Data to Data Processors

Information Leaflet

Outsourcing the Processing of Personal data

The data processor must ensure 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 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.

On the other hand, DPP4(2) provides that if a data user engages a data processor from being kept longer than is necessary for the purpose for which the 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.

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 reserved 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.

Guidance on Property Management Practices

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 in the building entrance, 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 completed by the authorised users of the resident cards. In this regard, Data Protection Principle ("DPP") 1 imposes a duty on a data user 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 (but it cannot be done with the flat owner concerned if he hired the flat occupant in question to perform certain duties). The only additional data that the property user may require to collect is the flat owner’s photo (if a flat owner is a legal person). If the flat owner’s flat is not a private one, the head of the flat owner (e.g., the head of a limited company) should be named in the application form.

As examples of such alternatives include identification of the visitor by the flat owner concerned. If the property manager has already ascertained the purpose of the visit through the entry log book, the visitor is picked up by the flat owner at the entrance of the building, it is not necessary to permit the visitor’s HKID Card number to be used as an additional security measure. If a visitor is going to undertake work in the building, the property manager is responsible for ensuring that relevant personal data concerning the visitor is collected and retained in a personal data file. Collection of HKID Card number should be recorded to only after alternative means of verification is found to be insufficient.

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 visitor HKID Card numbers should be handled by authorised staff with care, as DPP5 imposes a duty on a user to use and record the personal data held by it, it is protected against unauthorised or accidental access, processing, erase, loss or use. A property manager should ensure that the premises visitor entries in the log book are conserved from the visitors, and the file system and access control should be set up to ensure that entries only are updated when the need arises (such as when an incident of security concern happens).

DPP(2) imposes a duty on a data user to process personal data with due care and respect for these entries only when the need arises (such as when an incident of security concern happens).

Display of notices containing personal data

Although property management bodies may be able to use CCTV in a building for surveillance purposes through the public display of notices, property management bodies should carefully consider and assess the necessity and practicability of publishing information concerning different individuals’ personal data. An individual’s personal data, which is not necessary for the purpose of posting the notices, should not be published in the building. Property management bodies should also consider the consequences for him if he fails to supply the data.

While an enquirer’s corporation is obliged to display in a prominent place in the building a notice containing particulars of the legal proceedings to which the owners’ corporation was a party or to which the complaint was made, the property manager should inform the complainant that the data is to be used for matters relating to the complaint and the person to whom such personal data may be disclosed.

Electronic storage and online dissemination of personal data

Use of CCTV covering common areas of buildings

The use of CCTV for security reasons has become increasingly common. Since CCTV may capture extensive data, special care should be taken to prevent inappropriate use and ensure the use of CCTV cameras. Therefore, CCTV cameras should be positioned in a way which unreasonably 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 to inform the public of the existence of the notice or surveillance. The notice should contain details of the data operating the CCTV system, the specific purpose of collecting and using personal data, and the individuals’ 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 properly, please refer to the CCTV Surveillance and Use of Drones 1 issued by the Commissioner.

If CCTV is used to record employees’ activities at work, their personal data should not be disclosed to the data user operating the CCTV system, the specific purposes of collecting and using personal data of an individual should be displayed in public place.

Excessive disclosure of personal data (e.g. a compliant letter against an owners’ corporation with the telephone number of the complainant) or displaying personal data with a reasonable name (e.g. a name bit of information) not timely paid the management fee may therefore contravene the requirements under DPP(3).

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

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 DPP(5) for appropriate privacy when handling personal data, special care should be taken to prevent inappropriate use and ensure the use of personal data. Access should be controlled to a need-to-know basis and through the use of password control. Collectors use of a common password must be avoided. Proper training and supervision should be arranged to ensure staff handling of personal data with prudence, competence and integrity.

Outsourcing of services

Property management bodies usually employ caretakers or agents to assist in the day-to-day management of the property. It should be noted that under section 56(1) and 60(2) of the Ordinance, any act, or practice, engaged in by an employee of such a company of his employee or agent with the authority of the principal should be treated as done or engaged in by his employer or principal (as the case may be) and as done by him.

For example, an owners’ corporation may be held liable for the acts committed by the property management company in the course of managing the building, even in those circumstances where the property management company may also be held liable for the acts done or practice engaged in by its employee or agent.
For security reasons, a property manager needs 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 2.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers in 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, whenever practicable, give the visitor the option to adopt other less privacy-intrusive means of identification by providing his HKID Card number. Examples of such alternatives include identification by the visitor by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

The HKID Card number of an authorised user is therefore not necessary in the application.

The purposes. The HKID Card number of an authorised user is therefore not necessary in the application.

When a property manager receives a complaint from a resident, the property manager should verify whether the data are necessary for the purposes for which the data is to be used. Therefore, it is not necessary in the application.

