

Introduction to the Personal Data (Privacy) Ordinance



PCPD



H K



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



PDPO Overview



**Offences and
Compensation**



**Six Data Protection
Principles**



Q&A



**Direct
Marketing**

PCPD



H K



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



1. Introduction to the Concept of Privacy and the PDPO

PCPD



H K



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

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>

4

Privacy covers...

Personal
information

Person
(Bodily
privacy)

Personal
behaviour

Personal
communication

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

One of the earliest comprehensive data protection laws in Asia

OECD
Guidelines
1980



1995 EU
Data
Protection
Directive



PDPO
Adopt all OECD
Principles
except
Accountability

Legislative Intent

Business

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



Human Rights

- protect the privacy right of individuals

Personal Data (Privacy) Ordinance, Cap 486

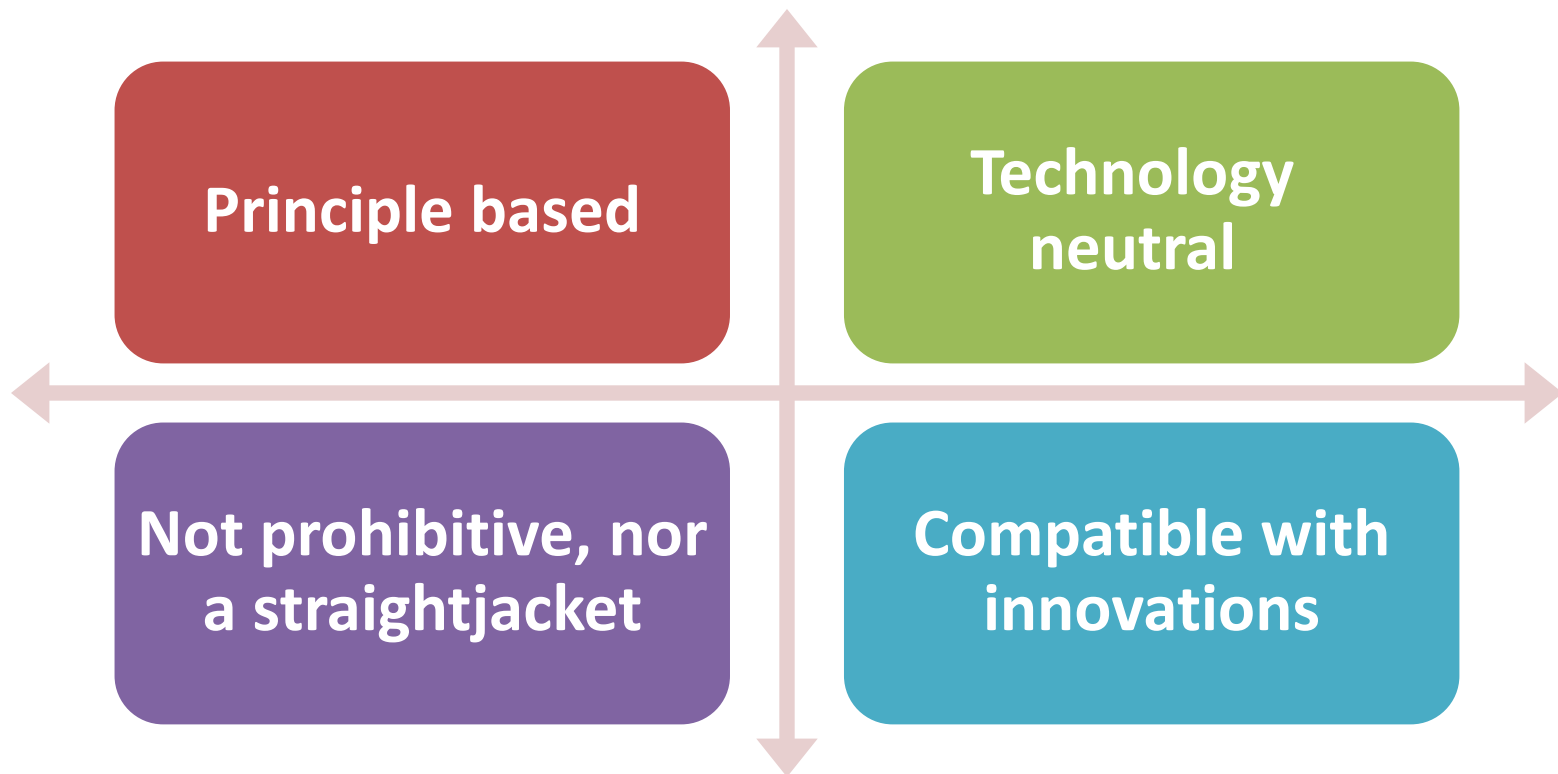
Established an independent authority, the Office of the Privacy Commissioner for Personal Data (PCPD)

