Webinar on the Protection of Personal Data Privacy for NGOs

The Hong Kong Council of Social Service

18 November 2020

01 Introduction to the PD(P)O

02 Six Data Protection Principles (DPPs)

03 Code of Practice on the Identity Card Number and Other Personal Identifiers

04 Offences and Compensation

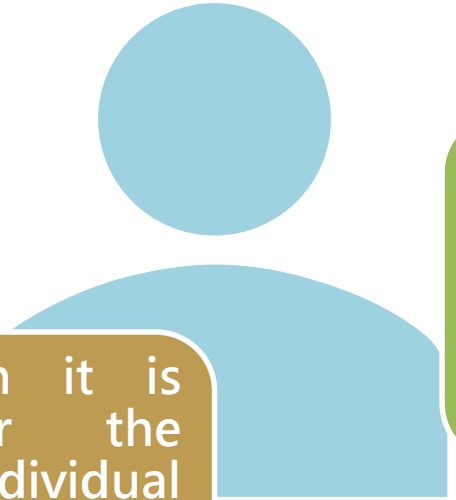
05 Case Sharing

06 QA session

1. Introduction to the PD(P)O

What is "Personal Data"?

(a) relating directly or indirectly to a living individual



(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

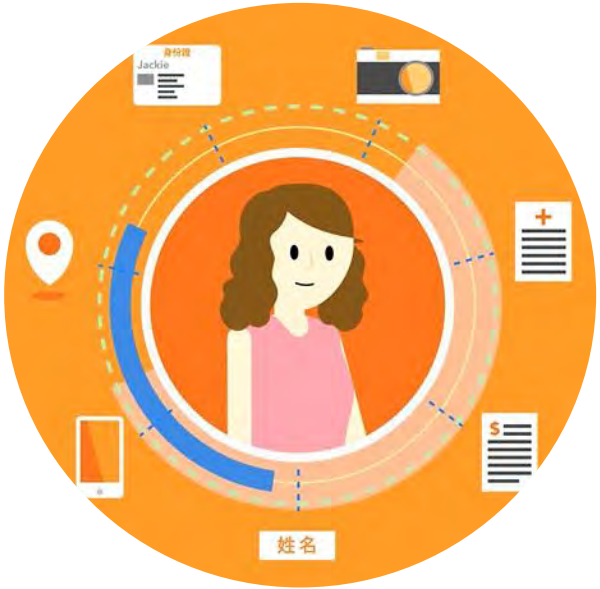
(c) in a form in which "access to" or "processing of" the data is practicable

Examples of personal data

123.456.789.12

Who is “Data Subject”?

- Data Subject is the individual who is the subject of the personal data



Who is "Data User"?

- Data User is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data
- Including government departments, public and private sector and individuals

2. Six Data Protection Principles (DPPs)

- The six data protection principles form the base of the PDPO

- data users must comply with the six data protection principles in the collection, holding, accuracy, retention period, security, privacy policy and access to and correction of personal data.

Link of video:

https://www.youtube.com/watch?v=86wYYT8173Q

Principles of the PDPO

Data Minimisation

Lawful and Fair Collection

Purpose Specification

Retention

Use Limitation

Data Security

Transparency

Rights of Data Subjects

Definition of “Collection” of Personal Data

Eastweek Publisher Limited & Another v

Privacy Commissioner for Personal Data (CACV 331/1999)

The *Eastweek* case

A complaint lodged with the PCPD in 1997

The complainant was photographed by a magazine without her knowledge or consent

The photograph published in the magazine accompanied by unflattering and critical comments on her dressing style

The *Eastweek* case

Conditions for "collection" of personal data

- the collecting party must be thereby compiling information about an individual
- the individual must be one whom the collector of information has identified or intends or seeks to identify
- the identity of the individual must be an important item of information to the collecting party

Principle 1 – Purpose and manner of collection

- shall be collected for purposes related to the functions or activities of the data user
- the means of collection must be lawful and fair
- the data collected should be adequate but not excessive

Collection of date of birth

Collect the age groups of services users
(e.g. aged 51-60)

Collect the month of birth or the day and month of birth rather than full D.O.B

Notification

"Personal Information Collection Statement"

1. the purposes of data collection ;
2. the classes of persons to whom the data may be transferred;
3. whether it is obligatory or voluntary for the data subject to supply the data;
4. where it is obligatory for the data subject to supply the data, the consequences for him if he fails to supply the data; and
5. the name or job title and address to which access and correction requests of personal data may be made.

