Introduction to the Personal Data (Privacy) Ordinance

01

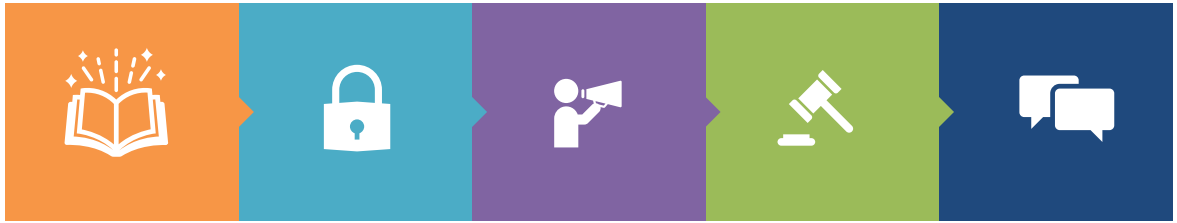
Introduction to the Concept of Privacy and the PD(P)O

03

Direct Marketing

05

Q&A



02

Six Data Protection Principles

04

Offences & Compensation

1 Introduction to the Concept of Privacy and the PD(P)O

What is “Privacy”?

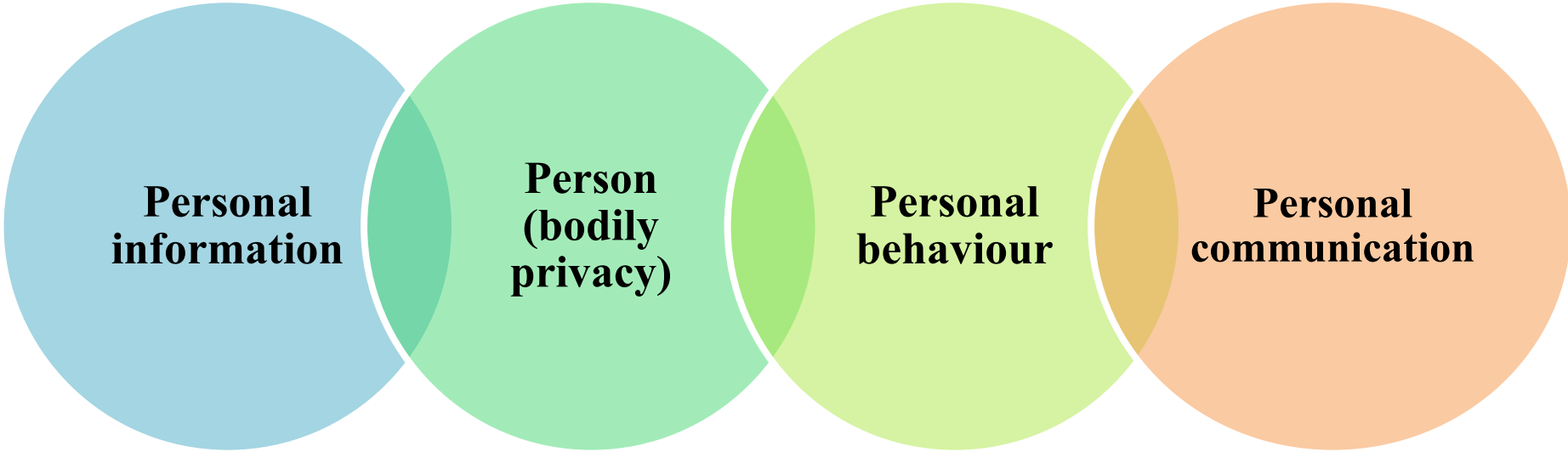
“the right to be let alone, or freedom from interference or intrusion”

https://iapp.org/about/what-is-privacy/

“Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.”

https://www.privacyinternational.org/explainer/56/what-privacy

Privacy covers…



HK: Personal Data (Privacy) Ordinance (PDPO) (came into effect in 1996)

