HKiB The Hong Kong Institute of Bankers 香港銀行學會

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

Professional Workshop on Data Protection

Data Protection and Data Access Request

16 August 2024

Disclaimer

The information provided in this PowerPoint for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (Cap 486) (“PDPO”). For a complete and definitive statement of law, direct reference should be made to the PDPO itself. The Office of the Privacy Commissioner for Personal Data makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this PowerPoint. The contents provided will not affect the exercise of the functions and powers conferred to the Commissioner under the PDPO.

PCPD
H K

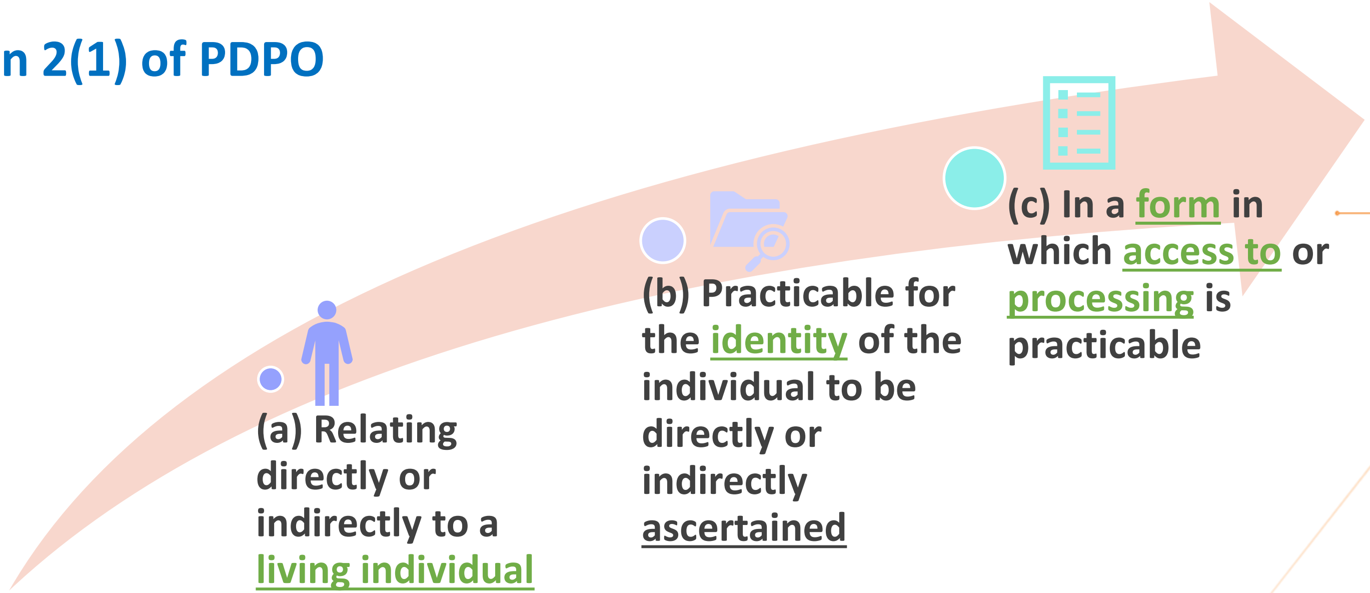
1. Overview of the Personal Data (Privacy) Ordinance (PDPO)
2. Data Access Request
3. Compliance with / Refusal of Data Access Request
4. Case Studies & Practical Tips
5. Q&A

1 Overview of the Personal Data (Privacy) Ordinance (PDPO)

What is “Personal Data”?

“**Data**” (資料) means *any representation of information (including an expression of opinion) in any document*.

Section 2(1) of PDPO



(a) Relating directly or indirectly to a living individual

(b) Practicable for the identity of the individual to be directly or indirectly ascertained

(c) In a form in which access to or processing is practicable

Definitions

資料當事人
Data Subject

- a living individual who is the subject of the personal data concerned

資料使用者
Data User

- a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data
- Liability of employers and principals

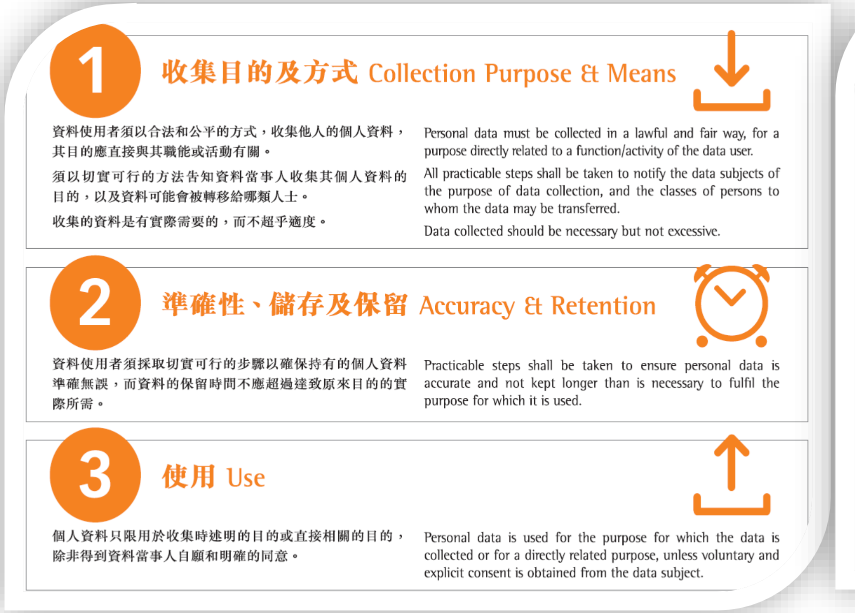
資料處理者
Data Processor

- a person who

a) processes personal data on behalf of another person; and

b)does not process the data for any of the person’s own purposes

The Six Data Protection Principles (DPPs)



1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性、儲存及保留 Accuracy & Retention