Example of PICS

The Alpha Corporation
Personal Information Collection Statement pertaining to Recruitment

The personal data collected in this application form will be used by the Alpha Corporation to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Personal Data Access Form" and forward it to our Data Protection Officer in the Human Resources.

Purpose Statement

Obligatory or optional to provide data

Classes of transferees

Access & correction right

Principle 2 – Accuracy and duration of retention

Data users shall take practicable steps to ensure:

- the accuracy of personal data held by them.
- personal data is not kept longer than is necessary for the fulfillment of the purpose

Data Retention

- Erase personal data held by the data user where the data is no longer required for the purpose
- If a data user engages a data processor to process personal data on the data user's 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

Principle 3 – Use of personal data

- personal data shall not, without the prescribed consent of the data subject, be used for a new purpose

- allow a "relevant person" to give prescribed consent for the data subject under specified conditions

New purpose: any purpose other than the purposes for which they were collected or directly related purposes

Principle 4 – Security of personal data

- all practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing, erasure, loss and use

- security in the storage, processing and transmission of data

- if a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

Common types of data breach

1. Loss of documents and USB
2. Improper setting of IT system or Hacking
3. Wrong (e)mailing address
4. Staff's integrity and prudence
5. Improper disposal of documents

Data Breach Notification

- it is **not a statutory requirement** on data users to inform the PCPD about a data breach incident concerning the personal data held by them, but data users are advised to do so as a recommended practice for proper handling of such incident.

To: Privacy Commissioner for Personal Data, Hong Kong

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

Data Breach Notification Form

Notice

Notification of a data breach to the Privacy Commissioner for Personal Data, Hong Kong (the **"Commissioner"**) by the data user ***(see Note 1)*** is not a legal requirement. In deciding whether or not to give this notification to the Commissioner, you should consider the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Commissioner. In most cases, it is advisable to give notifications to the data subject(s) ***(see Note 2)*** affected by the breach.

PARTICULARS OF THE PERSON GIVING THIS NOTIFICATION (i.e. the data user)

Name: _____

Address: _____

_____

Telephone number: _____ Fax number: _____

Email address: _____

Where the person giving this notification is an organization, please provide the following information:

Contact person :

Name (*Mr./Ms./Miss): _____

Relationship with the Reporting Organization (e.g. job title): _____

Telephone number: _____ Fax number: _____

Email address: _____

(*Please delete as appropriate)

DETAILS ABOUT THE DATA BREACH *(see Note 3)*:

ACTIONS TAKEN / WILL BE TAKEN TO CONTAIN THE BREACH *(see Note 4)*

Please set out details of any actions / measures taken or will be taken to mitigate and minimize the breach

RISK OF HARM *(see Note 5)*

Is there a real risk of harm to any individual? (Please tick one of the following boxes) ☐ Yes ☐ No

Please explain below why there is / there is no real risk of such harm

ASSISTANCE AND ADVICE OFFERED TO INDIVIDUALS

Describe (i) what has been done to inform the individual(s) affected by the breach; and (ii) if their safety, well-being or property is at risk as a result of the breach, what has been done or can be done to assist them in avoiding / mitigating that risk or its consequences

NOTIFICATION TO OTHER BODIES / REGULATORS / LAW ENFORCEMENT AGENCIES

Please provide details if such notification has been given

Signature: _____

Name: _____

Title: _____

Date: _____

https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

Data Breach Handling

Collecting Information Immediately

Immediate gathering of essential information for assessing the impact on data subjects including:

- When and where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of personal data was involved?
- How many data subjects were affected?

Data Breach Handling

Data Breach Handling

Data Breach Handling

Considering the Giving of Notification

When real risk of harm is reasonably foreseeable in a data breach, the data user should consider:

- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

Action by the PCPD

- Screen the information provided by the data user

- Consider conducting compliance check or compliance investigation (whether a great impact on the society and the number of people affected

Principle 5 – Information to be generally available

Transparency

Data users have to provide

(a) policies and practices in relation to personal data;

(b) the kind of personal data held;

(c) the main purposes for which personal data are used.

