

Introduction to the Personal Data (Privacy) Ordinance

Anti-Money Laundering Seminar for
Money Service Operators

9 December 2025



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

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

1

What is “Personal Data”?

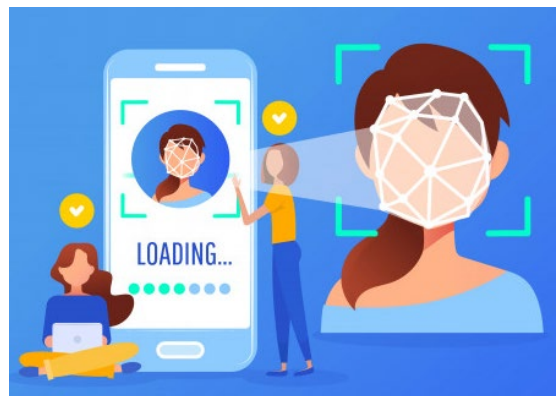
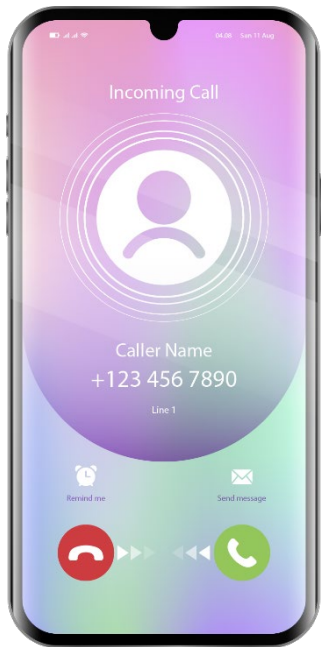


(a) relating directly or indirectly to a living individual

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

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

Examples of Personal Data



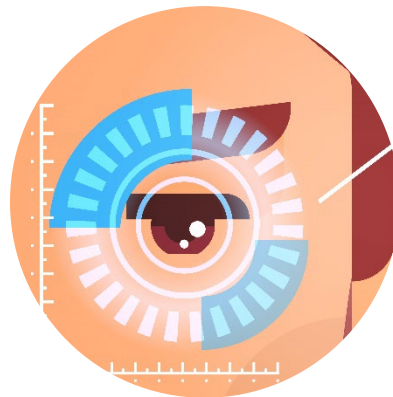
Applications of Biometric Data



Use of fingerprints
for transaction
authorisation



Use of facial
recognition to unlock
smartphones



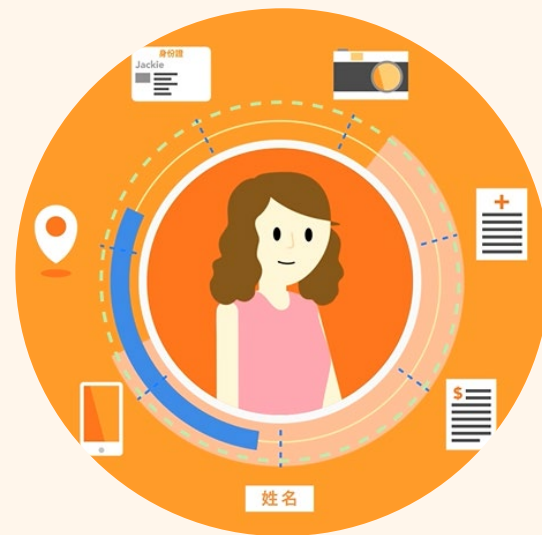
Use of retina
recognition system
for entry
monitoring



Use of voiceprints
for identity
verification in
telephone banking

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



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



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

PCPD.org.hk

Data Protection Principles

1

收集目的及方式 Collection Purpose Et 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，而不超乎程度。

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 Et Retention



資料使用者須確保持有的個人資料準確相關，資料的保留時間不應超過達成原來目的之實際所需。

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 Et 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.

Under the Personal Data (Privacy) Ordinance

Six Data Protection Principles



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

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

PCPD.org.hk

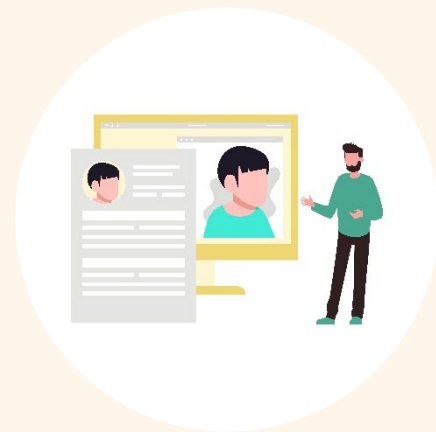
DPP1: Collection Purpose & Means

- 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**.