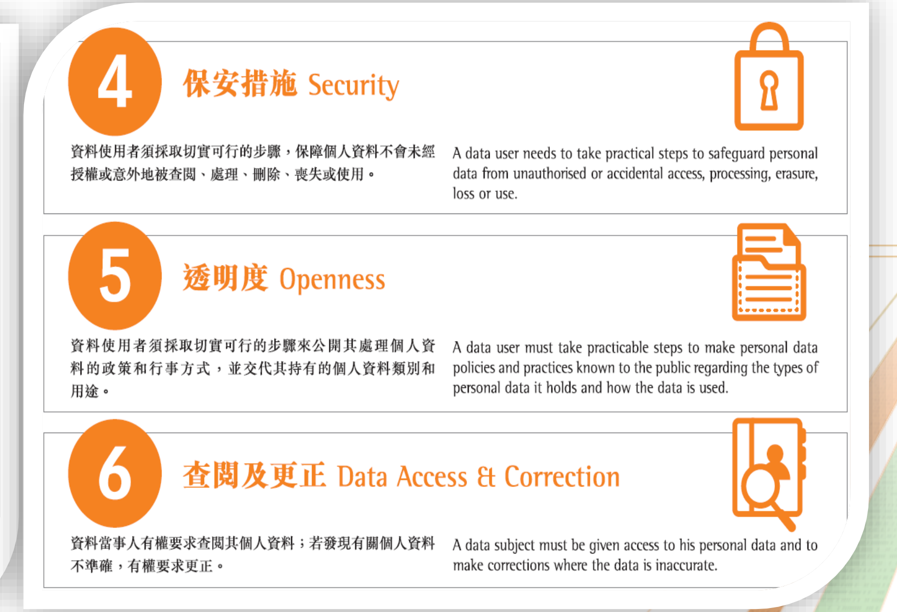
資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.



4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

Who is responsible?

Employees vs employers?

- Data user responsible for acts and practices of employees

  (section 65(1))

- Data user responsible for acts and practices of agents

  (section 65(2))

Defence:

- Data user has taken practicable steps to prevent his employees / agents from doing the alleged acts (section 65(3))

Where is the personal data held?

- Who is the owner (i.e. which department)?
- Held by data processors?
- Stored within the premises of the organization?
- Location of the storage / computer server?

Just right

- Streamline your processes for dealing with Data Access Requests
- Retention and deletion policies
- Information management systems

Complaint Handling by PCPD

Screening

- s37 Acceptance
- Prima facie case?
- Enquiry or Referral to Police*?

Mediation & Investigation

- Facts established
- Expectation of both sides
- Relay concern
- Education

Outcome

- Remedial actions
- Warning
- Enforcement Notice

*** Direct Marketing / Disclosing Personal Data obtained without consent from the data user / Doxxing**

Against PCPD's decision

Appeal to the Administrative Appeals Board (AAB)

Complainant

- Not to carry out an investigation
- Not to serve an Enforcement Notice

Data User (party complained against)

- Enforcement Notice served

2 Data Access Request

Data Access Request

- A data subject may make a **Data Access Request (DAR)**

  For example: personal data in (i) medical records,

  (ii) appraisal reports, (iii) application forms

- A data subject may also make a **Data Correction Request (DCR)** to correct his / her personal data

Right of access to personal data

- Data Protection Principle (DPP) 6 in Schedule 1 to PDPO

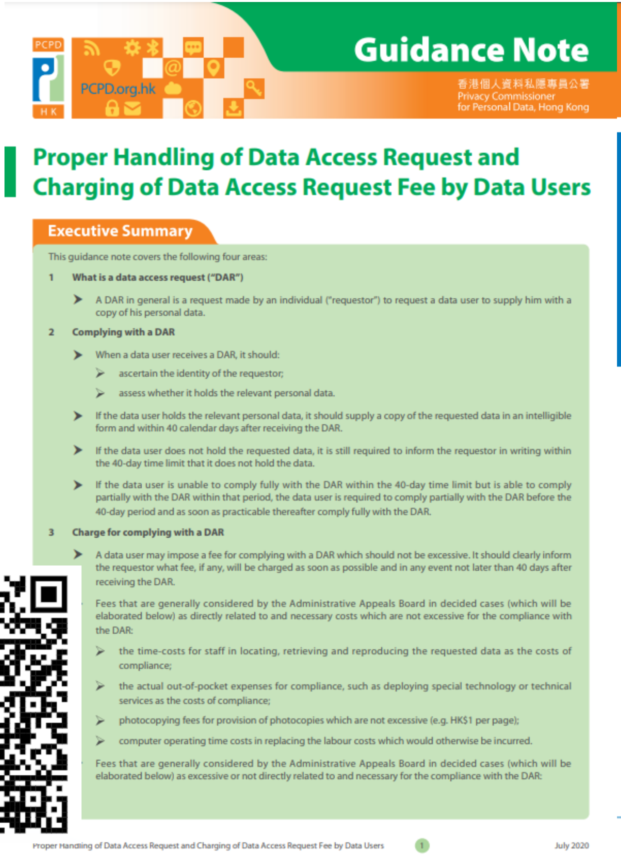
  Data subject shall be entitled to request access to personal data and correction of personal data
  [Remark: DPP 1(3) – Notification of DAR / DCR right during collection]

- Part 5 of PDPO – sections 17A, 18, 19, 20, 21, 27, 28 and 29

DPP 6

- **Highlight of the statutory requirement :**
  - ✓ Requestor must be data subject or relevant person
  - ✓ To be informed whether data user holds personal data (section 18(1)(a))
  - ✓ To be supplied with a copy of the data (section 18(1)(b))
  - ✓ Comply with the request within 40 days (section 19(1))
  - ✓ Refusal shall be made in writing with reasons within 40 days (section 21(1))

- **PCPD's Guidance on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users**



PCPD.org.hk

Guidance Note

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

Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users

Executive Summary

This guidance note covers the following four areas:

1 **What is a data access request ("DAR")**

- A DAR in general is a request made by an individual ("requestor") to request a data user to supply him with a copy of his personal data.

2 **Complying with a DAR**

- When a data user receives a DAR, it should:
  - ascertain the identity of the requestor;
  - assess whether it holds the relevant personal data.
- If the data user holds the relevant personal data, it should supply a copy of the requested data in an intelligible form and within 40 calendar days after receiving the DAR.
- If the data user does not hold the requested data, it is still required to inform the requestor in writing within the 40-day time limit that it does not hold the data.
- If the data user is unable to comply fully with the DAR within the 40-day time limit but is able to comply partially with the DAR within that period, the data user is required to comply partially with the DAR before the 40-day period and as soon as practicable thereafter comply fully with the DAR.