Principle 6 – Access to personal data

Rights of data subjects

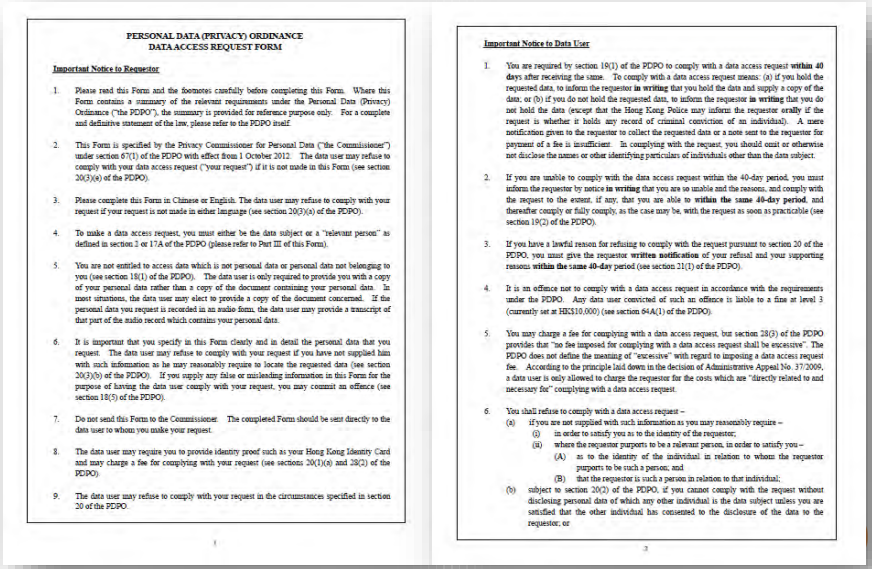
A data subject shall be entitled to：

i. request access to his/her personal data ；Data user may charge a fee for complying with the data access request

ii. request correction of his/her personal data

If the data user holds the relevant personal data, it should supply a copy of the requested data within 40 calendar days after receiving the DAR.

Data Access Request Form



PERSONAL DATA (PRIVACY) ORDINANCE
DATA ACCESS REQUEST FORM

Important Notice to Requestor

1. Please read this Form and the footnotes carefully before completing this Form. Where this Form contains a summary of the relevant requirements under the Personal Data (Privacy) Ordinance ("the PDPO"), the summary is provided for reference purpose only. For a complete and definitive statement of the law, please refer to the PDPO itself.
2. This Form is specified by the Privacy Commissioner for Personal Data ("the Commissioner") under section 67(1) of the PDPO with effect from 1 October 2012. The data user may refuse to comply with your data access request ("your request") if it is not made in this Form (see section 20(3)(e) of the PDPO).
3. Please complete this Form in Chinese or English. The data user may refuse to comply with your request if your request is not made in either language (see section 20(3)(a) of the PDPO).
4. To make a data access request, you must either be the data subject or a "relevant person" as defined in section 2 or 17A of the PDPO (please refer to Part III of this Form).
5. You are not entitled to access data which is not personal data or personal data not belonging to you (see section 18(1) of the PDPO). The data user is only required to provide you with a copy of your personal data rather than a copy of the document containing your personal data. In most situations, the data user may elect to provide a copy of the document concerned. If the personal data you request is recorded in an audio form, the data user may provide a transcript of that part of the audio record which contains your personal data.
6. It is important that you specify in this Form clearly and in detail the personal data that you request. The data user may refuse to comply with your request if you have not supplied him with such information as he may reasonably require to locate the requested data (see section 20(3)(b) of the PDPO). If you supply any false or misleading information in this Form for the purpose of having the data user comply with your request, you may commit an offence (see section 18(5) of the PDPO).
7. Do not send this Form to the Commissioner. The completed Form should be sent directly to the data user to whom you make your request.
8. The data user may require you to provide identity proof such as your Hong Kong Identity Card and may charge a fee for complying with your request (see sections 20(1)(b) and 28(2) of the PDPO).
9. The data user may refuse to comply with your request in the circumstances specified in section 20 of the PDPO.