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 PDPO



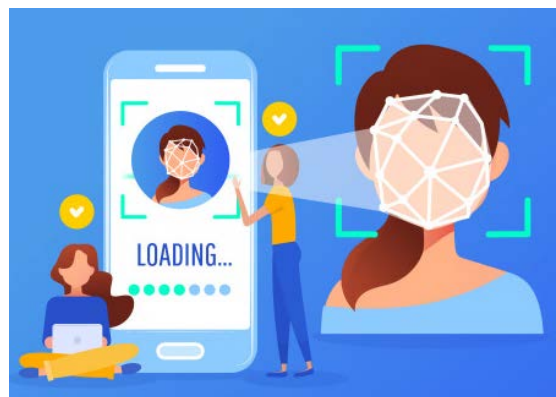
What is “Personal Data”?

(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



PCPD



H K

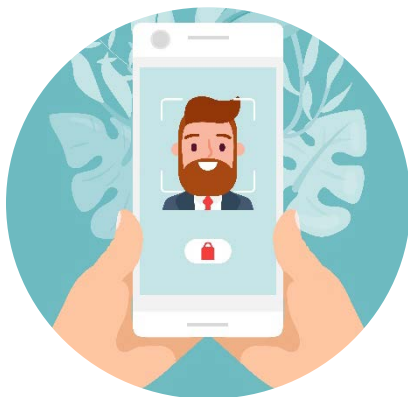


香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

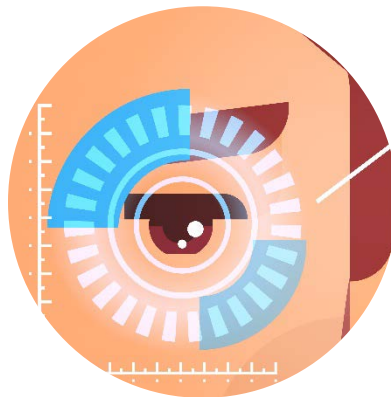
Applications of Biometric Data



Use of fingerprints
for transaction
authorisation



Use of facial
recognition to unlock
smartphones



Use of retina
recognition system
for entry
monitoring



Use of voiceprints
for identity
verification in
telephone banking

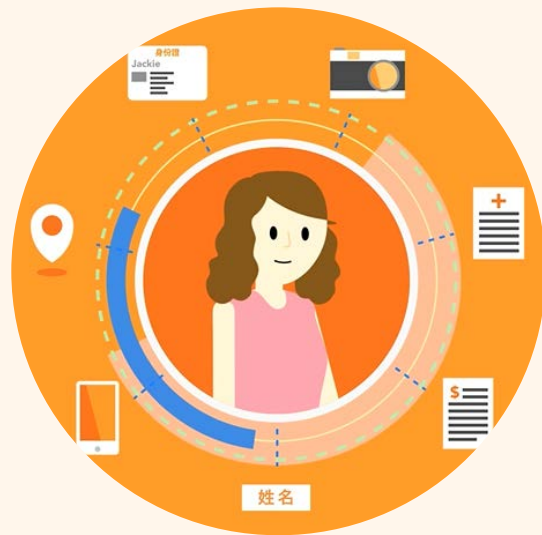
Is email address regarded as personal data?

- abc123@gmail.com
- [name]@[company's name].com



Who is the “Data Subject”?

- Data subject is **a living individual** who is the **subject of the personal data** concerned
- Under the PDPO, a person who passed away is **not** a data subject



Who is the “Data User”?

- A person, who, either **alone** or **jointly** or in common with other persons
- **Controls** the collection, holding, processing or use of the data
- Including government departments, public and private sector and individuals



15

Who is the “Data Processor”?