Case Sharing: Excessive Collection of Personal Data

- A financial institution **collected excessive personal data** from outsourced staff without providing personal information collection statement and **retained personal data for a period longer than necessary**
- The complainant was not employed by the financial institution but was required to provide his personal data including date of birth to the institution, and the complainant noticed that his personal data **would be retained for seven years from the date of termination** of his relationship with the financial institution.



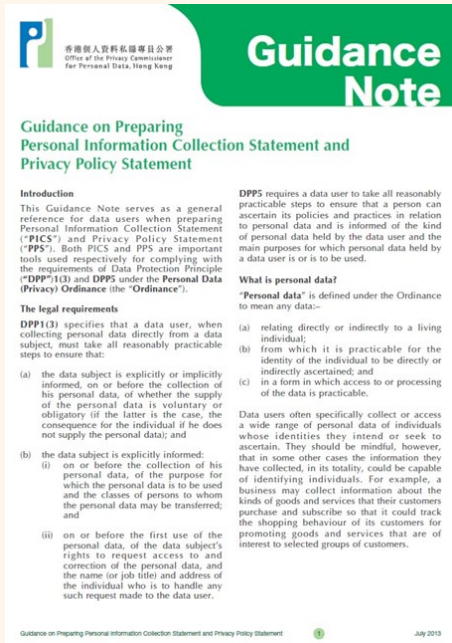
Case Sharing: Excessive Collection of Personal Data

- When employing staff through sub-contracting (including through third parties), organisations should pay particular attention to the handling of personal data.
- **As these organisations do not have a direct employment contract with the individual concerned, in general, they would collect less personal data from those subcontract staff than from its own staff.**
- If the data is collected directly from those **subcontract staff**, these **organisations should provide a PICS** to those staff.
- In addition, these organisations can only continue to retain the personal data of subcontract staff for the purposes for which the data was collected; or where there is a reasonable likelihood that such staff may be re-engaged for subsequent work.

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**



13

DPP2: Accuracy & Retention

Data users should take all practicable steps to ensure:

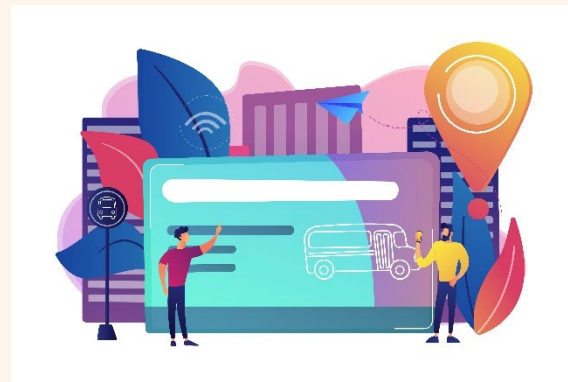
- the accuracy of the personal data
- the personal data is not kept longer than is necessary for the fulfilment of the purpose for which the data is used

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



Case Sharing: Data Accuracy

- The complainant visited a branch of the Bank and applied for a **change of his office address** in the bank records with the assistance of a staff member.
- The Bank had mistaken his application as **a change of his correspondence address**, resulting in the complainant receiving correspondence from the Bank at his office address.
- The Bank stated that the Staff **did not notice that “the type of address to be changed” had not been filled in** on the form.
- The Staff **inadvertently** checked the box for “Residential and Correspondence”, leading to the occurrence of the incident in this case.



Case Sharing: Data Retention

- A telecommunications company's inactive database had been intruded which caused leakage of personal data of about 380,000 customers and service applicants.
- The database should have been deleted after a system migration but was nevertheless retained and remained connected to internal network.
- The company **failed to give due consideration to the retention period of former customers' personal data** or provide relevant internal guidance.
- After the incident had come to light, the company decided **to shorten the retention period of personal data of former customers** whose accounts had been closed and cleared **from three years to six months**.