Important Notice to Data User

1. You are required by section 19(1) of the PDPO to comply with a data access request **within 40 days** after receiving the same. To comply with a data access request means: (a) if you hold the requested data, to inform the requestor **in writing** that you hold the data and supply a copy of the data; or (b) if you do not hold the requested data, to inform the requestor **in writing** that you do not hold the data (except that the Hong Kong Police may inform the requestor orally if the request is whether it holds any record of criminal conviction of an individual). A mere notification given to the requestor to collect the requested data or a note sent to the requestor for payment of a fee is insufficient. In complying with the request, you should omit or otherwise not disclose the names or other identifying particulars of individuals other than the data subject.
2. If you are unable to comply with the data access request within the 40-day period, you must inform the requestor by notice **in writing** that you are so unable and the reasons, and comply with the request to the extent, if any, that you are able to **within the same 40-day period**, and thereafter comply or fully comply, as the case may be, with the request as soon as practicable (see section 19(2) of the PDPO).
3. If you have a lawful reason for refusing to comply with the request pursuant to section 20 of the PDPO, you must give the requestor **written notification** of your refusal and your supporting reasons **within the same 40-day** period (see section 21(1) of the PDPO).
4. It is an offence not to comply with a data access request in accordance with the requirements under the PDPO. Any data user convicted of such an offence is liable to a fine at level 3 (currently set at HK$10,000) (see section 64A(1) of the PDPO).
5. You may charge a fee for complying with a data access request, but section 28(3) of the PDPO provides that "no fee imposed for complying with a data access request shall be excessive". The PDPO does not define the meaning of "excessive" with regard to imposing a data access request fee. According to the principle laid down in the decision of Administrative Appeal No. 37/2009, a data user is only allowed to charge the requestor for the costs which are "directly related to and necessary for" complying with a data access request.
6. You shall refuse to comply with a data access request –
   (a) if you are not supplied with such information as you may reasonably require –
      (i) in order to satisfy you as to the identity of the requestor;
      (ii) where the requestor purports to be a relevant person, in order to satisfy you –
         (A) as to the identity of the individual in relation to whom the requestor purports to be such a person; and
         (B) that the requestor is such a person in relation to that individual;
   (b) subject to section 20(2) of the PDPO, if you cannot comply with the request without disclosing personal data of which any other individual is the data subject unless you are satisfied that the other individual has consented to the disclosure of the data to the requestor; or

Who can make a data access request ?

- Data Subject
- Relevant person

a) where the individual is a minor, a person who has parental responsibility for the minor;

b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs;

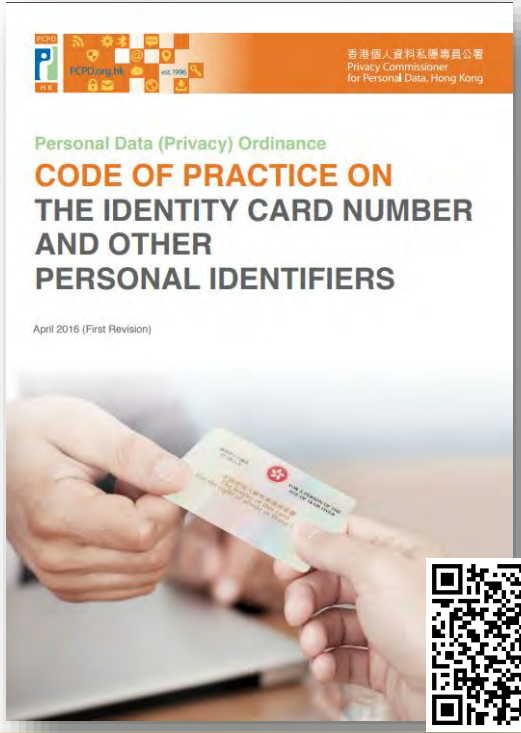
c) where a person appointed to be the guardian of that individual

d) if the guardianship of that individual is vested in, or the functions of the appointed guardian are to be performed by the Director of Social Welfare

3. Code of Practice on the Identity Card Number and Other Personal Identifiers

Code of Practice on the Identity Card Number and Other Personal Identifiers (PI Code)

- Unless authorised by law, no data user may compulsorily require an individual to furnish his HKID Card number and HKID copy *(paragraph 2.1 of the PI Code)*



HKID Card Number: Basic Position

- No right to compel an individual to provide a HKID Card number unless authorised by law

Point 1: Consider alternatives to collecting HKID Card numbers

- to use another personal identifier of the individual's choice, e.g. staff card number of a public utility company;
- to accept identification of the individual by someone known to the data user, e.g. where a resident at a block of flats known to the security guard identifies a visitor;
- to accept some form of security e.g. a monetary deposit