3 **Charge for complying with a DAR**

- A data user may impose a fee for complying with a DAR which should not be excessive. It should clearly inform the requestor what fee, if any, will be charged as soon as possible and in any event not later than 40 days after receiving the DAR.
- Fees that are generally considered by the Administrative Appeals Board in decided cases (which will be elaborated below) as directly related to and necessary costs which are not excessive for the compliance with the DAR:
  - the time-costs for staff in locating, retrieving and reproducing the requested data as the costs of compliance;
  - the actual out-of-pocket expenses for compliance, such as deploying special technology or technical services as the costs of compliance;
  - photocopying fees for provision of photocopies which are not excessive (e.g. HK$1 per page);
  - computer operating time costs in replacing the labour costs which would otherwise be incurred.
- Fees that are generally considered by the Administrative Appeals Board in decided cases (which will be elaborated below) as excessive or not directly related to and necessary for the compliance with the DAR:

Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users 1 July 2020

Leaflet

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

保障、尊重個人資料
Protect,Respect Personal Data
PCPD.org.hk

Exercising Your Data Access Rights under the Personal Data (Privacy) Ordinance

(Frequently Asked Questions and Answers)

Under the Personal Data (Privacy) Ordinance (the "**Ordinance**"), an individual has the right to request a data user, e.g. a government department or a company, to confirm whether it holds his personal data, and to supply a copy of the data. Such a request is called a data access request.

Common examples of data access requests include requests by employees for copies of their performance appraisal reports, requests by patients for copies of their medical records and requests by consumers for copies of their service application forms.

The following are some frequently asked questions and answers to assist individuals in making data access requests:

Exercising Your Data Access Rights under the Personal Data (Privacy) Ordinance (Frequently Asked Questions and Answers) / June 2016

Data Access Request

Data User should:

- Comply with the DAR within 40 days (s19)
- Notify in writing the reason of refusal within 40 days (s21)
- Fee imposed shall not be excessive (s28)
- Log keeping of reasons for refusing DARs for 4 years (s27)

If not, max. fine of $10,000 (s64A)

Offence against the Requestor (s18)

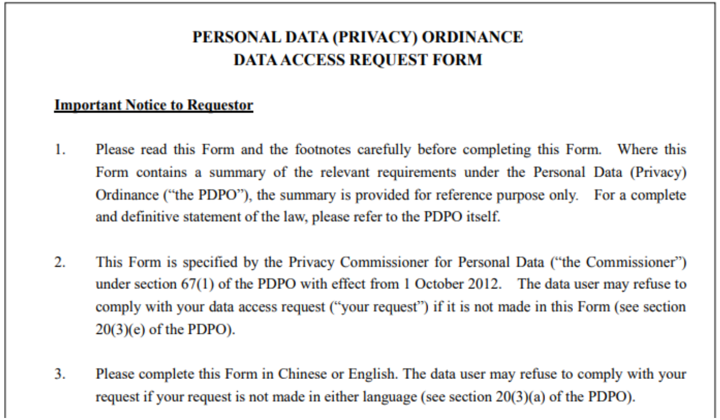
- supply false / misleading information in a material particular in DAR
- max. fine of $10,000 & max. imprisonment for 6 months

Data Access Request

Failure to comply with DAR

- Warning
- Enforcement Notice (s50)
- Non-compliance with EN (s50A - offence)
  - ➢Fine $50,000 & 2 years imprisonment
    [Subseq. convictions ➢ max. fine $100,000]
- Publication of investigation report by the Commissioner (s48)

The DAR form (s67) available at pcpd.org.hk



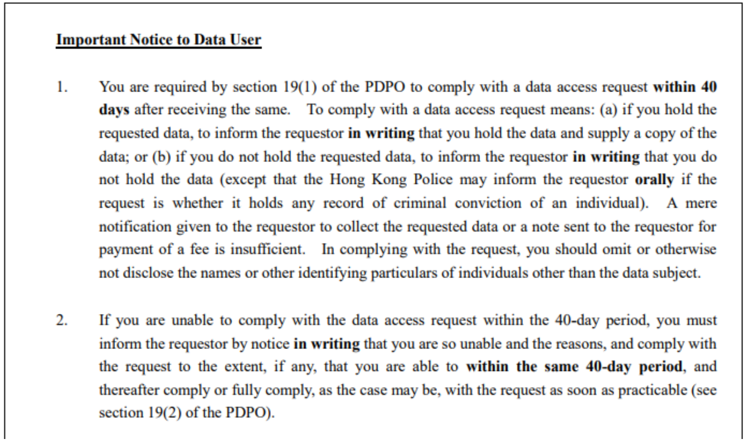
PERSONAL DATA (PRIVACY) ORDINANCE
DATA ACCESS REQUEST FORM

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).

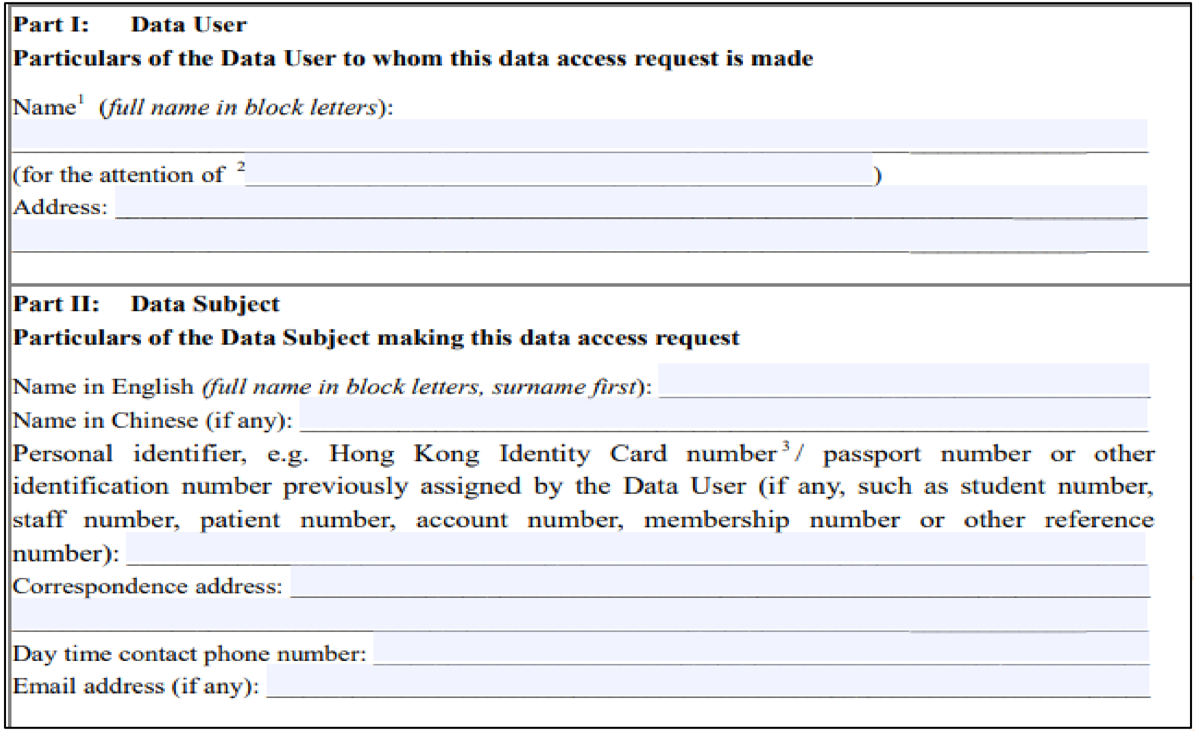


Important Notice to Data User

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).