- Processes personal data **on behalf of** another person; and
- Does not process the data for any of his own purposes
- **Data user is responsible** for acts and practices of employees and agents



16



Data Protection Principles (“DPPs”)

- All data users must comply with the six DPPs
- The six DPPs cover every item of personal data in the **whole data processing cycle** from collection, retention, use to destruction

6

保障資料原則 Data Protection Principles

PCPD.org.hk

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



資料使用者須確保保持有的個人資料準確無誤，資料的保留時間不應超過達成原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill 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



資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, 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.



The *Eastweek* case



Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data (CACV 331/1999)

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

“Collection” of Personal Data – Case Sharing

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

20

DPP1: Collection Purpose & Means

- Personal data must be collected in a **lawful** and **fair** way, for a purpose **directly related** to a function/activity of the data user.
- Data collected should be **necessary but not excessive**.
- 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**.



21



Example of Unfair Collection – Blind Advertisement



Intern

- University students
- Knowledge of company secretarial duties

Please send resume to PO Box 100

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



Intern

- University students
- Knowledge of company secretarial duties

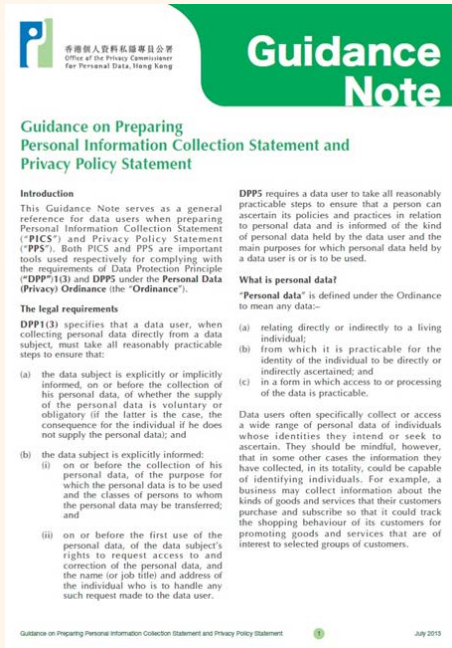
Interested parties please contact our Human Resource Officer, Miss Angel Chan on 2808-2808

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

Personal Information Collection Statement (PICS)

Inform data subject of the followings immediately/
in advance:

1. the **purpose** that the data to be used
2. **classes of persons** to whom the data may be transferred
3. whether it is **obligatory/voluntary** to supply (if obligatory, the **consequences of failure to supply**)
4. rights to make **data access/correction request**, and the relevant **channels**



Example of Personal Information Collection Statement (PICS)

ABC University

Admission - Personal Information Collection Statement

The personal data collected in this application form will be used by the ABC University for selection for admission, award of entrance scholarships, and communications on admission-related matters.

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 admission purpose for a period of six months. In case of application for admission to a programme jointly organised by the University and a partner institution, your personal data may be transferred to the partner institution concerned for the aforesaid purposes.

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 by [contact details].

**Purpose
Statement**

**Obligatory /
optional to
provide data**

**Classes of
transferees**

**Access &
correction
right**

Other practical tips for preparing the PICS



1. Design the layout of PICS (including font size, spacing and use of appropriate highlights) in an **easily readable** manner
2. Present PICS in a **conspicuous** manner (in a stand-alone notice/section)
3. Use reader friendly language (**simple words**)
4. Link to Privacy Policy Statement



DPP2: Accuracy & Retention

Data users should take all practicable steps to ensure:

- the accuracy of the personal data
- the personal data is not kept longer than is necessary for the fulfilment of the purpose for which the data is used

If a data processor is engaged to process personal data, the data user must adopt contractual or other means to prevent the personal data from being kept longer than is necessary