One of the earliest comprehensive data protection laws in Asia

Personal Data (Privacy) Ordinance
(came into effect in 1996)

Expected effect

Business Perspective

- To facilitate business environment
- To maintain Hong Kong as a financial and trading hub

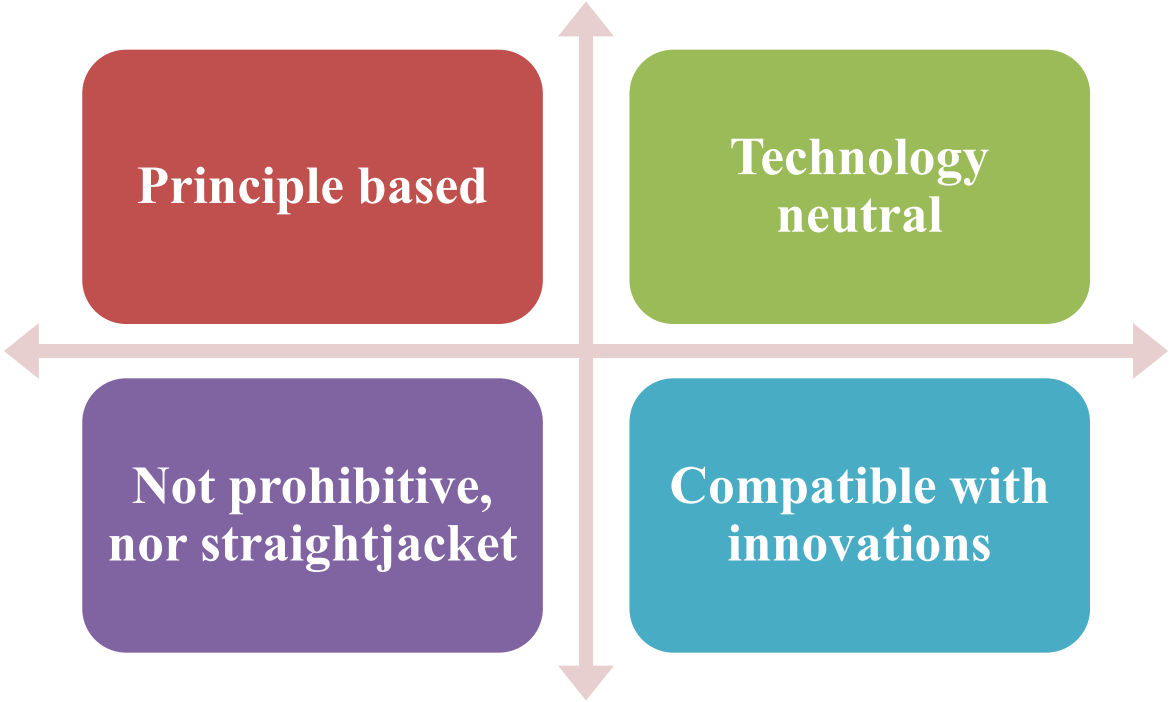
Human Rights Perspective

- Protect individuals' personal data privacy

Personal Data (Privacy) Ordinance, Cap 486
(came into effect in 1996)

- Established an independent authority, Privacy Commissioner for Personal Data
- Covers both public (government) and private sectors
- The Data Protection Principles outline how data users should collect, handle and use personal data
- Complemented by other provisions imposing further compliance requirements

Characteristics of the PD(P)O



What is “Personal Data”?

“Personal Data” should satisfy three conditions:

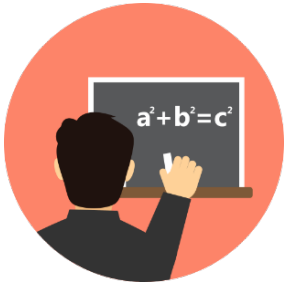
1) relating directly or indirectly to a living individual;

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

3) in a form in which “access to” or “processing of” the data is practicable.