The DAR form (s67) available at pcpd.org.hk



Part I: Data User

Particulars of the Data User to whom this data access request is made

Name[1] (*full name in block letters*): ______________________________

(for the attention of [2] ______________________________)

Address: ______________________________

____

Part II: Data Subject

Particulars of the Data Subject making this data access request

Name in English (*full name in block letters, surname first*): ______________________________

Name in Chinese (if any): ______________________________

Personal identifier, e.g. Hong Kong Identity Card number[3] / passport number or other identification number previously assigned by the Data User (if any, such as student number, staff number, patient number, account number, membership number or other reference number): ______________________________

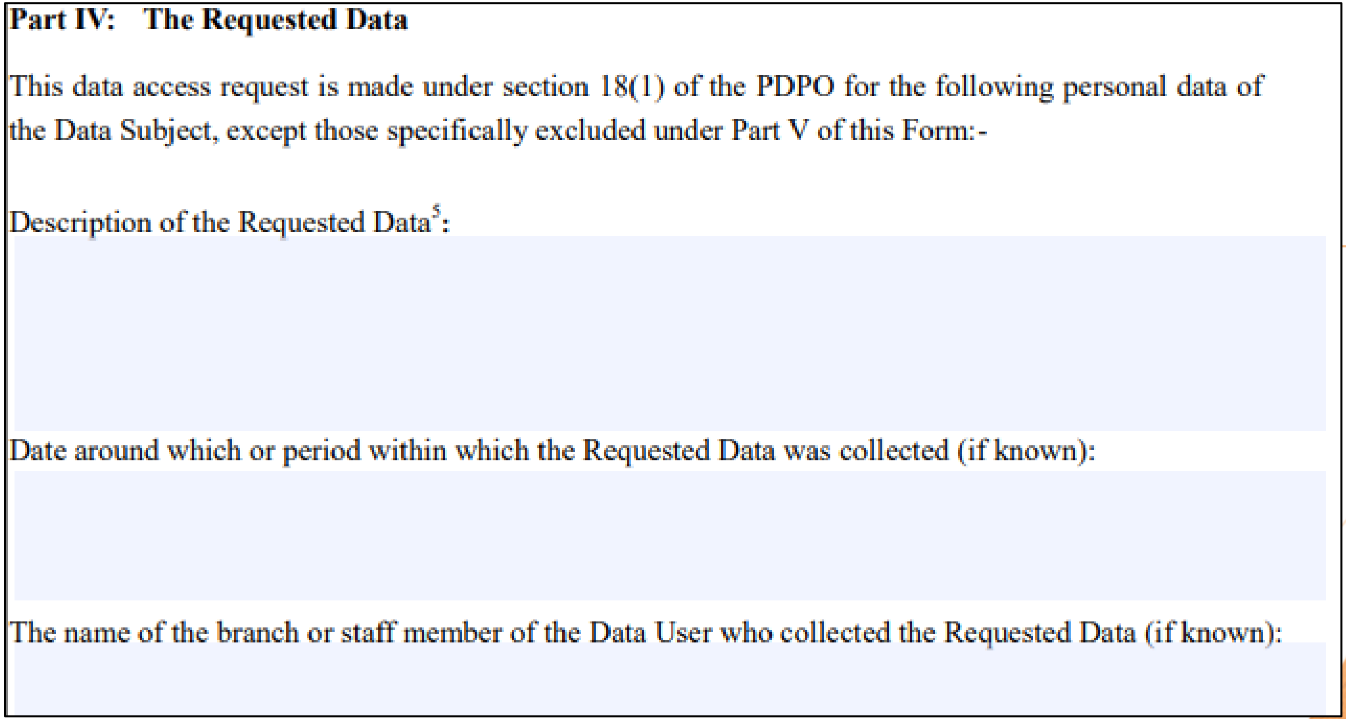
Correspondence address: ______________________________

____

Day time contact phone number: ______________________________

Email address (if any): ______________________________

The DAR form (s67) available at pcpd.org.hk



Part IV: The Requested Data

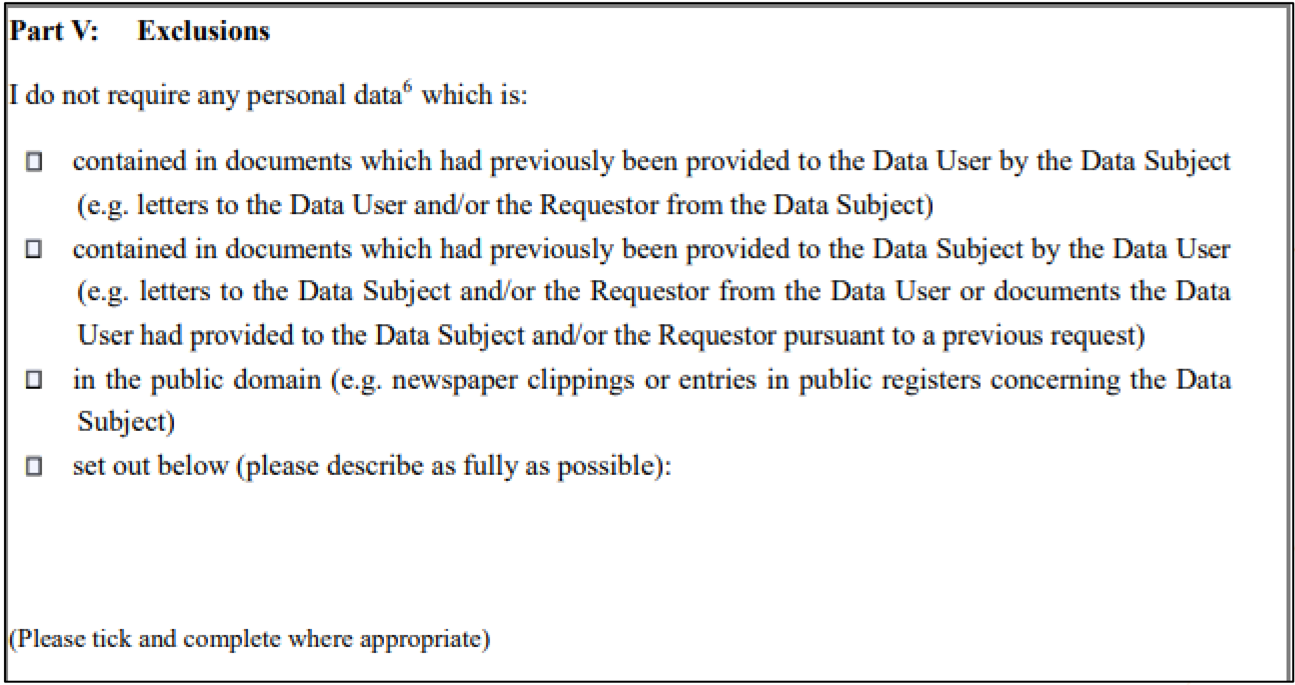
This data access request is made under section 18(1) of the PDPO for the following personal data of the Data Subject, except those specifically excluded under Part V of this Form:-