DPP3: Use of Personal Data

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

New purpose

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



27

Wrongful Use of Personal Data

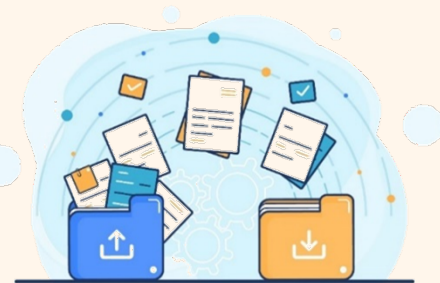
- making **direct marketing approaches**, e.g. offering services and goods of the employers
- transferring the job applicants' data to **third parties for business or other purposes**
- using the **interview records**, e.g. video recordings for **training purposes**
- using the applicants' data for **statistics or research purposes** without erasure of personally identifying particulars



DPP4: Security of Personal Data

DPP4(1): all practicable steps should be taken to protect personal data from **unauthorised/accidental** access, processing, erasure, loss/use

- ✓ **physical location** where the data is **stored**
- ✓ any **security measures** incorporated into any equipment in which the data is stored
- ✓ any measures taken for ensuring secure **transmission** of the data



DPP4: Security of Personal Data

DPP4(2): if a **data processor** is engaged to process personal data, data user must use **contractual/other means** to ensure that the personal data transferred to the data processor is protected against unauthorized/accidental access, processing, erasure, loss/use



30

Data Breach – Common Categories



Cyber attack or hacking



**Misconfiguration
of systems**



**Loss of documents or
portable devices**



**Improper/wrongful
disposal of personal data**



Errors with posts or emails



Staff misconduct

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



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

Data Breach Notification

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



36

Data Breach Notification

About PCPD | Data Privacy Law | News & Events | Compliance & Enforcement | Complaints | Legal Assistance | Education & Training | Resources Centre | Enquiry



Home > Compliance & Enforcement > Data Breach Notification

Compliance & Enforcement

Commissioner's Findings

Court Judgment

Administrative Appeals Board's Decisions

Case Notes

[Data Breach Notification](#)

Submissions on Privacy Issues

Consultations

Data Breach Notification

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

While 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, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident. You may make reference to our "[Guidance on Data Breach Handling and the Giving of Breach Notifications](#)" before submitting a data breach notification.

For submitting a data breach notification to the PCPD, please click [here](#) to download the Data Breach Notification Form. You can then fill in the form by making reference to the "Notice" and "Information Notes" contained therein.

After completing the form, please submit it and other relevant documents concerning the data breach (if any) which you wish to provide by clicking the icon below and following the instructions.

Upload Data Breach Notification Form and other documents:

(At most 20MB in total)

Acknowledgement through email

- Please note that if your submission of the Data Breach Notification Form is successful, you will receive a confirmation notification. You may also choose to provide your email address here:

Please Enter Email Address , so that the system can send an acknowledgement to your email address.

- Please input the verification code appearing in the picture on the right*:

8 7 A 1



歡迎 香港個人資料私隱專員公署



資料外洩事故通報表格

通知

資料使用者(或根據《個人資料私隱條例》(下称「條例」)作出資料外洩事故通報,並按法律規定,你在決定是否向專員作出通報時,應考慮專員發出的《資料外洩事故的處理及通報指引》。在大多數情況下,通知安妥的資料當事人(或根據《條例》作出通知)是明智之舉。

通報人士(即資料使用者)的資料

姓名:
地址:
電話號碼: 傳真號碼:
電郵地址:

如由機構作出通報,請提供下列資料:

聯絡人:
姓名 (*先生/女士/小姐):
與通報機構的關係(例如: 職員): 傳真號碼:
電話號碼:
電郵地址:
(*請填上正確傳真)

資料外洩事故的詳情 (是處註*)

已接收: 將會採取的資料外洩事故的行動 (是處註*)
請詳列已採取或將會採取的行動, 措施, 以減低及減少事故的影響

資料風險: (是處註*)
事件是否造成資料風險, 對個人資料造成風險? (請在以下一格加上「√」號) ☐ 是 ☐ 否
請解釋為何有/沒有實質的資料風險

向資料人士提供的協助及建議
請詳列 (a) 如何通知受事故影響的個人資料人士; 及 (b) 如何門戶安全, 協助或提供因有資料外洩事故而受風險, 你做了甚麼或可以與甚麼以協助他們處理, 減低有關風險或後果

通報其他機構 / 監管機構 / 執法部門
如已作出有關通報, 請提供詳情

簽署:
姓名:
職銜:
日期:

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



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

PCPD



H K

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
專題網頁
Data Security
Webpage



[https://www.pcpd.org.hk/tc_chi/
data_security/index.html](https://www.pcpd.org.hk/tc_chi/data_security/index.html)



DPP5: 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**



DPP6: Data Access & Correction

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 data access request.