The PD(P)O Governs All Data Users

- A "data user" is a person who either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.



2

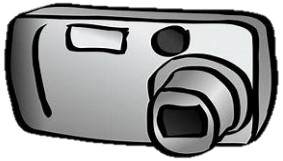
Six Data Protection Principles (DPPs)

- The six data protection principles (DPPs) form the base of the PD(P)O.

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

“Collection” of Personal Data – Case Sharing

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**

Example of unfair collection – blind advertisement

Company Assistant

- Form 5 or above
- Knowledge of company secretarial duties

Please send resume to PO Box 100

- Submission of personal data by job applicants
- No identity of the employer provided
- No notification of purpose of use of the data
- Job applicants are denied of data access rights

Company Assistant

- Form 5 or above
- Knowledge of company secretarial duties

Interested parties please contact our Human Resource Officer, Miss Angel Chan on 2808-2808

- No submission of personal data by job applicants
- Contact person provided from whom applicants:
  - may seek to identify the employer
  - may seek information about purpose statement

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**

Principle 1 – Purpose and manner of collection

Advice to Data Subjects

- Provide necessary but not excessive personal data to organisations for the prescribed purpose

Principle 1 – Purpose and manner of collection

inform the data subject of the following immediately or in advance:

a) the purposes of data collection;

b) the classes of persons to whom the data may be transferred;

c) whether it is obligatory or voluntary for the data subject to supply the data;

d) where it is obligatory for the data subject to supply the data, the consequences for him if he fails to supply the data; and

e) 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 1 – Purpose and manner of collection

Personal Information Collection Statement (PICS)

- Should ensure that a PICS is effectively communicated to the data subjects. Considerations include the layout and language used in the PICS

- Should define the purpose of use and class of data transferees with a reasonable degree of certainty

Principle 1 – Purpose and manner of collection

Advice to Data Subjects

- Read the Personal Information Collection Statement thoroughly before providing personal data for any individuals or organisations

Principle 1 – Purpose and manner of collection

Advice to Data Subjects

- When providing personal data to organisation for commercial promotion to obtain free service or gifts, data subjects should consider whether there are risks if they provide personal data to the organisation concerned
- Data subjects should also consider if the provision of personal data is proportionate to the value of the free service or gifts

Principle 2 – Accuracy and duration of retention

- Data users shall take practicable steps to ensure the accuracy of personal data held by them

- All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of 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

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

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

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

Data Breach Handling – Action

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 – Action

Contacting the Interested Parties & Adopting Containment Measures

Interested parties may include:

- The law enforcement agencies
- The relevant regulators (e.g. Privacy Commissioner for Personal Data, Hong Kong (the "Commissioner"))
- The Internet companies
- IT experts

Data Breach Handling – Action

Assessing the Harm

Assessing the potential harm caused by a data breach, for examples:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and employment opportunities

Data Breach Handling – Action

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

What is a data breach notification?

- A formal notification given by the data user to the data subjects affected and the relevant parties and regulators in a data breach.
- 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.

What is a data breach notification?

- If a data user decides to report a data breach to the Commissioner, the data user may complete a Data Breach Notification Form and submit the completed form to us online, by fax, in person or by post.

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

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: _____

Principle 5 – Information to be generally available

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 5: Advice to Wi-fi Service Provider

- Privacy Policy Statement of Wi-fi service should not be made in unreasonably small fonts
- Wi-fi service provider should ensure that the Privacy Policy is effectively communicated to Wi-fi users. Considerations include the font size, layout and language used in the Privacy Policy

Principle 6 – Access to personal data

- A data subject shall be entitled to
  (a) request access to his/her personal data;
  (b) request correction of his/her personal data

- Data user may charge a fee for complying with the data access request

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)(a) 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).

