

Introduction to the Personal Data (Privacy) 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



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. PDPO Overview

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>

3

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)

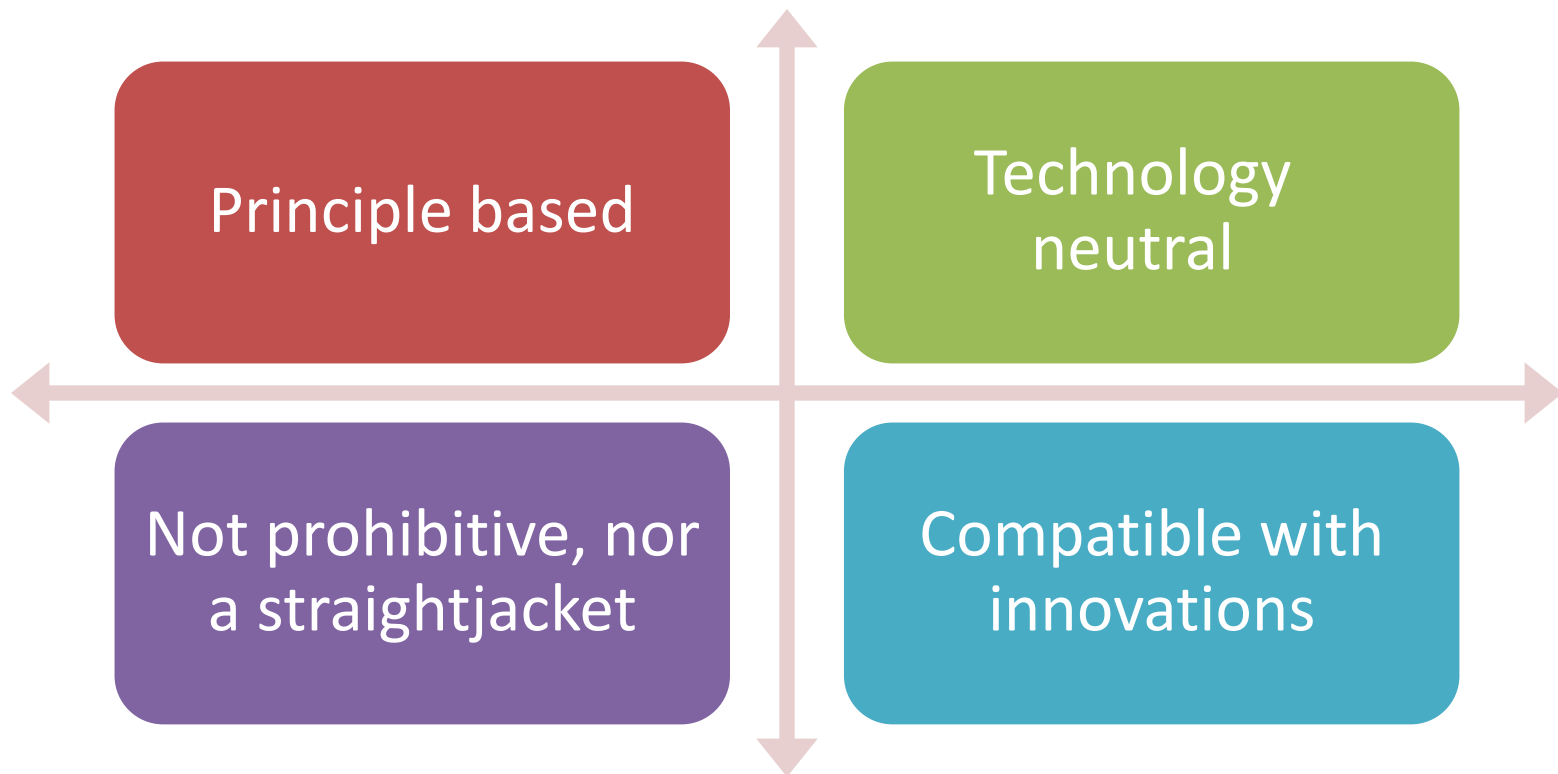
Covers both public (government) and private sectors

The Data Protection Principles outline how data users should collect, handle and use personal data

Complemented by other provisions imposing further compliance requirements

7

Characteristics of the PDPO



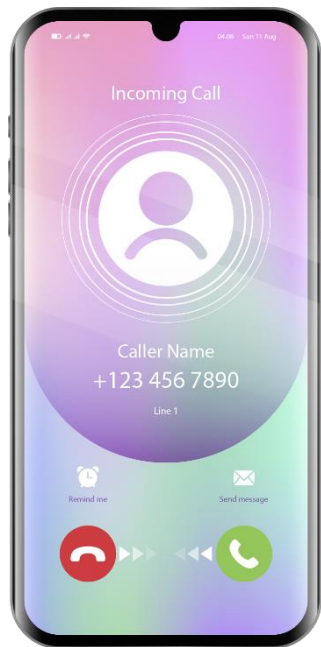
What is “Personal Data”?