Description of the Requested Data[5]:

Date around which or period within which the Requested Data was collected (if known):

The name of the branch or staff member of the Data User who collected the Requested Data (if known):

The DAR form (s67) available at pcpd.org.hk



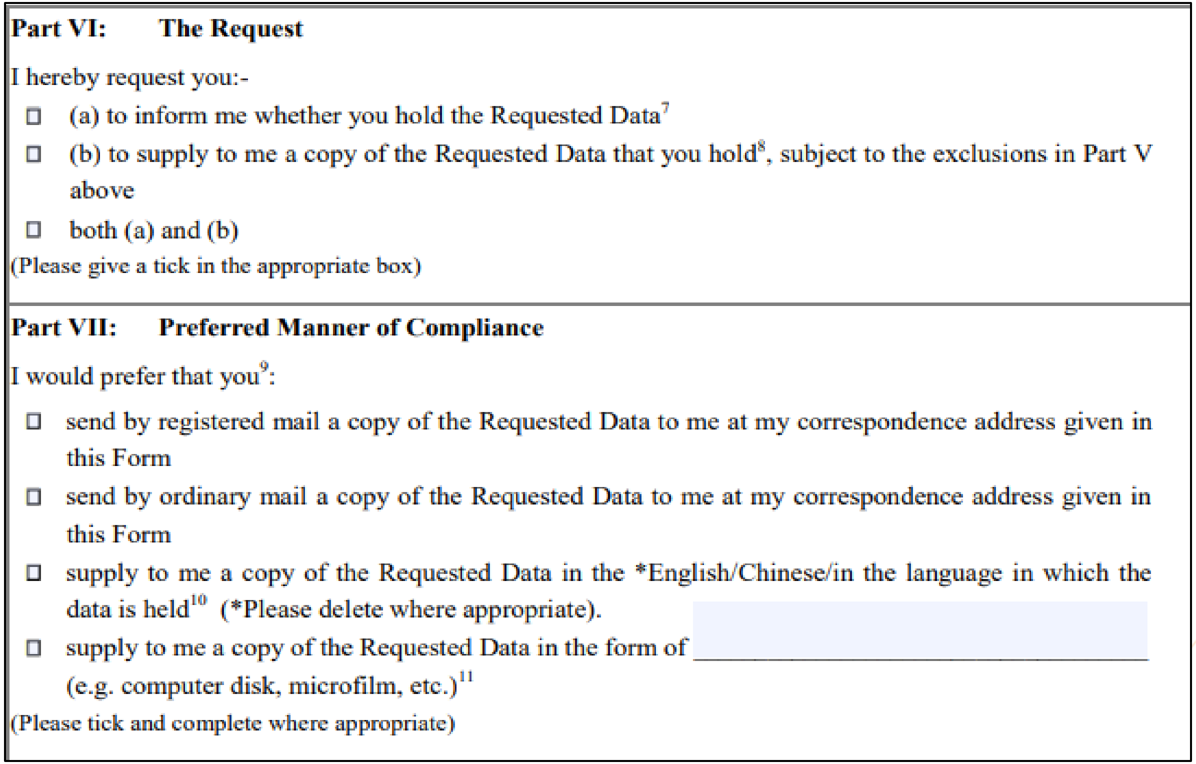
Part V: Exclusions

I do not require any personal data[6] which is:

- □ contained in documents which had previously been provided to the Data User by the Data Subject (e.g. letters to the Data User and/or the Requestor from the Data Subject)
- □ contained in documents which had previously been provided to the Data Subject by the Data User (e.g. letters to the Data Subject and/or the Requestor from the Data User or documents the Data User had provided to the Data Subject and/or the Requestor pursuant to a previous request)
- □ in the public domain (e.g. newspaper clippings or entries in public registers concerning the Data Subject)
- □ set out below (please describe as fully as possible):

(Please tick and complete where appropriate)

The DAR form (s67) available at pcpd.org.hk



Part VI: The Request

I hereby request you:-

□ (a) to inform me whether you hold the Requested Data[7]

□ (b) to supply to me a copy of the Requested Data that you hold[8], subject to the exclusions in Part V above

□ both (a) and (b)

(Please give a tick in the appropriate box)

Part VII: Preferred Manner of Compliance

I would prefer that you[9]:

□ send by registered mail a copy of the Requested Data to me at my correspondence address given in this Form

□ send by ordinary mail a copy of the Requested Data to me at my correspondence address given in this Form

□ supply to me a copy of the Requested Data in the *English/Chinese/in the language in which the data is held[10] (*Please delete where appropriate).

□ supply to me a copy of the Requested Data in the form of ______________________________ (e.g. computer disk, microfilm, etc.)[11]

(Please tick and complete where appropriate)

Data Access Request

What if the requestor make the request without using the form?

PCPD's position

- the use of form is a technical requirement
- encourage to comply with if the request substantially contains the details required

The PDPO

s20(3)(e) – may refuse the DAR if it is not made in the form

③ Compliance with / Refusal of Data Access Request

Compliance with Data Access Request

Things to note upon receipt of DAR

(Who? What? When? How?)

- Identification
- Clarification
- Timing - 40 calendar days to respond in writing
- Free or Fee

Identification

- s20(1)(a) – shall refuse DAR if the data user is not satisfied with the identity of the requestor

- Collection of HKID Card number and / or HKID Card copy?