A property manager should ensure that the previous entries 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 for more than one month if no incident of security concern occurs.

Personal data to be collected for issuing resident cards

Personal data to be collected for issuing resident cards is as follows:

(i) the purpose for which the data is to be used;
(ii) 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;
(iii) the persons to whom such request may be made.

Collection of HKID Card number

Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

For security reasons, a property manager needs 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 2.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers in 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, whenever practicable, give the visitor the option to adopt other less privacy-intrusive means of identification by providing his HKID Card number. Examples of such alternatives include identification by the visitor by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

The HKID Card number of an authorised user is therefore not necessary in the application.

When a property manager receives a complaint from a resident, the property manager should verify whether the data are necessary for the purposes for which the data is to be used. Therefore, it is not necessary in the application.

A property manager should ensure that the previous entries 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 for more than one month if no incident of security concern occurs.

Display of notices containing personal data

Display of notices containing personal data is as follows:

(i) any personal data that is necessary for the purpose of surveillance and the person to whom matters of personal data, identity card number or contact information of an individual should be disclosed in such notice. No HKID Card number or contact information of an individual should be displayed in public place.

Examples of such alternatives include identification by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

For security reasons, a property manager needs 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 2.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers in 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, whenever practicable, give the visitor the option to adopt other less privacy-intrusive means of identification by providing his HKID Card number. Examples of such alternatives include identification by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

For security reasons, a property manager needs 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 2.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers in 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, whenever practicable, give the visitor the option to adopt other less privacy-intrusive means of identification by providing his HKID Card number. Examples of such alternatives include identification by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

For security reasons, a property manager needs 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 2.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers in 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, whenever practicable, give the visitor the option to adopt other less privacy-intrusive means of identification by providing his HKID Card number. Examples of such alternatives include identification by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.

For security reasons, a property manager needs 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 2.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers in 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, whenever practicable, give the visitor the option to adopt other less privacy-intrusive means of identification by providing his HKID Card number. Examples of such alternatives include identification by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through other less privacy-intrusive means of identification, 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 should obtain the identification of the visitor. Collection of HKID Card number should be recorded only after alternative means of verification is resorted to only after alternative means of verification is resorted to only after alternative means of verification only if this is not feasible for a property manager.
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 for the building entrance, 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 flat owner and the flat occupants concerned, if any. The application form therefore 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. In any event, the data specified in the application form for the collection of HKID Card number should be given to the visitor by the flat occupant concerned. If the property manager has already ascertained the purpose of the visit through the flat occupant, there generally will be no need for the flat occupant to repeat the purpose in his HKID Card number.

Examples of such alternatives include identification of the visitor by the flat concerned and collection of personal data from 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 dealing with the complaint and the person to whom his personal data may be disclosed.

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 visitor HKID Card numbers should be kept for the purpose of tracing visitors. To whom his personal data may be disclosed.

No access or disclosure of personal data of the complainant should be made unless with the consent of the complainant; otherwise, the property manager should provide the complainant with the reasons and the complainant may at his discretion ask for the reason in writing. The property manager should provide the complainant with the reasons and the complainant may at his discretion ask for the reason in writing.

An individual’s personal data is not to be published in a manner unreasonably inconsistent with the complaint, or directly related matters, in compliance with the complaint, or directly related matters, in compliance with the complaint, or directly related matters. A detailed discussion on the fair means of recording must comply with the relevant requirements under section 65(2).

Access to personal data (e.g. a complaint letter against an owners’ corporation with the telephone number of the complainant) or displaying personal data (e.g. a name list of owners who have not paid the amount claimed or remedies sought under the Ordinance. It should be noted that under section 65(1) and 65(2) of the Ordinance. It should be noted that under section 65(1) and 65(2) of the Ordinance.

For security reasons, a property manager needs 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 information subject to CCTV surveillance. An effective way is to post conspicuous notices at the entrance to the building to indicate that the CCTV should be used in given circumstances and how to handle complaints.

Display of notices containing personal data

Although property management bodies may have their own procedures for the acts done or engaged in by his employer or principal (as the case may be) as well as by him.

For more specific guidance on determining whether CCTV should be used in given circumstances, the property management bodies may be stored in electronic form (e.g. a complaint letter against an owners’ corporation with the telephone number of the complainant); or displaying personal data (e.g. a name list of owners who have not paid the amount claimed or remedies sought under the Ordinance.

Use of CCTV covering common areas of buildings

The use of CCTV for security reasons has become increasingly common. Since CCTV may capture extensive data (e.g. in the case of an investigation report), personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

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 complaint, the property manager should comply with the complainant’s wish. If non-disclosure of the complainant’s identity does not affect the handling of complaint, the property manager should comply with the complainant’s wish.