(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

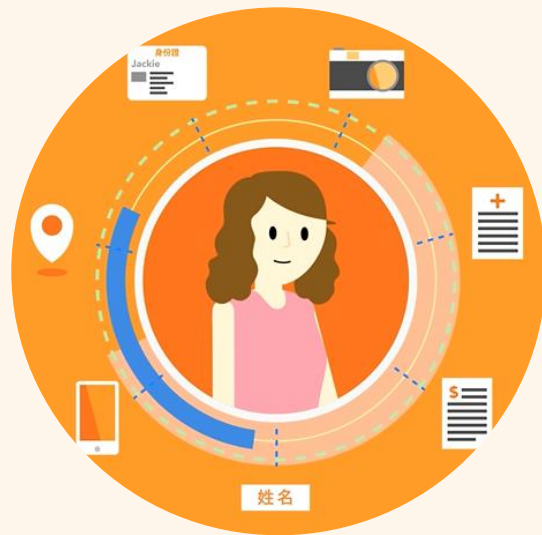
(c) in a form in which “access to” or “processing of” the data is practicable

Examples of Personal Data



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



11

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



12

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



13



2. Six Data Protection Principles

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達明的目的或直接相關的用途，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.

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**.

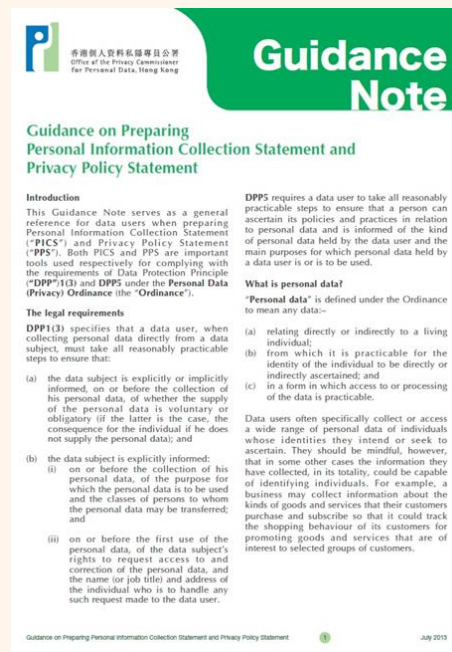


16

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**



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



18

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



20

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



Data Breach – Common Categories



Cyber attack or hacking



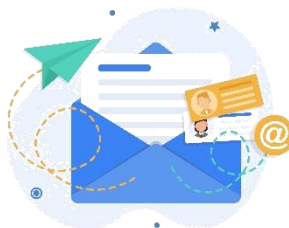
**Misconfiguration
of systems**



**Loss of documents or
portable devices**



**Improper/wrongful
disposal of personal data**



Errors with posts or emails



Staff misconduct

23

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.



24

Data Breach Notification

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



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



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:

Browse...

Add 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 > A 1

Clear all fields

Submit



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

資料外洩事故通報專員

資料外洩事故通報表格

通知

資料使用者(或組織)向香港個人資料私隱專員(下稱「專員」)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(或組織)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):

電話號碼: 傳真號碼:

電郵地址:

(*請無法不虛傳真)

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

損害評估 (是處註*)
事件是否造成實際風險, 對個人資料造成風險? (請在以下「是」或「否」) 是 ☐ 否 ☐
請解釋為何有/沒有實際的損害風險

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) 如何協助他們的安全, 協助或減輕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)

25



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

Governance and Organisational Measures

A data user should establish **clear internal policy** and **procedures** on data governance and data security, covering:



NOTE

A data user should **review** and **revise** its policies and procedures on **data governance and data security periodically** and in a **timely manner** based on prevailing circumstances, such as new industry standards and new threats to data security.



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

Enhance training on Data Security

Sufficient training should be provided for staff members at induction and regularly



Technical and Operational Security Measures



Securing Computer Networks



Database Management



Access Control



Firewalls and Anti-malware



Protecting Online Applications



Encryption



Emails and File Transfers



Backup, Destruction and Anonymisation

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
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



30

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

[illegible]

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”?