Identification

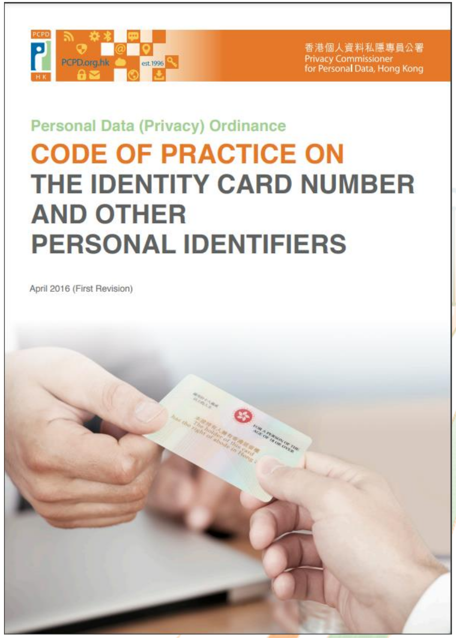
s20(1)(a) – may refuse DAR if not satisfy the identity

Footnote 3 of the Form: "… *The identity card number needs not be provided in this Form if you have reasonable grounds to believe that this will not be necessary for the unique identification of the Data Subject by the Data User in the Circumstances*"

Identification

- The Code [s12 – 3 codes: PI, HR & Consumer Credit Data]
- Collection of HKID Card number
  - ➢ 2.3.3.1 – interest of the card holder
  - ➢ 2.3.3.2 – prevention of detriment of other person
  - ➢ 2.3.3.3 – safeguard against damage / loss of the data user
- Collection of HKID Card copy
  - ➢ 3.2.2.3 – as alternative of physical production for checking

[remark: choice of data subject, not data user]



PCPD.org.hk est.1996

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

Personal Data (Privacy) Ordinance

CODE OF PRACTICE ON
THE IDENTITY CARD NUMBER
AND OTHER
PERSONAL IDENTIFIERS

April 2016 (First Revision)

Eligibility

- Data subject (資料當事人)
- Relevant person (有關人士) on behalf of the data subject
- “Relevant person” means
  - where the individual is a minor, a person who has parental responsibility for the minor
  - where the individual is incapable of managing his own affairs, a person who has been appointed by the court to manage those affairs
  - guardian of a mentally incapacitated person under Part IIIA or Part IVB of the Mental Health Ordinance (《精神健康條例》) (Cap 136)
  - person authorized in writing to make a DAR

  (sections 2(1) and 17A)

Clarification

- s20(3)(b) – may refuse DAR if data user is not supplied with information reasonably required to locate the requested data
- Is "requesting all data" a good reason to refuse?
- AAB No. 16/2008 "…*There could be cases where the personal data held by the data user is actually very simple and all of them can be located by the data user easily without any further specification or information*…"

Timing

Within 40 days after receipt of the DAR:

- to confirm the holding of the requested data and supply a copy of it [s19(1)(a)]
- to notify in writing that the data user does not hold the data [s19(1)(b)]
- to explain in writing why the data user is unable to provide the requested data and to provide the data as soon as possible [s19(2)]
- to notify in writing the refusal with reason(s) [s21(1)(a) & s21(1)(b)]
- to notify in writing the name and address of the data user who indeed controls the use of the data [s21(1)(c)]

Timing

S19(2) - Partial provision is still required

AAB No. 19/2018

"… What it does mean is that before the end of the prescribed period, the data user has to provide such documents as he is able at that time to do so. Thereafter, the data user is obliged to complete his obligations as soon as practicable."

Fee

Shall not be excessive (s28)

AAB No. 37/2009
"a fee that exceeds such direct and necessary costs is … excessive"

AAB No. 2/2018
"In not fixing the amount of fees in the legislation … the legislature must have recognized that the costs for complying with a data access request may vary not only with the scope and complexity of the data access request, but also with different data users"

Fee

The word “excessive” … should be construed as confining the fee only to cover those costs which are directly related to and necessary … but this does not mean that the data user can recover all its actual costs incurred …

If a flat rate fee is charged, so long as the flat rate fee that is imposed is lower than that direct and necessary costs for complying with a DAR …

Fee

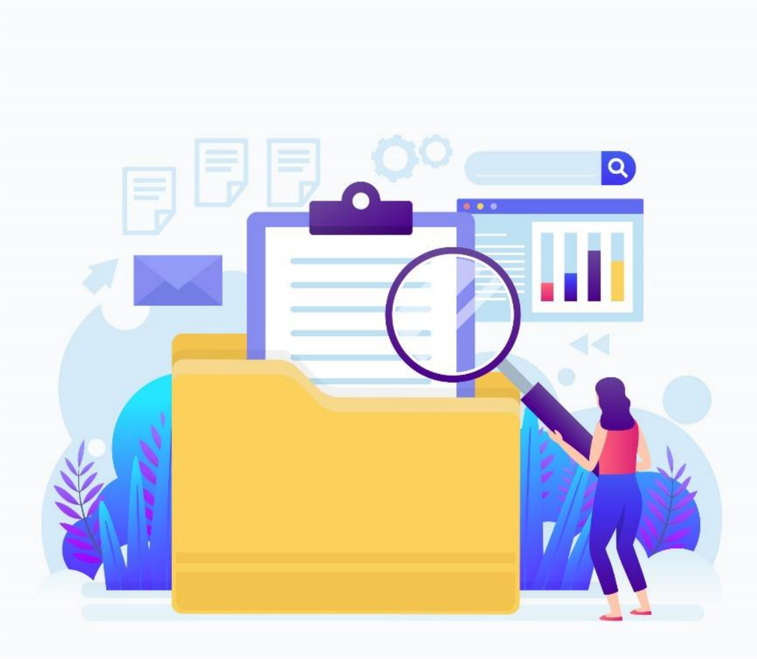
Example: A clinic to provide medical records in response to a patient’s DAR

Direct and Necessary Work	Time Spent
Retrieving the medical record	20 Minutes
Photocopying the record for redaction	10 Minutes
Redaction of personal data of other person	50 Minutes
Photocopying the redacted copy for provision	10 Minutes

Fee to collect: 1.5 x hour rate of nurse (not doctor) + photocopying fee (per page)

3

Compliance with DAR – Data provided and recorded



Compliance with DAR - Refusal

Reasons for refusal

- The DAR is not made in the form prescribed by PCPD (form OPS003)
- The data user is entitled under any Ordinance not to comply with the DAR
- Compliance with the DAR may for the time being be refused under PDPO, whether by virtue of an exemption under Part 8 or otherwise

Compliance with DAR - Refusal

Reasons for refusal

- Identity not satisfied [s20(1)(a)]
- Request not in writing in the Chinese or English language [s20(3)(a)]
- Insufficient info. to locate the requested data [s20(3)(b)]
- 2 or more similar DARs & unreasonable to comply [s20(3)(c)]
- Another user controls the use of data prohibiting the compliance [s20(3)(d)]

How?