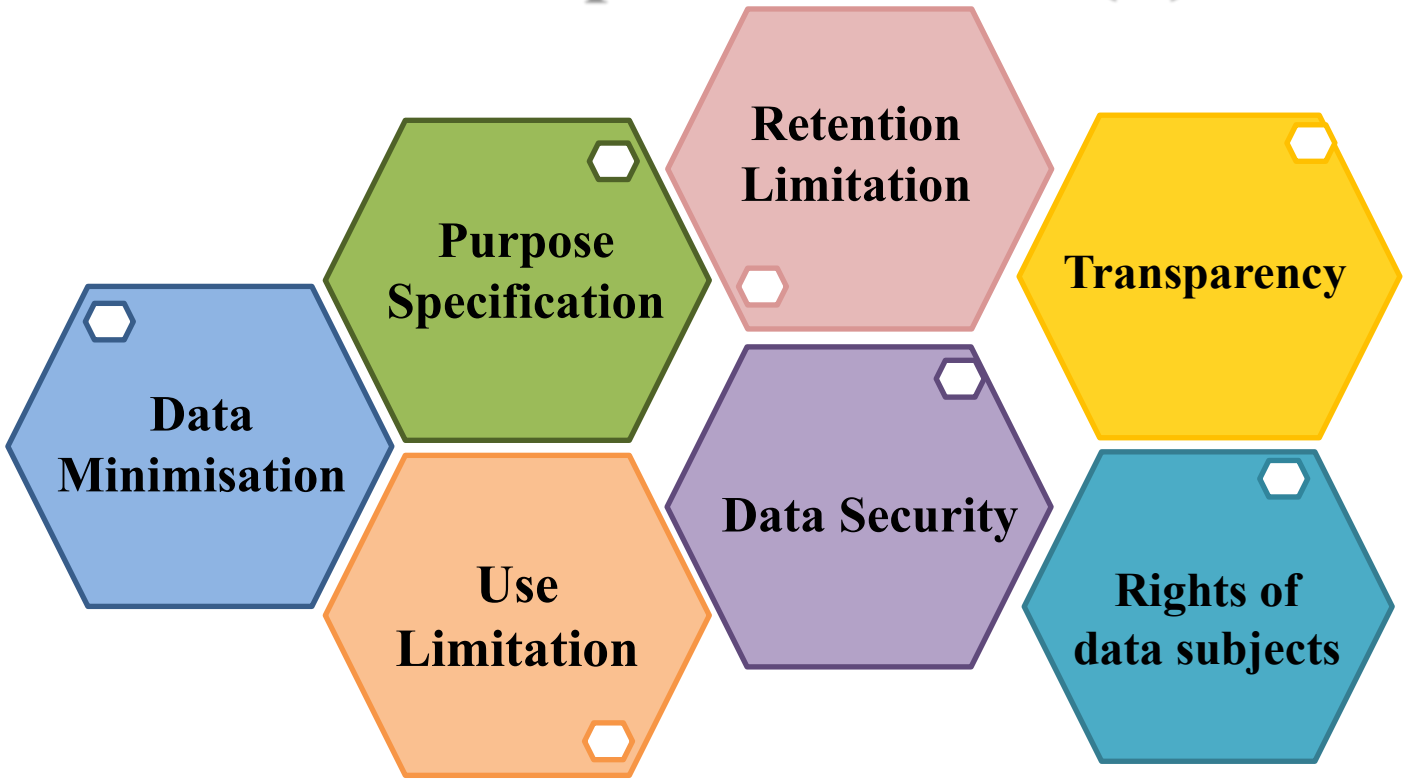
3. If you have a lawful reason for refusing to comply with the request pursuant to section 20 of the PDPO, you must give the requestor **written notification** of your refusal and your supporting reasons **within the same 40-day** period (see section 21(1) of the PDPO).