DPP3: Use of Personal Data

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

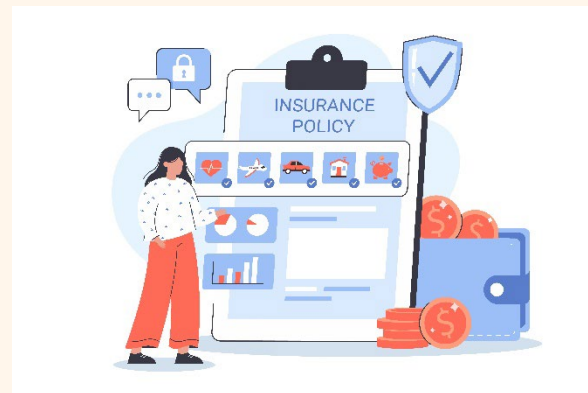
New purpose

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



Case Sharing: Use of Personal Data

- The Complainant was a policyholder of an insurance company (“the Company”) and had instructed the Company to **discharge Agent A as her insurance agent**.
- However, the Complainant **continued to receive promotional materials from Agent A** under the Company’s name.
- The Company explained that **it was its practice to allow former insurance agents** (who had first signed the customer up with the Company) and their supervisors **to access customers’ policy-related personal data from the Company’s customer database** in order to follow-up with policy-related matters.



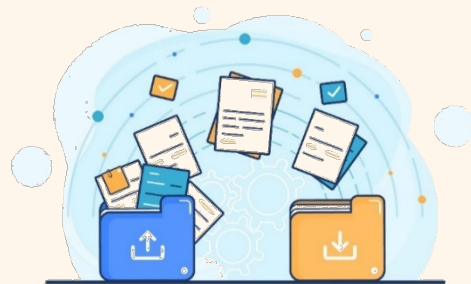
Case Sharing: Use of Personal Data

- The Commissioner held that **it was reasonably practicable** for the Company to arrange disclosure of relevant policy-related data only when such needs arise, and that the Company's granting of **indiscriminative access rights** to policy related data to insurance agents and their supervisors of former customers under the circumstances of the case **had violated DPP3**.
- The Company accepted the Commissioner's recommendations:
 - Review its access-rights mechanism;
 - Remove the access right of former insurance agents and their supervisors; and
 - Allow only current insurance agents and their supervisors to access and use the personal data of their policyholder customers.

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



20

Case Sharing: Cyberattack

- A company reported that its computer systems and file servers had been attacked by ransomware and maliciously encrypted. A hacker group had demanded a ransom payment from the company to unlock the encrypted files. The Incident resulted in the leakage of the personal data of **more than 13,000 data subjects, about 40% of whom were unsuccessful job applicants and former employees.**

The Incident was caused by the following deficiencies:

1. Lack of effective detection measures in its information systems
2. Failure to enable multi-factor authentication for remote access to data
3. Insufficient security audits of the information systems
4. Lack of specificity in the information security policy
5. Unnecessary retention of personal data



21

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.



Data Breach Notification

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

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

Keyword Search

Home > Compliance & Enforcement > Data Breach Notification

RSS A A A 繁 簡

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 > A 1

致：香港個人資料私隱專員

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

資料外洩事故通報表格

通知

資料使用者(「**數據使用者**」)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，並非法律規定，但在決定是否向專員作出通報時，專員專員編出的《資料外洩事故處理及通報指引》，在大多數情況下，通知受事故影響的資料當事人(「**數據受影響人士**」)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：_____

如由轉機件出通報，請提供下列資料：

聯絡人：_____

姓名 (*先生/女士/小姐)：_____

與通報有關的關保(例如：聯繫)：_____

電話號碼：_____ 傳真號碼：_____

電郵地址：_____

(*請填寫下列資料)

資料外洩事故詳情 (「**數據受影響**」)

已採取 / 將會採取的管性外洩事故的行動 (「**數據受影響**」)
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

損害風險 (「**數據受影響**」)

事件是否真實風險，對資料當事人構成威脅？ (請在其中一方格加上「√」號) 是 否
請解釋為何有 / 沒有實質的損害風險

向資料人士提供的協助及建議

請詳述 (a) 如何通知受事故影響的資料人士；及 (b) 如何他們的受安全、隱私或數據外洩事故受影響，你做了甚麼或可以採取甚麼以協助他們受安全、隱私或數據外洩事故

通報其他機構 / 規管機構 / 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)

PCPD 香港個人資料私隱專員公署
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

PCPD



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

H K



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

Data Access Request Form

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.