Data Access Request Form

個人資料(私隱)條例 查閱資料要求表格	
查閱資料要求表格的重要提示	
1. 請在填寫表格前，細閱本表格的內容及註釋。如本表格載有《個人資料(私隱)條例》(下稱「本條例」)內有關規定的摘要，該摘要只作參考之用。關於本條例的詳細說明內容，請參閱本條例的條文。	
2. 本表格是供個人資料主(下稱「專員」)根據本條例第 47(1)條而發出的。其有效期間為 2012 年 10 月 1 日。如你不相信本表格能反映查閱資料要求(下稱「你的要求」)，資料使用者可拒絕提供你的要求(見本條例第 200(1)(b)條)。	
3. 請以中文或英文填寫本表格。如你的要求不是以中文或英文作出，資料使用者可拒絕提供你的要求(見本條例第 200(1)(b)條)。	
4. 查閱資料要求必須由你作為資料當事人或由本條例第 2 條或 17A 條所指的「有關人士」(請參閱本表格第 III 節)提出。	
5. 你沒權查閱不屬於你的個人資料或有關個人資料的資料(見本條例第 18(1)(b)條)。資料使用者只須向你提供你的個人資料的副本，而不能載有你的個人資料的文件或副本。在大多數情況下，資料使用者或選擇提供有關文件的副本。如你所要求的個人資料是以錄音形式記錄，資料使用者可提供該段載有你的個人資料的錄音副本。	
6. 你必須在本表格內清楚及詳細地指明你所要求的個人資料。如你未能向資料使用者提供你為作出此項要求而提供的個人資料，資料使用者可拒絕提供你的要求(見本條例第 200(1)(b)條)。如你未能向資料使用者提供你的要求(即在本表格內提供虛假或誤導性的資料，可構成違反本條例第 18(1)(b)條)。	
7. 請勿在本表格填寫專員、填妥的表格應直接遞交資料使用者，以作出你的要求。	
8. 資料使用者可要求你提供身分證、例如你的身分證、及向你索取從查閱資料要求的費用(見本條例第 200(3)(a) 及 200(3)(b)條)。	
9. 資料使用者在本條例第 200 條規定的情況下可拒絕提供你的要求。	
第 I 節：資料使用者 向其提出查閱資料要求的資料使用者資料 姓名或名稱 (正印全名)：_____ (附印) 地址：_____ 電話：_____ 傳真：_____	
第 II 節：資料當事人 提出查閱資料要求的資料當事人資料 中文姓名：_____ 英文姓名(正印全名，附印)：_____ 個人資料代號、例如香港身分證號碼、護照號碼或以往由資料使用者編配的其他身分識別號碼(附印，例如學生編號、教員編號、病人編號、帳戶號碼、會員號碼或其他參考編號)：_____ 通訊地址：_____ 以附印地址號碼：_____ 電郵地址(如可)：_____	
第 III 節：查閱資料要求者 查閱資料要求者的資料及身分 中文姓名：_____ 英文姓名(正印全名，附印)：_____ 通訊地址：_____ 以附印地址號碼：_____ 電郵地址(如可)：_____	
第 IV 節：查閱資料要求者與資料當事人、或資料當事人 查閱資料要求者與資料當事人、或資料當事人 資料當事人與本人是本人擬下達情況以「有關人士」的身分，代表資料當事人作出的： <input type="checkbox"/> 資料當事人是未成年人士，本人對資料當事人有作為父母親的責任。 <input type="checkbox"/> 資料當事人無力處理其本身事務，本人由法庭委任以處理其事務。 <input type="checkbox"/> 資料當事人是《精神健康條例》(第 136 章)第 2 條所指的病人上無行為能力，而： <input type="checkbox"/> 本人根據該條例第 44A、44B 或 44C 條獲委任為他的代理人。 <input type="checkbox"/> 本人根據該條例第 44B(2A)條獲委任，為其代理人或獲委任為他的代理人。 <input type="checkbox"/> 本人是資料當事人，曾向法院代表他/她提出此項查閱資料要求。 請的填妥表格內加上「已」印。	

Who could make a DAR?