- Refusal shall be made in writing with reasons within 40 days (section 21(1))

- Notice must be in the language in which the DAR is made, if that language is Chinese or English (section 29)

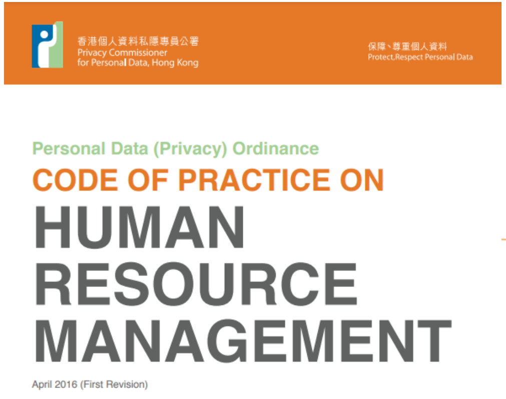
- Where there is another data user that controls the use of the data in such a way as to prohibit the data user from complying with the DAR, to notify the requestor the name and address of the other data user (section 21(1)(c))

Exemptions (Part 8 of PDPO)	Not to confirm the possession	Not to supply a copy	Expiry ?
51A – Judicial Functions	√	√	
52 – Domestic	√	√	
53 – Staff Planning		√	
55 – Relevant Process		√	Yes
56 – Personal Reference		√	Yes
59 – Health		√	
60 – Legal Professional Privilege		√	
60A – Self Incrimination		√	
61 – News		√	Yes

Compliance with DAR – Exemption for refusal

- s53 – Staff planning (職工策劃)

Personal data relevant to staff planning proposal to fill any series of positions or to cease any group of individuals' employment (e.g. restricting, reorganizing, redundancy or succession plans involving group of employees)



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

保障、尊重個人資料
Protect,Respect Personal Data

Personal Data (Privacy) Ordinance

CODE OF PRACTICE ON

HUMAN RESOURCE MANAGEMENT

April 2016 (First Revision)

Compliance with DAR – Exemption for refusal

- s55 – Relevant process (有關程序)
  - Process to determine employment / professional qualification / disciplinary action exclude the process where no appeal may be made against the determination
  - Exemption until the completion of process

Compliance with DAR
– Exemption for refusal

- s56 – Personal references (個人評介)
  - Personal reference given by an individual (A) other than in the ordinary course of his occupation and relevant to another individual (B)'s suitability to fill a position
  - Exemption until individual (A) has no objection for disclosure or individual (B) is informed of the result

Consequences of breach of DAR provisions

- Failure to comply with a DAR within 40 days (section 19(1) & (2)) or failure to give notification of refusal within 40 days (section 21(1)) – a fine at level 3 (section 64A(1))
- Data subject may take civil action against the data user to claim compensation for any damage suffered, including injury to feelings, by reason of a breach of a requirement under PDPO (section 66)
- Data subject may also make a complaint to PCPD against the data user concerned (section 37)

4 Case Studies and Practical Tips

(1) Facts of the Case

The Appellant is an officer of a Department. He submitted a DAR to the Department for a copy of all reports and documents associated with the disciplinary charge laid against him. The requested data was described as:

“ALL relevant reports / documents / correspondence associated with investigation(s) on me which led to disciplinary charge against me with regard to incident on **[dd.mm.yyyy]*****, which formed part of my personal data under relevant legislations, which are currently under custody by the Director of*** **[the Department]*****”***

(1) Facts of the Case

- The Appellant complained that the Department has not complied with his DAR within 40 days
- The Department subsequently provided the Appellant with a copy of 161 pages of the requested data, with third party information contained therein being redacted
- The Appellant considered that the Department should not make the redaction in certain items provided to him

(1) The Commissioner's Findings

- No evidence showing that the Department had deliberately delayed the compliance with the DAR

- Taking into account the volume of the requested documents that were gathered from different units, the Commissioner opined that the Department had not delayed in complying with the Appellant's DAR

- Redacted parts are either identifying particulars of other individuals or the reference number of the memo concerned. As the Appellant is only entitled to a copy of his data, the Department was not required to release the redacted parties to the Appellant in response to his DAR

(1) AAB’s Findings

Was there a potential breach of s19(2)(a)(ii) of PDPO that was not investigated by the Commissioner ?

- If the Department cannot comply with the Appellant’s DAR, the Department had to do two things:-
  - ✓Informing the Appellant by notice in writing that the Department was unable to comply with the DAR, and the reasons why the Department was unable to comply (“1st requirement”)
  - ✓Complying with the DAR to the extent that the Department was able to comply (“2nd requirement”)

(1) AAB's Findings

1st requirement – whether the Department gave notice in writing & explanation?

- ✓ Yes, the Department had informed the Appellant in writing within 40 days.

  > *"Your application is being processed by this department. Since large amount of relevant materials are required to be examined, our reply is expected to be available before* [dd/mm/yyyy]"

(1) AAB's Findings

2nd requirement – whether the Department provided documents to the extent that the Department was able to comply?

- ✓ Doubtful
- ✓ The Department provided the requested documents to the Appellant on the Day 51 upon receipt of the request
- ✓ It is reasonable to infer that the at least some of the documents were available, and could be provided to the Appellant by the end of the 40-day period. All documents were provided only 11 days after that period
- ✓ The Department's obligation was to comply with the DAR within the 40-day period to the extent that the Department was able to

(1) AAB's Findings

✓The Department had given notice and reasons within the prescribed 40-day period that it was not able to provide the documents within time

✓The delay was a relatively short delay

✓No substantial prejudice suffered by the Appellant as a result of delay

✓The Department complied with the Appellant's DAR despite the compliance was late

✓The AAB: No further investigation required

(2) Facts of the Case

- Appellant lodged a DAR to a clinic for :-
  "all medical records (including but not limited to handwritten notes made by attending doctors Mr 王XX & Ms 胡XX on [2 separate dates]) related to her"

- Clinic imposed DAR fee which included :-
  - ❖administrative fee of HK$100
  - ❖copying fee of HK$5 per page

