Guidance on Property Management Practices

Executive Summary

This guidance note covers the following areas:

- **Personal data to be collected for issuing resident cards** – The collection of the authorised user's name and contact telephone number in the resident card application form will generally suffice for tracking purpose. The application form should contain a Personal Information Collection Statement ("PICS").
- **Recording of Hong Kong Identity ("HKID") Card numbers of visitors** – Collection of HKID Card number should be resorted to only after alternative means of verification is duly considered. The property manager should, wherever practicable, give the visitor the option to adopt other less privacy-intrusive alternatives.
- **Visitors' log book** – The property manager should ensure that the previous entries in the visitors' log book are concealed from visitors. The personal data recorded in the log book should be deleted as soon as practicable once the purpose of collection is fulfilled.
- **Handling of complaints from residents** – 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.
- **Display of notices containing personal data** – Property management bodies should carefully consider and assess the necessity and extent of publishing information containing an individual's personal data. No HKID Card number or contact information of an individual should be displayed in public place.
- **Use of CCTV covering common areas of buildings** – People should be explicitly informed that they are subject to CCTV surveillance. The notices should contain details of the data user operating the CCTV system and the specific purpose of surveillance etc.
- **Electronic storage and online dissemination of personal data** – Property management bodies should protect the personal data stored in electronic form against unauthorised or accidental access, processing, erasure, loss or use. Access should be confined to a need-to-know basis and through the use of password control.
- **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 is one of the essential factors to enable property management bodies (such as owners' corporations, owners' committees, mutual aid committees and property management companies) to win residents' trust and support in fulfilling their management duty. On the other hand, improper handling of personal data may give rise to disputes between the parties and even discourage residents from participating in building management.

This guidance note aims to assist property management bodies to understand the application of the Personal Data (Privacy) Ordinance (the "**Ordinance**") to specific situations commonly encountered by them.

Personal data to be collected for issuing resident cards

It is common for property managers of private housing estates to install electronic door access card systems at the building entrances, and a flat occupant may use his resident card to enter the building or use club facilities.

For the purpose of issuance of resident cards, a property manager usually requires a flat owner to provide, in 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 Ordinance 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.

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

The application form for resident cards should contain a notice informing an applicant of the matters required under DPP 1(3) as follows:

(i) whether it is obligatory or voluntary for him to supply his personal data and, where obligatory, the consequences for him if he fails 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.

Recording of HKID Card numbers of visitors

For security reasons, a property manager needs to monitor the entry of visitors, who may visit the building only with permission. 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 (the "**PI Code**") issued by the Privacy Commissioner for Personal Data, Hong Kong (the "**Commissioner**"). However, pursuant to paragraph 2.2 of the PI Code, the property manager should, wherever practicable, give the visitor the option to adopt other less privacy-intrusive alternatives 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 (for example 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 his identity. Collection of HKID Card number should be resorted to only after alternative means of verification is duly considered.

A clear PICS and notice of the alternatives to the provision of HKID Card number should be given to visitors.

Visitors' log book

A log book containing visitors' 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 the need arises (such as when an incident of security concern happened).

DPP2(2) imposes a duty on a data user to ensure that there is no excessive retention of personal data. Therefore, the personal data recorded in the log book should be deleted as soon as practicable once the purpose of collection is fulfilled. It is recommended that

entries in the log book should be deleted regularly and should not be retained over one month if no incident of security concern arises.

Previous entries in a visitors' log book should be concealed from future visitors, 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, personal data of the complainant 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.

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[1] of the data subject, be used for a new purpose[2].

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 comply with the complainant's wish. If non-disclosure of the complainant's personal data makes it impracticable for the property manager to deal with the matters complained of, the property manager should explain this difficulty to the complainant.

Inform a complainant 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

Although property management bodies may have to inform owners of building management affairs by the public display of notices[3], 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, which is not necessary for the purpose of posting the notice must be edited out.

While an owners' corporation is obliged to display in a prominent place in the building a notice[4] 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 (rather than their names), 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 of an individual should be displayed in 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 not timely paid the management fee) may therefore contravene the requirements under DPP3(1).

An individual's personal data is not to be published in management notices unnecessarily, and in particular, no HKID Card number or contact information of an individual is to be displayed in public.

Use of CCTV covering 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 controlled to avoid intrusion into the privacy of

---

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

2 "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.

3 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.

4 Section 26A of the BMO

individuals. CCTV cameras should be positioned in a way that will not unnecessarily intrude into the privacy of individuals.

People should be explicitly informed that they are subject to CCTV surveillance. An effective way is to post conspicuous notices at the entrance to the monitored area and affix further notices 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 personal data privacy issues can be raised.

For more specific guidance on determining whether CCTV should be used in given circumstances and how to use CCTV responsibly, please refer to the *Guidance on CCTV Surveillance and Use of Drones*[5] issued by the Commissioner.

If CCTV is used to record employees' activities at a workplace, such means of recording must comply with DPP1(2), i.e. personal data shall be collected by means which are lawful and fair in the circumstances of the case. A detailed discussion on the fair means of collection of data by CCTV can be found in the investigation report[6] published by the Commissioner.

If CCTV is used to monitor the security in the common area, conspicuous notices need to be posted to inform people of the fact that CCTV is in use, the details of the operator of the CCTV and the purpose of using it.

Electronic storage and online dissemination of personal data

Personal data collected by property management bodies may be stored in electronic form (e.g. information collected from resident card applications). To comply with the security requirements under DPP4(1), appropriate privacy enhancement systems and procedures should, as far as practicable, be employed to protect the personal data against unauthorised or accidental access, processing, erasure, loss or use. Access should be confined to a need-to-know basis and through the use of password control. Collective use of a common password must be avoided. Proper training and supervision should be arranged to ensure staff's handling of personal data with prudence, competence and integrity.

Details of collection, display or transmission of personal data through the Internet can also be found in the *Guidance for Data Users on the Collection and Use of Personal Data through the Internet*[7] issued by the Commissioner.

Personal data stored or disseminated via the Internet must be safeguarded against unauthorised or accidental access, processing, erasure, loss or use. Restriction of access to need-to-know basis and password control are recommended.

Outsourcing of services

Property management bodies usually employ caretakers or engage service contractors to assist in their daily work. It should be noted that under section 65(1) and 65(2) of the Ordinance, 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.

A property management company 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 Ordinance.

5 www.pcpd.org.hk//english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf

6 www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R12_4839_e.pdf

7 www.pcpd.org.hk//english/resources_centre/publications/files/guidance_internet_e.pdf

On the other hand, DPP2(3) provides that if a data user engages a data processor[8] 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*[9] issued by the Commissioner.

Promulgate guidelines and work procedures for security staff to handle personal data and monitor the performance of frontline staff to ensure compliance with the Ordinance.

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

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

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

First Published in November 2006
August 2011 (First Revision)
August 2016 (Second Revision)