Point 2: Check whether collection of HKID Card numbers comes under one or other of the circumstances where this is permitted in the Code

- to enable the data user to identify the individual concerned or to attribute data to him where any of the following is necessary

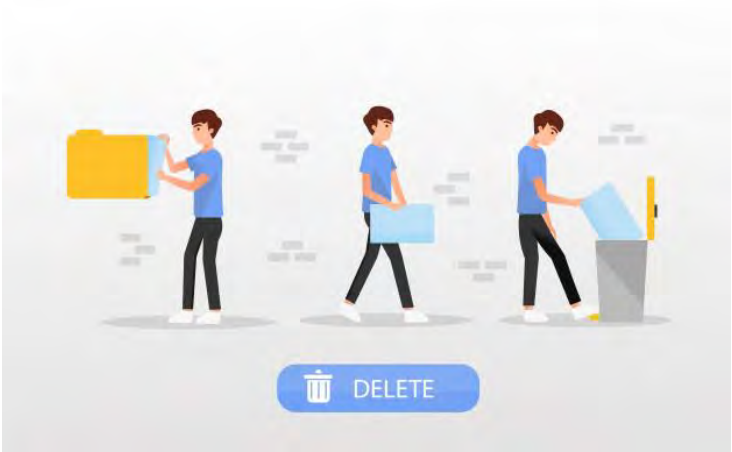
Point 2: Check whether collection of HKID Card numbers comes under one or other of the circumstances where this is permitted in the Code

- for inclusion in a document that establishes or is evidence of any legal or equitable right or interest or legal liability that is not trivial, e.g. in documents that establish an individual's right of ownership of a flat.

Point 3: Check that you do not keep records of HKID Card numbers for longer than is necessary to fulfil the purpose for which they were collected

- for future identification of an individual who has been permitted to enter premises or use equipment, the record should be erased within a reasonable period after the individual has left the premises or ceased to use the equipment

- for giving the individual custody or control of property, the record should be erased within a reasonable period after that custody or control has ceased.



Copies of HKID Cards: Basic Position

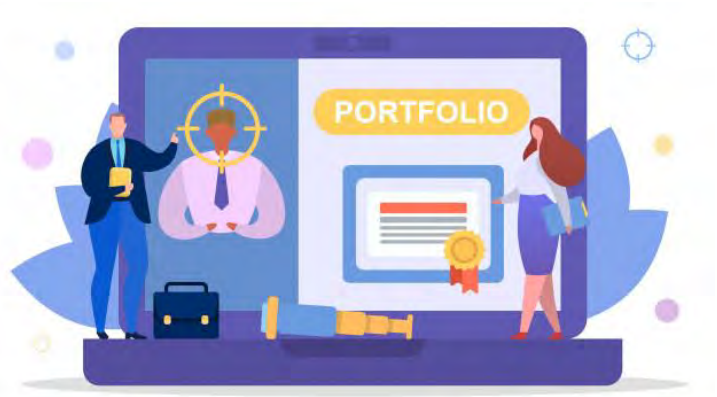
- No right to compel an individual to provide a copy of a HKID Card unless authorised by law

Point 1: Check whether collection of copies of HKID Cards comes under one or other of the circumstances where this is permitted in the code

- safeguarding of security, defence or international relations in respect of Hong Kong
- prevention or detection of crime, and the assessment or collection of any tax or duty
- action permitted under the Code

Point 2: Make sure that collection of copies of HKID Cards does NOT come under one or other of the circumstances where this is specifically NOT permitted in the code

- merely in anticipation of a prospective relationship with the individual, e.g. it would not be permissible for an employer to collect a copy of the HKID Card of an individual only because the employer may wish to offer him employment at some stage.



Point 3: Check that you are implementing adequate security safeguards for copies of HKID Cards that you hold or transmit

- mark it "copy" in the presence of the individual.

Contravention of PI Code

- **Non-compliance with the Code is not itself unlawful.**
- **However, it will give rise to a presumption against the party concerned in any proceedings involving an alleged breach of the PDPO.**

4. Offences and Compensation

Examples of Criminal Offences under PDPO

Contravention of DPP	• not an offence • enforcement notice directing the data user to remedy the contravention
Non-compliance with an enforcement notice	commits an offence penalty of a fine at $50,000 and imprisonment for 2 years
Repeated non-compliance with enforcement notice	• penalty of a fine at $100,000 and imprisonment for 2 years • in case of a continuing offence, a daily fine of $2,000
Same infringement of the second time	• penalty of a fine at $50,000 and imprisonment for 2 years

Criminal offences under PDPO

Section 64 – Disclosing Personal Data Obtained Without Consent from Data User

(1) A person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent—

(a) to obtain gain in money or other property, whether for the benefit of the person or another person; or

(b) to cause loss in money or other property to the data subject.