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

Principles of the PD(P)O



3 Direct Marketing

Use of Personal Data in Direct Marketing

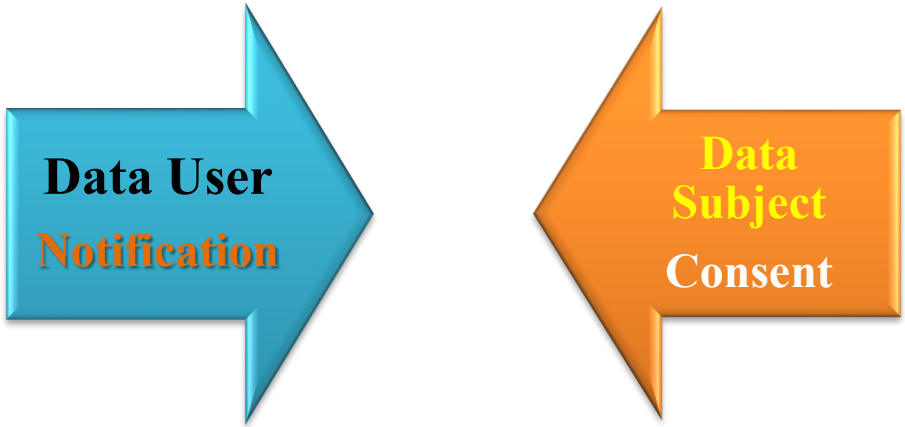
- Direct Marketing means sending promotional information of goods or services, addressed to specific persons by name by mail, fax, email or phone

- Under the existing Ordinance, data user must notify a data subject of his opt-out right when using his personal data in direct marketing for the first time

- Upon receiving an opt-out request, the data user must cease using the data

Regulatory Regime of Direct Marketing

Intends to use personal data or provide personal data to another person for use in direct marketing



Provision of Personal Data

▪ Provide data subjects with "prescribed information" and response channel through which the data subject may elect to give consent ▪ Notification should be easily understandable	▪ Should be given explicitly and voluntarily ▪ "consent" includes an indication of "no objection"

Regulatory Regime of Direct Marketing

Use of Personal Data in Direct Marketing	Provide Personal Data to another person for Use in Direct Marketing
1. The data user intends to use the personal data of the data subject for direct marketing;	1. The data user intends to provide the personal data of the data subject to another person for use by that person in direct marketing;
2. The data user may not so use the data unless the data user has received the data subject's consent to the intended use;	2. The data user may not so provide the data unless it has received the data subject's **written consent** to the intended provision;
3. The kinds of personal data to be used;	3. The provision of the data is **for gain** (if it is to be so provided);
4. The classes of marketing subjects in relation to which the data is to be used;	4. The kinds of personal data to be provided;
5. The response channel	5. The classes of persons to which the data is to be provided;
	6. The classes of marketing subjects in relation to which the data is to be used; and
	7. The response channel

“Consent” includes an “indication of no objection”

Example of indicating no objection *generally*:

We intend to use your name, telephone number and address for direct marketing credit card and insurance products/services but we cannot so use your personal data without your consent.

Please sign at the end of this statement to indicate your agreement to such use. Should you find such use of your personal data not acceptable, please indicate your objection before signing by ticking the box below.

☐ The customer named objects to the proposed use of his/her personal data in direct marketing.

_____

Signature of the customer
Name: xxx
Date: yyyy/mm/dd

Return the signed form but did not check the box indicating objection = consent

Regulatory Regime of Direct Marketing
Higher Penalties for Non-Compliance

	Maximum Fine (HK$)	Maximum Imprisonment
Non-Compliance	500,000	3 years
Non-Compliance if the personal data is provided to third party for its use in direct marketing in exchange for gain	1,000,000	5 years

Guidance to help data user

- **"New Guidance on Direct Marketing"**(Jan 2013 edition), explaining the requirements under the new regime and providing practical guidance to data users.
- **Professional Workshop**, to familiarise organisations with the new provisions and compliance measures.