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

- 請在填寫本表格前，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》(以下稱「本條例」)的有關規定和例案，該例案只供參考之用，屬於非法律評語及明確內容，請參閱本條例的條文。
- 本表格是個人資料私隱專員(稱「專員」)根據本條例第 47(2)條所印用的，其生效日期為 2012 年 10 月 1 日。如你不採用本表格來提交查閱資料要求(以下稱「你的要求」)，資料使用者可拒絕按你的要求(見本條例第 203(6)(b)條)。
- 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，資料使用者可拒絕按你的要求(見本條例第 203(6)(b)條)。
- 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。
- 你授權查閱不屬於你的個人資料或不屬於個人資料的資料(見本條例第 1(1)(3)條)，資料使用者只須向你提供你的個人資料的副本，而不需將你的個人資料的文件的副本。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有關你的個人資料的錄音副本。
- 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，如你未與資料使用者提供他/她為你的要求查閱的個人資料符合規定的資訊，資料使用者可拒絕按你的要求(見本條例第 203(6)(b)條)。如你為使資料使用者按你的要求而在本表格內提供虛假或有誤導性的資訊，可構成違反本條例第 18(5)條。
- 請勿把本表格遞交專員，填寫表格應直接遞交資料使用者，以作出你的要求。
- 資料使用者若要求你提供身分證、個別或准身分證，及向你收取從查閱資料要求收費(見本條例第 203(1A) 及 203(2)(b)條)。
- 資料使用者在本條例第 20 條指定的情況下可拒絕按你的要求。

第 I 部：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)： _____

姓： _____ (姓)
地址： _____

第 II 部：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，先填姓)： _____
個人身分代號，供知香港身分證號碼，請提供或以以往資料使用者編號的其他身分證號碼(如軍、例如軍士編號、職員編號、病人編號、客戶號碼、會員號碼或其他參考編號)： _____
通訊地址： _____
日間聯絡電話號碼： _____
電郵地址(如有)： _____

如你屬查閱資料要求的資料當事人提出，請填寫本節

第 III 部：查閱資料要求者
查閱資料要求的資料及身分*

中文姓名： _____
英文姓名(正印全名，先填姓)： _____
通訊地址： _____
日間聯絡電話號碼： _____
電郵地址(如有)： _____

此項查閱資料要求是本人(以下簡稱為「有關人士」)的身份，代表資料當事人作出的：

資料當事人尚未成年，本人對資料當事人有作為父母的責任；

資料當事人無力處理其本身事務，本人是法定委任以處理該等事務；

資料當事人屬《精神健康條例》(第 136 章)下的精神病人的法定代理人(如為能力、智、或) 本人根據條例第 44A、590 或 590 條獲委任擔任他的監護人，或執行他/她的監護人的職責；

本人屬資料當事人屬因提供代表他/她提出此項查閱資料要求。

請將填妥表格寄往：「I」節

* 請填上所有與提出查閱資料要求的資料有關的姓名或名稱。
 1. 查閱資料的資料應與資料當事人的姓名或名稱、地址、電話號碼、傳呼號碼或流動電話號碼或傳呼號碼有關。
 2. 查閱資料的資料應與資料當事人的身分有關。
 3. 查閱資料的資料應與資料當事人的身分有關，如你為資料當事人的代理人，則應填上資料當事人的姓名、地址、電話號碼、傳呼號碼或流動電話號碼或傳呼號碼。
 4. 資料當事人的姓名、地址、電話號碼、傳呼號碼或流動電話號碼或傳呼號碼，應與資料當事人的身分有關。



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

Criminal Offence - Section 64(1)

- Under Section 64 (1) of the PD(P)O, a person commits an offence if he discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent –
 - a) to obtain gain in money or other property, whether for the benefit of the person or another person; or
 - b) to cause loss in money or other property to the data subject