(2) A person commits an offence if —

(a) the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent; and

(b) the disclosure causes psychological harm to the data subject.

Maximum penalty: a fine of $1,000,000 and imprisonment for 5 years

Examples of Breach of Section 64

Disclosure of an individual's personal data on the Internet for the unlawful purposes of bullying, incitement and intimidation without consent

Sale by an employee of a company of customers' personal data without the company's consent, and for which he received payment from the purchaser.

An ex-employee of a bank called the customers of the bank to promote loan products on behalf of a financial institute (his new employer).

Uploading of a celebrity's intimate photos to the Internet by staff of a laptop repair company, which he retrieved from the laptop without that celebrity's consent, and causing psychological harm to the celebrity.

Court decisions

Contravention of Section 64 of the PDPO

- A telecommunications technician who obtained the personal data of a family member of a police officer for doxxing by using his office computer was charged with, among others, an offence under section 64(2) of the PDPO.
- The defendant, who was convicted after trial in October 2020, **was sentenced to imprisonment for 18 months. Together with other convictions, he was sentenced to imprisonment for 24 months** in November 2020.

The PCPD combats doxxing acts

As of 30 October 2020, the PCPD:-

- has handled over 4,000 doxxing cases
- has written more than 200 times to request the operators of a total of 18 online platforms concerned to remove more than 3,500 web links
- has referred over 1,400 cases to the Police for follow-up
- has referred 45 cases of possible violations of the interim injunction orders relating to doxxing to the Department of Justice for follow-up

Compensation

Section 66B : Privacy Commissioner can grant assistance to data subject in respect of these legal proceedings

5. Case Sharing

Case sharing (1) – Collection of Personal Data

Excessive collection of personal data by social worker

(AAB No. 9 of 2018)

- The complainant's daughter suffered injuries in an SEN school. He sought assistance from an Integrated Family Services Centre.
- The social worker inquired the complainant whether their residence was a privately owned property and whether there was any outstanding mortgage. The information collected was recorded.

Case sharing (1) – Collection of Personal Data

Excessive collection of personal data by social worker

(AAB No. 9 of 2018)

- The social worker wanted to have a better understanding of the complainant's financial hardship, if any, so as to render appropriate assistance to him
- Whether the social worker stated provision of the info was mandatory/voluntary?

Case sharing (1) – Collection of Personal Data

- **Excessive collection of personal data by social worker**
  (AAB No. 9 of 2018)

Remedial actions taken

- Information deleted from computer system
- Issued (and regularly circulated) a new memo reminding its employees that provision of information by the aided person was purely voluntary.
- Info to be included in the Personal Information Collection Statement (PICS) presented to the aided person upon collection of his personal data.
- The PICS would be posted at a conspicuous position. It would also be presented and explained by the interviewing staff to the aided person.

Case sharing (1) – Collection of Personal Data

- **Excessive collection of personal data by social worker**
  (AAB No. 9 of 2018)

Lesson learnt

- Importance of communication of PICS with service users and among staff

Case sharing (1) – Collection of Personal Data

Personal Information Collection Statement

- To ensure readability to customers of normal eyesight (font size, spacing and use of appropriate highlights)
- To present the PICS in a conspicuous manner (in a stand-alone notice or section of the form)
- To use reader-friendly language
- To assist customers' understanding (e.g. provide enquiry service to customers)

Case sharing (2) – Collection of Personal Data

Excessive collection of copies of ID documents for Old Age Allowance

- The complainant applied for Old Age Allowance
- The staff collected photocopies of the complainant's passport and home return permit

Case sharing (2) – Collection of Personal Data

Excessive collection of copies of ID documents for Old Age Allowance

Criteria for collection of copies

- Passport – eligible if applicants stay in HK for over 56 days 1 year prior to the date of application
- Home return permit – if there is no full DOB on the applicants on HKID card