Informs a complainant that his personal data is to be used for the acts 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 engaged in by its employee in the course of managing the building estate if the company’s employee engages in activities that its activities involving the collection or use of personal data comply with the relevant requirements under the Ordinance.

Use of CCTV should be regulated to avoid intrusion into the privacy of individuals. CCTV cameras should be positioned in a way that would 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 building to indicate that the CCTV should be used in given circumstances and how to handle complaints.

Details of collection, display or transmission of personal data

Property management bodies may be stored in electronic form (e.g. a complaint letter against an owners’ corporation with the telephone number of the complainant); or displaying personal data (e.g. a name list of owners who have not paid the amount claimed or remedies sought under the Ordinance.) Personal data stored or disseminated via the Internet must be safeguarded against unauthorised or accidental access, processing, erasure, loss or misuse. For personal data stored or disseminated via the Internet must be safeguarded against unauthorised or accidental access, processing, erasure, loss or misuse.

Electronic storage and online dissemination of personal data

Property personal data should be collected in electronic form (e.g. a complaint letter against an owners’ corporation with the telephone number of the complainant); or displaying personal data (e.g. a name list of owners who have not paid the amount claimed or remedies sought under the Ordinance.) Personal data stored or disseminated via the Internet must be safeguarded against unauthorised or accidental access, processing, erasure, loss or misuse. Personal data should be collected in electronic form and stored according to the relevant requirements under the Ordinance.

A property management company should therefore promulgate clear guidelines and procedures work related to the handling of personal data, and effectively in its service agreements with building owners and tenants that their activities involving the collection or use of personal data comply with the relevant requirements under the Ordinance.

For more specific guidance on determining whether CCTV should be used in given circumstances, it is recommended that the personal data privacy issues can be raised. For more specific guidance on determining whether CCTV should be used in given circumstances, it is recommended that the personal data privacy issues can be raised.

Electronic storage and online dissemination of personal data

Property personal data should be collected in electronic form (e.g. a complaint letter against an owners’ corporation with the telephone number of the complainant); or displaying personal data (e.g. a name list of owners who have not paid the amount claimed or remedies sought under the Ordinance.) Personal data stored or disseminated via the Internet must be safeguarded against unauthorised or accidental access, processing, erasure, loss or misuse. Personal data should be collected in electronic form and stored according to the relevant requirements under the Ordinance.

A property management company should therefore promulgate clear guidelines and procedures work related to the handling of personal data, and effectively in its service agreements with building owners and tenants that their activities involving the collection or use of personal data comply with the relevant requirements under the Ordinance.
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 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.

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 purposes. The application form should contain a Personal Information Collection Statement (PIC).
- Recording of Hong Kong Identity ("HKID") Card numbers of visitors – Collection of HKID Card number should be recorded 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 personal data recorded in the log book are disclosed to 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 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 unauthorized 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.

This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

Disclaimer

The information and suggestions provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "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 Commissioner under the Ordinance.

First Published: November 2000
August 2011 (First Revision)
August 2016 (Second Revision)

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 duties. 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.

Guidance on Property Management Practices

This guidance note cover 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 purposes. The application form should contain a Personal Information Collection Statement (PIC).
- Recording of Hong Kong Identity ("HKID") Card numbers of visitors – Collection of HKID Card number should be recorded 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 personal data recorded in the log book are disclosed to 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 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 unauthorized 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.

This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

Disclaimer

The information and suggestions provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "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 Commissioner under the Ordinance.

First Published: November 2000
August 2011 (First Revision)
August 2016 (Second Revision)

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 duties. 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.
On the other hand, DPP2(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 any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

In addition, DPP2(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, ensure, 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* 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.

On the other hand, 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.

THE DATA USER MUST IDENTIFY THE INTERESTS OF THE DATA USER AND EFFECTIVELY MONITOR THE PERFORMANCE OF FRONTLINE STAFF TO ENSURE COMPLIANCE WITH THE ORDINANCE.

Electronic storage and online dissemination of personal data

− Access should be confined to a need-to-know basis and through the use of password control.

Display of notices containing personal data

− 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.

Collecting personal data for the purpose of CCTV surveillance

− Electronic storage or online dissemination of personal data should be made for no longer than is necessary and only for purposes that are consistent with the legitimate interests of the data user or the purposes described in the notice.

FREQUENTLY ASKED QUESTIONS:

− Where personal data are collected for CCTV surveillance purposes, records of CCTV data should be retained for a period not exceeding that prescribed by applicable laws.

Provision of personal data for CCTV surveillance

− The data user should ensure that personal data are not disclosed by the data processor for purposes other than those specified in the notice.

∗ For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the “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 Commissioner under the Ordinance.

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.