- Data subject
- Relevant person 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 authorised in writing to make a DAR (sections 2(1) and 17A)

3. Direct Marketing

What is “Direct Marketing”?

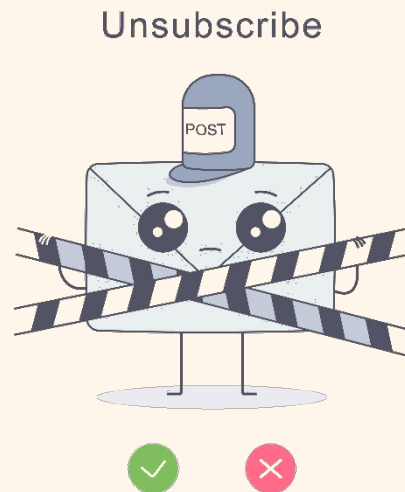
- a. the offering, or advertising of the availability, of goods, facilities/ services; or
- b. the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political/ other purposes,

through **direct marketing means** (s.35A(1)).








What is “Direct Marketing”?

- “Direct marketing means” is further defined to mean:
 - a. sending information or goods, addressed to **specific persons** by name, by mail, fax, electronic mail or other means of communication; or
 - b. making telephone calls to specific persons.



Examples of DM

1. A bank encloses a donation form of a charitable organisation in the monthly bank statements it sends to its personal customers 
2. A telecommunications service provider approaches its existing customers by telephone to offer upgraded services 
3. Direct mail sent to an address or the “occupant” of an address without addressing specific persons by name 
4. A customer service manager introduces goods/services to a customer face-to-face 
5. A bank sends a supermarket gift voucher to an existing customer as a token of appreciation 

45

Regulatory Regime of Direct Marketing

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

- Provide data subjects with “prescribed information” and response channel through which the data subject may elect to give consent
- Notification should be easily understandable

Data User
Notification



Data Subject
Consent

Provision of
Personal Data :

- “Consent” includes an indication of “no objection”

“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**

47



4. Offences and Compensation



Offences under the PDPO



Contravention of DPPs

- **not** an offence
- may serve an enforcement notice on the relevant data user directing the data user to remedy the contravention

Non-compliance with an enforcement notice

- **Criminal** Offence
- a penalty of a fine at \$50,000 and imprisonment for 2 years.

Repeated non-compliance with enforcement notice

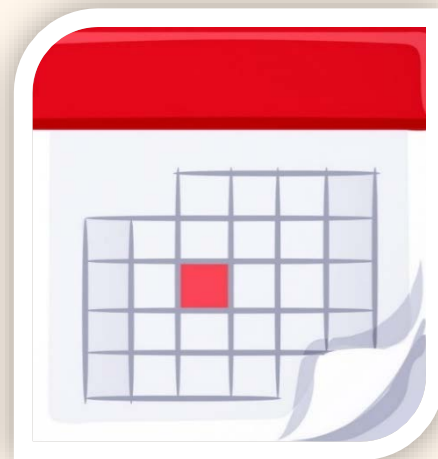
- a penalty of a fine at \$100,000 and imprisonment for 2 years
- in case of a continuing offence, a daily fine of \$2,000

Same infringement of the second time

- a penalty of a fine at \$50,000 and imprisonment for 2 years
- in case of a continuing offence, a daily fine of \$1,000

Commencement date of the Amendment Ordinance

The Amendment Ordinance was published in the gazette and came into effect on **8 October 2021**.

