners' corporation. The property management company may also be held liable for the acts done or practice engaged in by its employees or agents.

Therefore, property management bodies should therefore promulgate clear guidelines and work procedures in relation to the handling of personal data, and effectively monitor the performance of frontline staff to ensure that their activities involving the collection or use of personal data comply with the relevant requirements under the PDPO.

11 https://www.pcpd.org.hk//english/resources_centre/publications/files/IL_cloud_e.pdf

Meanwhile, DPP2(3) provides that if a data user engages a data processor[12] to process personal data on its behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

In addition, DPP4(2) provides that if a data user engages a data processor to process personal data on its behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor.

For more specific guidance on the types of obligations to be imposed on data processors, please refer to the Information Leaflet "Outsourcing the Processing of Personal Data to Data Processors"[13] issued by the PCPD.

**Promulgate guidelines and work procedures to ensure handling of personal data in compliance with the PDPO.**

## Conclusion

The property management industry is closely related to the life of the public. As public expectation on personal data privacy protection grows, the public's demands on proper handling of personal data of residents or visitors by property management bodies are also on the rise. In addition, there are a lot of stakeholders in the property management industry. The estate management alone involves owners' organisations (e.g. owners' corporations, owners' committees), property management companies, various types of outsourced service providers, and more. It is insufficient for property management bodies to only do the least possible regarding personal data privacy protection to comply with the PDPO, while ignoring or giving insufficient regard to the residents or visitors' expectation of personal data privacy protection. The Commissioner encourages property management bodies to integrate the ideas of data privacy protection into their corporate governance and to demonstrate organisational commitment to personal data privacy; to designate a data protection officer from top management to develop personal data privacy management programmes and monitor the progress of the implementation of the same, and to nurture the culture of respecting privacy within the organisation through well-structured training. Handling personal data in line with the principles of respect, reciprocity and fairness would also demonstrate that an organisation handles personal data in a responsible manner and in compliance with the PDPO.

Proper protection of the personal data privacy of residents and visitors is an indispensable part of the optimisation and professionalism of the property management industry. By acting with a sense of respect for the personal data privacy of residents and visitors, property management practitioners are able to not only highlight their high quality services, enhance their competitiveness, and gain the trust of residents and visitors, but also minimise disputes and misunderstandings, and create a win-win situation for everyone to live and work in contentment.

12 "Data processor" means a person who processes personal data on behalf of another person and does not process the data for any of the person's own purposes.

13 https://www.pcpd.org.hk//english/resources_centre/publications/files/dataprocessors_e.pdf

PCPD website

Download this publication

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


**Enquiry Hotline** : **(852) 2827 2827**
**Fax** : **(852) 2877 7026**
**Address** : **Room 1303,13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
**Email** : **communications@pcpd.org.hk**




**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.


June 2022