4 Offences & 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 • in case of a continuing offence, a daily fine of $1,000

Compensation

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

Factors to be considered in vetting an application

- ✓ whether there is sufficient evidence to show that there is a contravention of a requirement under the Ordinance by a data user
- ✓ whether the applicant can provide sufficient evidence to show that he/she has suffered damage by reason of a contravention of a requirement under the Ordinance (the applicant has to provide evidence to support his/her application)
- ✓ whether the case raises grave privacy concern and data protection implications
- ✓ whether it is unreasonable to expect the applicant to deal with the case unaided

How to provide proof of damage?

- injury to feelings? (e.g. certificate of attendance, sick leave certificate)
- financial loss? (e.g. receipts for the expenses incurred)
- damage to reputation? (e.g. information posted on the internet)

To prove that the damages suffered were caused by the contravention of the requirement of the Ordinance

Code of Practice

- Identity Card Number and other Personal Identifiers
- Human Resource Management
- Consumer Credit Data

Guidelines and leaflets

- Privacy Management Programme: A Best Practice Guide (Revised in August 2018)
- New Guidance on Direct Marketing
- Monitoring and Personal Data Privacy at Work
- Guidance on Collection and Use of Biometric Data
- Guidance on CCTV Surveillance Practices
- Guidance on Data Breach Handling and the Giving of Breach Notification

Guidelines and leaflets

- Guidance on the Use of Portable Storage Devices
- Guidance for Data User on the Collection and Use of Personal Data through the Internet
- Guidance on Personal Data Erasure and Anonymisation
- Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users

Guidelines and leaflets

- Booklet: European Union General Data Protection Regulation 2016 (Effective 25 May 2018) (March 2018)
- Information Leaflet: An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012
- Information Leaflet: Offence for disclosing personal data obtained without consent from the data user
- Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors

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

PCPD.org.hk

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

About PCPD | Data Privacy Law | News & Events | Enforcement Reports | Frequently Asked Questions | Compliance & Enforcement | Doxxing Offences NEW! |
Complaints | Education & Training | Resources Centre | Contact Us

- Publications
- Multimedia
- Industry-specific Resources
- Resources by Topics
- Publications for Sale

- Court Judgment
- Administrative Appeals Board's Decisions
- Case Notes
- Data Breach Notification
- Submissions on Privacy Issues
- Consultations

A Quick | Hot Search | Advan | rch

Follow

What's New More

Response to me dent of Celebrations
Coordination O

PCPD organised a Webinar on "Recommended Model Contractual Clauses for Cross-border Transfers of Personal Data"

Reaching Out to the Community — Assistant Privacy Commissioner attended Meeting of the Southern District Fight Crime Committee

PCPD Made an Arrest For a Suspected Doxxing Offence

PCPD Publishes Two Investigation Reports and a New Edition of Guidance Note for the Property Management Sector

DAB's Seminar – Privacy Commissioner briefed members of the Democratic Alliance for the Betterment and Progress of Hong Kong on the Personal Data (Privacy) (Amendment) Ordinance 2021 and related enforcement actions

Reaching out to Governance Professionals - PCPD Delivered a Presentation at the HKCGI's "23rd Annual Corporate and Regulatory Update"

Privacy Commissioner Publishes an Article on "Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data" at Hong Kong Lawyer

Privacy Commissioner Contributes to the Guidance Issued by The Hong Kong Chartered Governance Institute Regarding Personal Data Retention in the Due Diligence Process

Privacy Commissioner Publishes an Article on the "Guidance on the Ethical Development and Use of Artificial Intelligence" in the Global Privacy Assembly May 2022 Newsletter

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

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** Room 1303, 13/F
  Dah Sing Financial Centre
  248 Queen's Road East
  Wanchai, Hong Kong


追蹤公署社交平台以
接收最新資訊 ！
Follow us to receive PCPD's latest updates!
FOLLOW US
保障、尊重個人資料私隱
Protect, Respect Personal Data Privacy