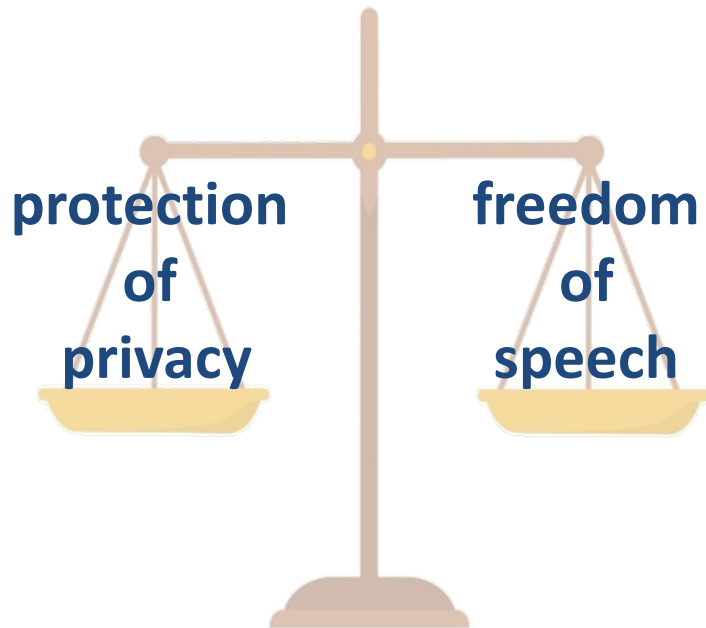


The Personal Data (Privacy) (Amendment) Ordinance 2021

Major aspects of the amendments

- Criminalising doxxing acts
- Empowering the Privacy Commissioner to carry out criminal investigation and institute prosecution
- Conferring statutory powers on the Privacy Commissioner to direct the removal of a doxxing message

A balance between



A two-tier structure of the doxxing offence



	Prosecution means	Threshold for conviction	Maximum penalty
First Tier	Summary offence	<ul style="list-style-type: none">• Disclosing personal data without the data subject's consent; and• With intent to cause specified harm or being reckless as to whether specified harm would be caused	<p>Fine of \$100,000</p> <p>Imprisonment for 2 years</p>
Second Tier	Indictable offence	<ul style="list-style-type: none">• Disclosing personal data without the data subject's consent;• With intent to cause specified harm or being reckless as to whether specified harm would be caused; and• Specified harm has been caused to the data subject or his or her family member	<p>Fine of \$1,000,000</p> <p>Imprisonment for 5 years</p>

Compensation

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



53

Publications

- Report on “Privacy Concerns on Electronic Food Ordering at Restaurants”
- General Reference Guide-Privacy Management Programme (PMP) Manual
- Guidance Note on Data Security Measures for Information and Communications Technology
- Report on "Comparison of Privacy Settings of Social Media")
- Guidance on CCTV Surveillance and Use of Drones
- Guidance on Direct Marketing
- Guidance on Collection and Use of Biometric Data



Guidance on Direct Marketing

PART 1: Introduction

Purpose of guidance

1.1 Direct marketing is a common business practice in Hong Kong. It often involves collection and use of personal data by an organization for direct marketing itself and in some cases, the provision of such data by the organization to another person for use in direct marketing. In the process, compliance with the requirements under the Personal Data (Privacy) Ordinance (the "Ordinance") is essential. This document is issued by the Privacy Commissioner for Personal Data (the "Commissioner") to provide practical guidance on data users' compliance with the new regulatory requirements for direct marketing under the new Part VIA of the Ordinance. It helps data users to fully understand their obligations as well as to promote good practice. Data users should also make reference to other laws, regulations, guidelines and codes of practice that are relevant for direct marketing purposes, insofar as they are not inconsistent with the requirements under the Ordinance.

1.2 This Guidance shall take effect on the

takes effect, the Commissioner's "Guidance on the Collection and Use of Personal Data in Direct Marketing" remains fully valid.

What is "direct marketing"?

1.3 The Ordinance does not regulate all types of direct marketing activities. It defines "direct marketing" as:

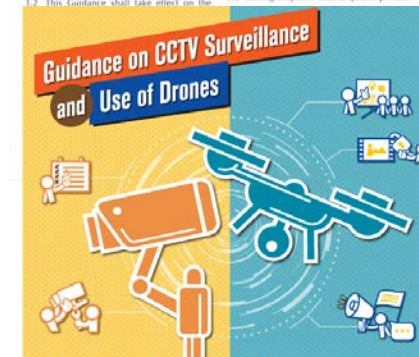
(a) the offering or advertising of the availability of goods, facilities or services; or

(b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means.

"Direct marketing means" is further defined to mean:

(a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or

(b) making telephone calls to specific persons.