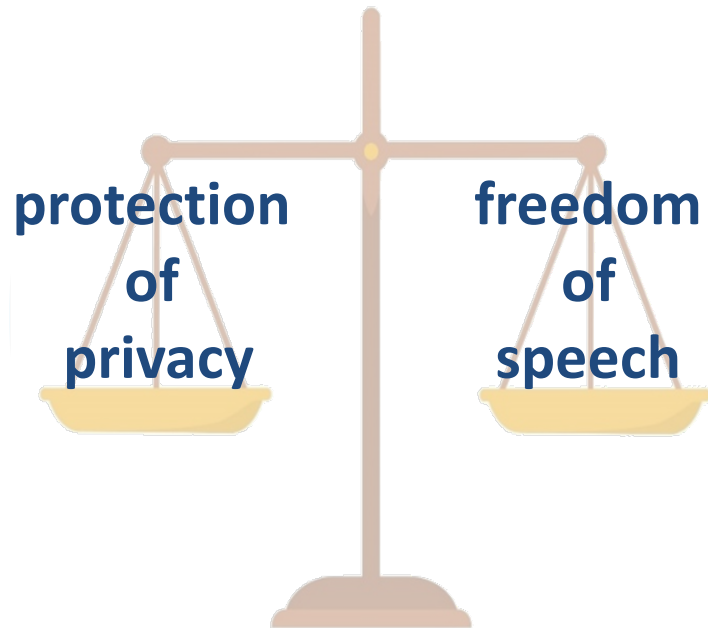
Maximum fine of \$1,000,000 and 5 years' imprisonment

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



29

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>

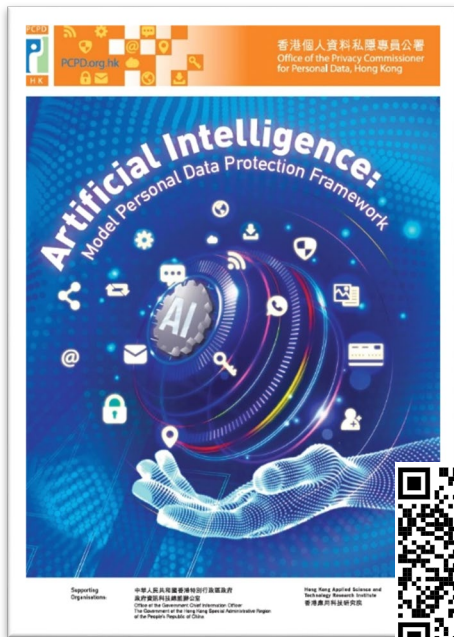


“Specified Harm” consists of four limbs

- Harassment, molestation, pestering, threat or intimidation to the person;
- Bodily harm or psychological harm to the person;
- Harm causing the person reasonably to be concerned for the person's safety or well-being; or
- Damage to the property of the person.



Artificial Intelligence: Model Personal Data Protection Framework

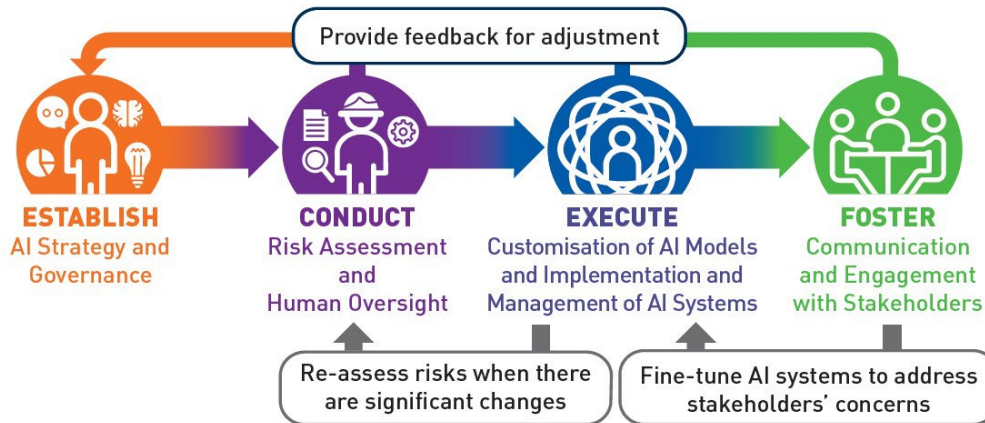


A set of recommendations on the best practices regarding governance of AI for the protection of personal data privacy for organisations procuring, implementing and using any type of AI systems, including generative AI