Case sharing (2) – Collection of Personal Data

Excessive collection of copies of ID documents for Old Age Allowance

Remedial actions taken

- Issued an apology letter
- Destroyed the concerned photocopies
- Strengthened internal control to avoid recurrence of similar incidents

Case sharing (2) – Collection of Personal Data

Excessive collection of copies of ID documents for Old Age Allowance

Lesson learnt

- Data users should ensure procedures in place for collection of data and provide adequate training to staff

Case sharing (3) – Collection of Personal Data

Collection of HKID card number of a visitor by an elderly home

- Visitor was the resident's grandson
- Required information:
  - Relationship between the visitor and the resident
  - HKID number of the visitor

Case sharing (3) – Collection of Personal Data

Collection of HKID card number of a visitor by an elderly home

Lesson learnt

To explore less privacy intrusive alternatives

- recognition by the resident
- recognition by the next of kin of the resident

Case sharing (4) – Collection of Personal Data

[redacted]安老院 被指攝院友沖涼

【本報訊】[redacted]安老院被指拍攝院友沖涼情況，家人得悉事件後大為不滿，向個人資料私隱專員公署投訴，公署正跟進，並指有關做法本質上可能已屬侵犯被拍攝者私隱。不過，安老院接受本報查詢時否認拍攝院友沖涼情況，持與院方談話紀錄的家人怒斥該院講大話，一錯再錯。

Source: https://orientaldaily.on.cc/cnt/news/20180315/00176_050.html

Case sharing (4) – Collection of Personal Data

Taking videos and photos of an elderly person during provision of service

- Private setting in shower room
- No consent from the data subject
- Other alternatives
- Unfair collection

Case sharing (5) – Use of Personal Data

Use of personal data in complaint handling

- The complainant complained against a social worker over her handling of an issue in a youth centre
- The youth centre provided the complainant's identity and contact information to the social worker being complained
- The social worker contacted the complainant

Case sharing (5) – Use of Personal Data

Use of personal data for complaint handling

Lesson learnt

- Complaint handling policy should be communicated to staff and complainants/data subjects; and
- Transfer of personal data in complaints should be based on “need to know” principle.

Case sharing (6) – Security of Personal Data

Leakage of service user's personal data on social media

- A social worker was preparing a client's report
- He uploaded a photo of a report being drafted on a social media platform
- Client's personal data was inadvertently disclosed in the post

Case sharing (6) – Security of Personal Data

Leakage of service user's personal data on social media

Lesson learnt

- Data users to devise guidelines and communicate it to staff
- Enhance staff awareness

Case sharing (7) – Security of Personal Data

Personal data of the residents of an elderly home found on street

- Name, HKID card no., diets and medical consultation records
- Retention period and disposal procedure
- Data processor
- All practicable steps taken?

Case sharing (8) – Data Access Request

DAR in relation to Traffic Accident Victims Assistance

- A domestic helper submitted a DAR to a govt department for “all records” of her application
- The department provided her with copies of documents in physical files

Case sharing (8) – Data Access Request

DAR in relation to Traffic Accident Victims Assistance

- There were outstanding documents withheld by the department
- Categorised data e.g. Officer's report, the assessment of payments, notification etc.
- Computerised data being left out (details of computerised process?)

Case sharing (8) – Data Access Request

DAR in relation to Traffic Accident Victims Assistance

Lesson learnt

- Failure to handle DARs without reasonable excuse may constitute an offence
- Data users should have guidelines in place and provide adequate training to staff

Download Our Publications

Download Our Publications

JOIN

Data Protection Officers' Club

(Membership Application)

保障資料主任聯會 DATA PROTECTION OFFICERS' CLUB

By becoming a DPOC member, you will:

- **advance your knowledge and practice of data privacy compliance through experience sharing and training;**
- **enjoy 20% discount on the registration fee for PCPD's Professional Workshops;**
- **receive updates on the latest development in data privacy via regular e-newsletter**

As a DPOC member, your organisation's name will be published on DPOC membership list at PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK$350 per year

Enquiries: dpoc@pcpd.org.hk

https://www.pcpd.org.hk/misc/dpoc/files/AppForm_1920_NewMembers.pdf

Contact Us

- **Hotline** 2827 2827
- **Fax** 2877 7026
- **Website** www.pcpd.org.hk
- **E-mail** communications@pcpd.org.hk
- **Address** 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, HK