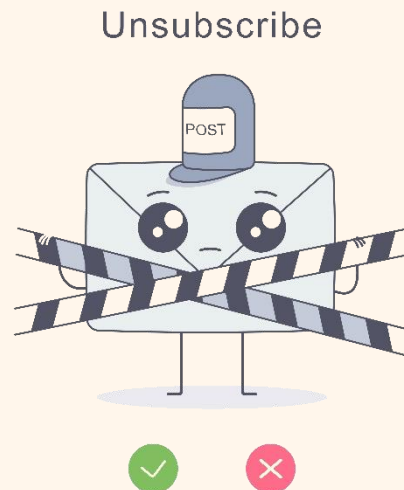
- a. the offering, or advertising of the availability, of goods, facilities/ services; or
- b. the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political/ other purposes,

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 

36

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**

38

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



39

Guidance to Help Data Users

- **Guidance on Direct Marketing:** 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.





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

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 VI A of the Ordinance¹. 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 same date as the date of commencement of Part VI A of the Ordinance (the "commencement date"). It will supersede and replace the Commissioner's "Guidance on the Collection and Use of Personal Data in Direct Marketing" issued in November 2012. For the avoidance of doubt, until Part VI A of the Ordinance
¹ The new Part VI A under the Ordinance was introduced by the Personal Data (Privacy) (Amendment) Ordinance 2012. It will take effect on 1 April 2013.
² Please refer to the Unsolicited Electronic Messages Ordinance (Cap. 593, Laws of Hong Kong) enforced by the Office of the Communications Authority.
Guidance on Direct Marketing 1 April 2013



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

直接促銷指引
第1部：導言
指引目的
1.1 直接促銷在香港是常見的商業活動，一般是將機構收集及使用市民的個人資料以向資料當事人促銷產品或服務。某些機構會將收集所得的個人資料交給他人作直接促銷之用。在上述直接活動中的資料使用者必須遵從《個人資料(私隱)條例》(下稱「條例」)的規定。個人資料私隱專員(下稱「專員」)發出本指引，向資料使用者提供實務性指引，以闡釋條例下新增的第VI A部有關直接促銷的條文¹，並協助資料使用者全面瞭解其責任和推廣良好行方式。資料使用者亦應參考其他不抵觸條例規定而賦予直接促銷的例、規則、指引及實務守則。
1.2 本指引將於條例第VI A部實施日期起即日生效(下稱「生效日期」)，並取替專員於2012年11月發出的《收集及使用個人資料作直接促銷指引》。為免生疑，在條例第VI A部生效前，專員的《收集及使用個人資料作直接促銷指引》繼續有效。
甚麼是「直接促銷」?
1.3 條例並非規管所有類型的直接促銷活動。根據條例「**直接促銷**」指透過**直接促銷方法**：
(a) 要約提供產品、服務或服務，或為該等產品、服務或服務可予提供而進行廣告宣傳；或
(b) 1.4 Hence, "direct marketing" under the Ordinance does not include unsolicited business electronic messages sent to telephones, fax machines or email addresses without addressing to specific persons by name and person-to-person calls being made to phone numbers randomly generated.
例子：
✓ 發送至具名人士的流動電話號碼的促銷短訊屬直接促銷。
✓ 電話提供服務或以電話聯絡現有客戶要約提供升級服務屬直接促銷。
✗ 直銷郵件送交某地址或某地址的「住戶」不屬於直接促銷，因為不是向指名特定人士提交。
✗ 連鎖與專門向有潛質的顧客推銷其產品不屬於直接促銷。
✗ 客戶服務經理向客戶電話介紹產品/服務並不屬於直接促銷(但是其後使用該客戶的個人資料向他寄發推廣資料，則屬直接促銷)。
✗ 向指明人士的電話號碼發出的促銷電話不屬於直接促銷。
¹ 條例下的第VI A部是2012年個人資料(私隱)(修訂)條例其中新加入的部分。該修訂於2013年4月1日生效。
² 第35A(1)條。
³ 請參考通訊事務管理局執行《Unsolicited Electronic Messages Ordinance》(香港法律第593號)。
直接促銷指引 1 2023年4月



4. Offences and Compensation

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



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

Offence for Disclosing Personal Data Without Consent

Section 64(1)

- A **person** commits an offence if he discloses any personal data of a data subject obtained from a data user **without the data user's consent** with the intention to:
 - 1) obtain **gain** in the form of money or other property, whether for his own benefit of or that of another person; or
 - 2) cause **loss** in the form of money or other property to the data subject
- *Example:* **Sale of customers' personal data** by an employee without the company's consent