《人工智能 (AI)：個人資料保障模範框架》

Artificial Intelligence: Model Personal Data Protection Framework



《僱員使用生成式AI的指引清單》

Checklist on Guidelines for the Use of Generative AI by Employees

Thematic webpages



Case notes

Compliance & Enforcement

Court Judgment

Administrative Appeals Board's Decisions

Case Notes

Data Breach Notification

Submissions on Privacy Issues

Consultations

Case Notes

Administrative Appeals Board's Decisions Case Notes

Complaint Case Notes

Enquiry Case Notes

Case Notes for Compliance Action

You Are Looking For			--Year--	--Category--	--By Provisions/DPPs/COPs--	Go
--By Topic/Subject Matter--			Please Enter Keyword			
Case No.:2024C03 New! An online store sent invoices containing personal data to customers via unencrypted weblinks. <more>	Case No.:2024C02 New! Mobile Wi-Fi device rental company took inadequate security measures to protect customers' personal data. <more>	Case No.:2024C01 New! Collection of copies of Hong Kong Identity Card and bank card from a job applicant by an employer prior to the acceptance of employment offer. <more>				
Areas of Concern:DPP4	Areas of Concern:DPP4	Areas of Concern:DPP1, Human Resources, Identity Card				
Case No.:2023DB03 New! A folder that contained personal data of students and parents was accidentally disposed of – DPP 4 – security of personal data. <more>	Case No.:2023DB02 New! A staff member of a sports organisation accidentally uploaded and transmitted the personal data of event participants – DPP 4 – security of perso. <more>	Case No.:2023DB01 New! An educational institution's improper password management led to unauthorised access to the personal data of students and parents – DPP 4 – secur. <more>				
Areas of Concern:DPP4	Areas of Concern:DPP4	Areas of Concern:DPP4				

Resources centre

Resources Centre

Publications

Annual Reports
e-Newsletters
Guidance Notes/Reports
Books
Leaflets
Posters & Infographics
Forms
Surveys/ Study Reports
"Mainland Corner" Column

Multimedia

Resources by Topics

Annual Reports

You Are Looking For			--Year--	Go
2022-2023 	2021-2022 	2020-2021 		
2019-2020 	2018-2019 	2017-2018 		

PCPD



H K



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

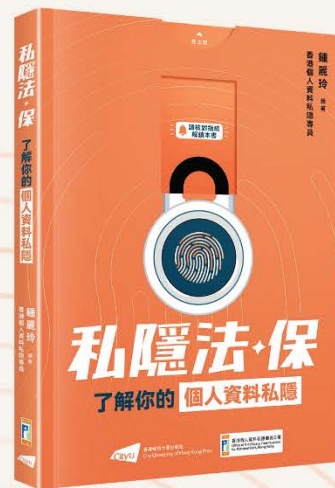
“The Treasure-trove of Privacy – Understanding Your Personal Data Privacy”



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





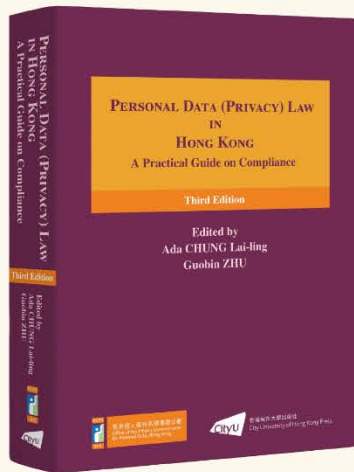
Ms Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data,
Hong Kong



Professor ZHU Guobin
Professor ZHU Guobin
City University of Hong Kong

PERSONAL DATA (PRIVACY) LAW IN HONG KONG

A Practical Guide on Compliance (Third Edition)



Highlights:

- Provisions of the PDPO on combatting doxxing
- Cross-border transfers of personal data from Hong Kong
- The Mainland's personal information protection regime
- Recent decisions by the Administrative Appeals Board and the Court
- PCPD's investigation reports and materials
- Comparison table on the personal data protection laws of Hong Kong, the Mainland and the European Union

Buy Now



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



Contact Us



2827 2827



2877 7026



www.pcpd.org.hk



communications@pcpd.org.hk



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

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

Follow
Us



Disclaimer

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



PCPD



H K



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