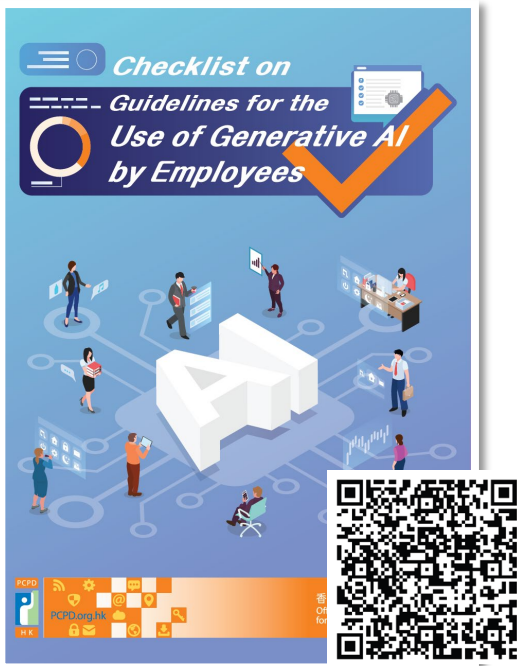


Assist organisations in complying with the requirements of the PDPO

The Model Framework



Checklist on Guidelines for the Use of Generative AI by Employees



Help organisations develop internal policies or guidelines for employees' use of GenAI at work while complying with the requirements of the PDPO



Scope



Protection of Personal Data Privacy



Lawful and Ethical Use and Prevention of Bias



Data Security



Violations of the policies or guidelines

Publications

- 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**")
- Report on "**Privacy Concerns on Electronic Food Ordering at Restaurants**"
- **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 VI A 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



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

<p>Case No.:2024C03 New!</p> <p>An online store sent invoices containing personal data to customers via unencrypted weblinks... <more></p> <p>Areas of Concern:DPP4</p>	<p>Case No.:2024C02 New!</p> <p>Mobile Wi-Fi device rental company took inadequate security measures to protect customers' personal data... <more></p> <p>Areas of Concern:DPP4</p>	<p>Case No.:2024C01 New!</p> <p>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></p> <p>Areas of Concern:DPP1, Human Resources, Identity Card</p>
<p>Case No.:2023DB03 New!</p> <p>A folder that contained personal data of students and parents was accidentally disposed of – DPP 4 – security of personal data... <more></p> <p>Areas of Concern:DPP4</p>	<p>Case No.:2023DB02 New!</p> <p>A staff member of a sports organisation accidentally uploaded and transmitted the personal data of event participants – DPP 4 – security of perso... <more></p> <p>Areas of Concern:DPP4</p>	<p>Case No.:2023DB01 New!</p> <p>An educational institution's improper password management led to unauthorised access to the personal data of students and parents – DPP 4 – secur... <more></p> <p>Areas of Concern:DPP4</p>

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

<p>2023-2024</p> 	<p>2022-2023</p> 	<p>2021-2022</p> 
<p>2020-2021</p> 	<p>2019-2020</p> 	<p>2018-2019</p> 

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

Thematic webpages



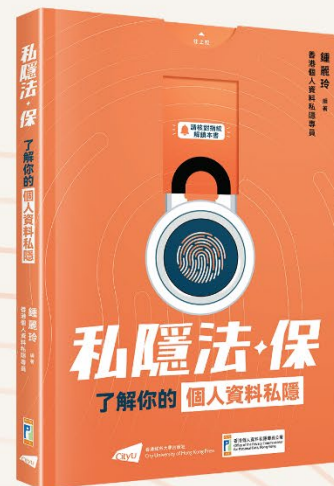
“The Treasure-trove of Privacy – Understanding Your Personal Data Privacy”



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





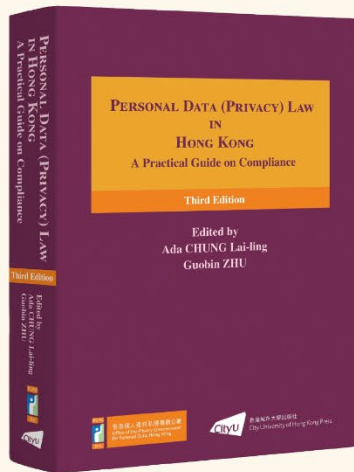
Ms Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data,
Hong Kong



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



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.