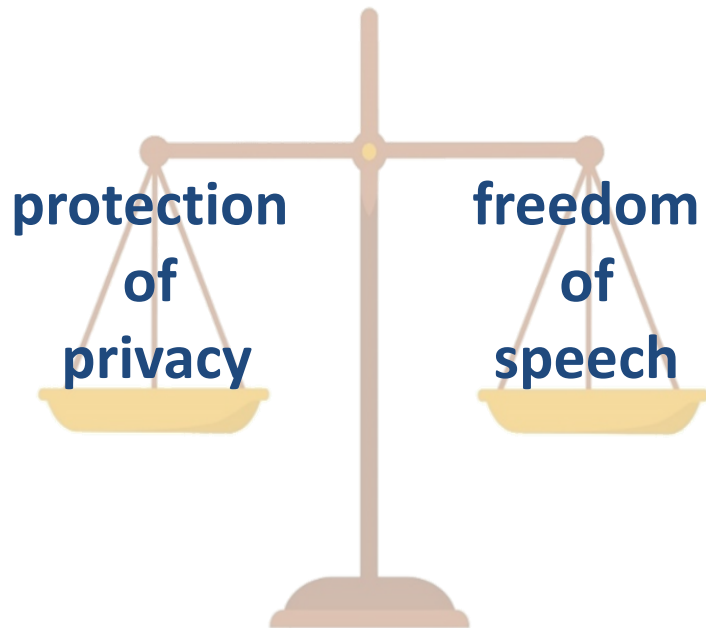
The maximum penalty: a **fine of \$1,000,000** and imprisonment for **5 years**

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



44

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



46

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.

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:

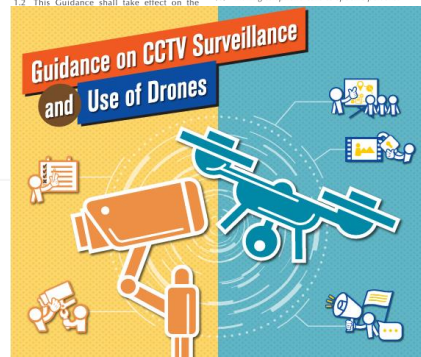
(a) the offering, or advertising of the availability, of goods, facilities or services; or

(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:

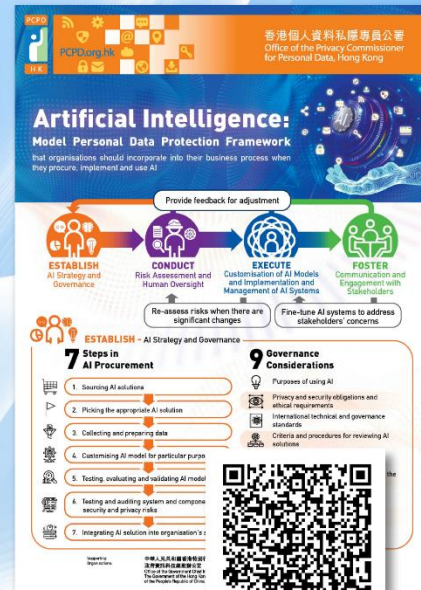
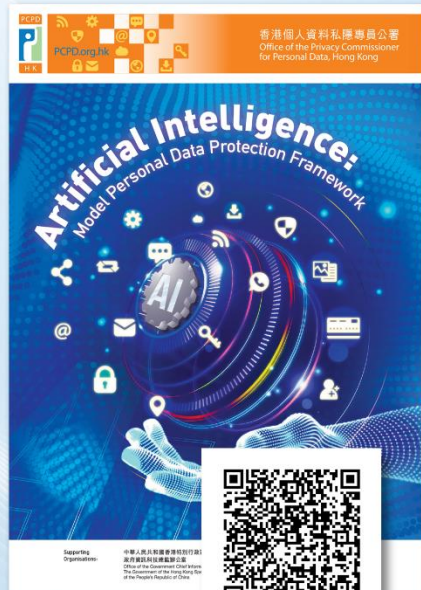
- (a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or
- (b) making telephone calls to specific persons.

1.2 This Guidance shall take effect on the



《人工智能 (AI)：個人資料保障模範框架》

Artificial Intelligence: Model Personal Data Protection Framework



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> Areas of Concern:DPP4	Case No.:2024C02 New! Mobile Wi-Fi device rental company took inadequate security measures to protect customers' personal data. <more> Areas of Concern:DPP4	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: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> Areas of Concern:DPP4	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> Areas of Concern:DPP4	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			

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
2023-2024	2022-2023	2021-2022	
			

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





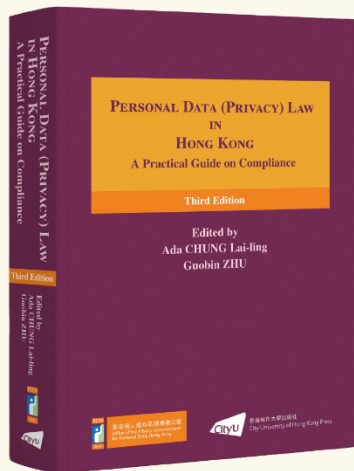
Ms Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data,
Hong Kong



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