- Appellant considered the fee to be excessive and refused to pay

(2) The Commissioner’s Findings

Breakdown of the administrative fee

- Costs of management staff’s administrative work: HK$41.77
- Costs of doctor’s approval: HK$83.30
- Cost of frontline staff’s copying work (including electricity, paper, ink and printer depreciation): Approximately HK$2/page

(2) The Commissioner's Findings

Whether the hourly rate and time taken for staff's administrative work are excessive (HK$41.77)

- No information provided by clinic on hourly rate
- Reference made to the statistics from the Census and Statistics Department
- Average hourly rate of "general office clerk" : HK$76.33

(2) The Commissioner’s Findings

- Equals to about 33 minutes work
- Amount of HK$41.77 was not excessive, after taking into account:-
  - estimated time for taking the “direct and necessary steps” in complying with the DAR; and
  - average hourly rate of a “general office clerk” to perform the tasks involved

(2) The Commissioner’s Findings

Whether the hourly rate and the time taken for doctor’s approval are excessive (HK$83.30)

Clinic provided breakdown of HK$83.30 :

- **Doctor needs to review medical record before making the copy**
- **Review of medical note (2 minutes at least): HK$83.30**
    - ➢**Hourly rate of doctor : HK$2,499**

(2) The Commissioner's Findings

- Medical record is sensitive personal data of a patient
- Necessary for a doctor to take a quick look at the document(s) requested
- Two items of labour costs, i.e. HK$41.77 + HK$83.30 = HK$125.07
  - ➢This amounts to direct and necessary costs for complying with the DAR
  - ➢Not excessive as administrative fee of HK$100 is lower

(2) The Appeal

Appellant's Arguments (only challenged doctor's costs of HK$83.30)

Two grounds of appeal:

- There is no evidentiary basis regarding how the amount of HK$83.30 was arrived at, and the Commissioner should have disallowed such sum claimed by the clinic; and
- Even if the clinic's claim for costs of doctor's work should be allowed, the actual costs incurred should have been found to be below HK$100 in total, and hence the administrative fee so charged was excessive

(2) The Appeal

AAB's Findings

- Confirmed necessary for doctor to review medical notes :-
  - ➢Medical records contain sensitive information of a very private nature about a patient
  - ➢Medical notes sought are prepared by two doctors
  - ➢"A patient may not wish others to know about his/her medical condition, illness or disease, and his/her medical records should therefore be handled with particular care"

(2) The Appeal

- The AAB also confirmed that the hourly rate and the time taken for reviewing the medical notes was reasonable.
- Therefore, the doctor's costs is directly related to and necessary for complying with the DAR.

Takeaways

- Consider the circumstances of each case
- "Excessive": only costs which are directly related to and necessary for complying with a DAR will be allowed (principles in AAB 37/2009 followed)
- As the medical records contained sensitive personal data, it would be reasonable for a doctor to review the same before releasing to the requestor

Practical tips and case studies

Redaction – put yourself in the shoes of the requestor when considering what to redact

ABC Company, in response to the DAR made by its former employee David, provided a redacted copy of an email showing "… [redacted] David is not a team player … "

Practical tips and case studies

Redaction – put yourself in the shoes of the requestor when considering what to redact

ABC Company, in response to the DAR made by its former employee David, provided a redacted copy of an email showing "… [redacted] David is not a team player … "

Clean copy of the email examined by PCPD: "… HR would like us to elaborate incidents illustrating why David is not a team player …"

Data Access Request

Practical Tips

What sort of data to be disclosed?

✓ Prohibition against disclosure under other ordinances (section 20(1)(c)), such as the secrecy provisions under

(i) section 378 of Securities and Futures Ordinance;

(ii) section 120 of Banking Ordinance; and

(iii) section 53A of Insurance Ordinance

Data Access Request

Practical Tips

- “Personal data of third party thereon” not valid ground for refusal
- Extracts - copy of personal data of data subject, not copy of document containing the data
- Redaction
- Consent of third party

Data Access Request

Practical Tips

- Fees to be charged and explained with justification by data user

- Cost generally not allowed to impose

  - legal advice (even if the advice is sought for considering whether exemption should be invoked)

  - administrative / office overheads

Training and Education

- Tailored to specific needs of relevant employees
- Cover organisation’s policies and procedures
- Be delivered in an appropriate and effective manner
- Be given to new employees in its induction programme and periodically thereafter
- Circulate essential information to relevant employees as soon as practical if an urgent need arises
- Monitor and keep records for attendance

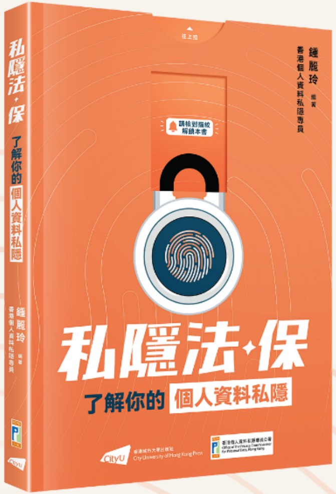
"The Treasure-trove of Privacy – Understanding Your Personal Data Privacy"

Ms Ada CHUNG Lai-ling

Privacy Commissioner for Personal Data,
Hong Kong

Highlights:

- Data Protection Principles
- Combating Doxxing
- Trends of Privacy Protection
  - ♦ Artificial Intelligence
  - ♦ Chatbot
- Savvy Tips for Protecting Privacy



Buy Now

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

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner

https://www.pcpd.org.hk/Toolkit/tc/

數據安全新!

數據安全

七大資料保安建議措施

- 資料管治和機構性措施
- 風險評估
- 技術上及操作上的保安措施
- 資料處理者的管理
- 資料保安事故發生後的補救措施

數據安全專題網頁
Data Security Webpage

https://www.pcpd.org.hk/tc_chi/data_security/index.html

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$450 per year

Enquiries: dpoc@pcpd.org.hk

https://www.pcpd.org.hk/misc/dpoc/files/AppForm_23_24_NewMember_OnlineVersion.pdf

Disclaimer

- The information provided in this PowerPoint for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (Cap 486) (“**PDPO**”).
- For a complete and definitive statement of law, direct reference should be made to the PDPO itself.
- The Office of the Privacy Commissioner for Personal Data makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this PowerPoint.
- The contents provided will not affect the exercise of the functions and powers conferred to the Commissioner under the PDPO.

Contact Us

Hotline 2827 2827　　Fax 2877 7026

Website www.pcpd.org.hk

Email communications@pcpd.org.hk

Address Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen’ s
Road East, Wanchai, Hong Kong

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

追蹤我們
最新資訊

Thank you!

PCPD HK