Introduction to the Personal Data (Privacy) Ordinance

Anti-Money Laundering Seminar for Money Service Operators

9 December 2025

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

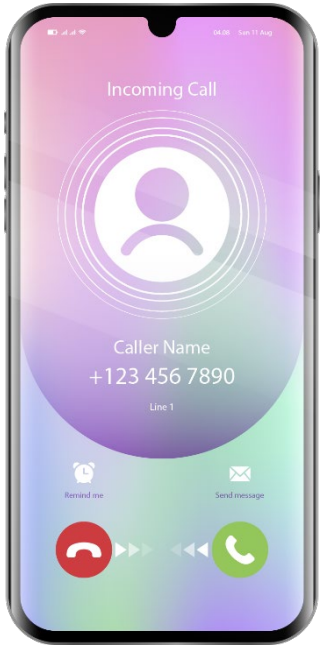
What is “Personal Data”?

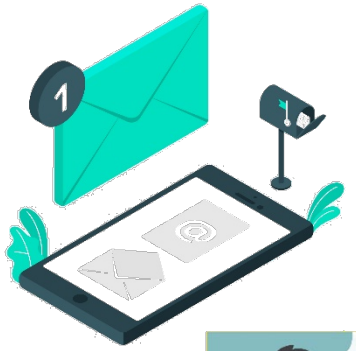
(a) relating directly or indirectly to a living individual

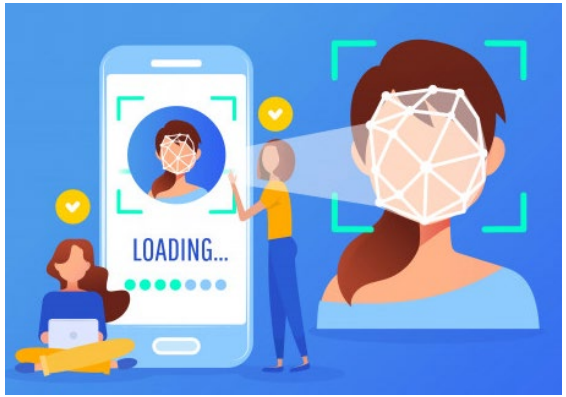
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

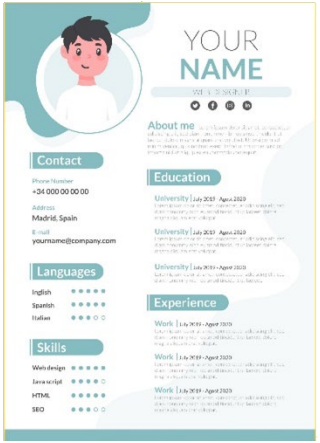
(c) in a form in which “access to” or “processing of” the data is practicable

Examples of Personal Data



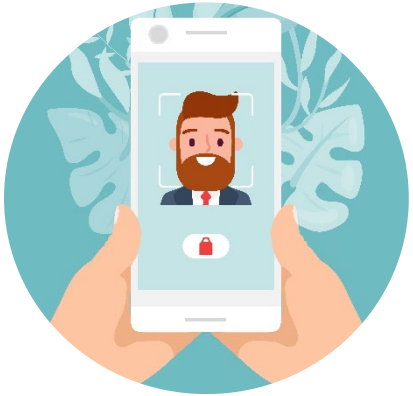




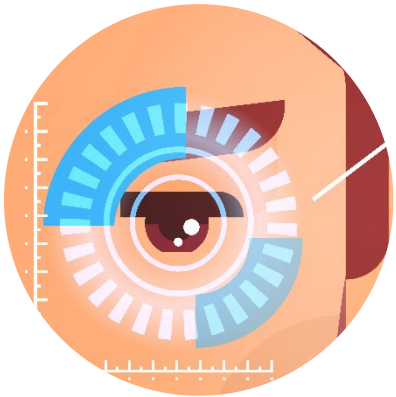


Applications of Biometric Data

Use of fingerprints for transaction authorisation



Use of facial recognition to unlock smartphones



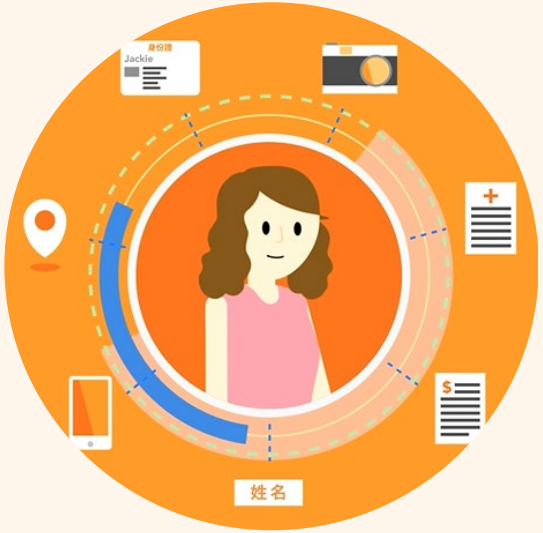
Use of retina recognition system for entry monitoring

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

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

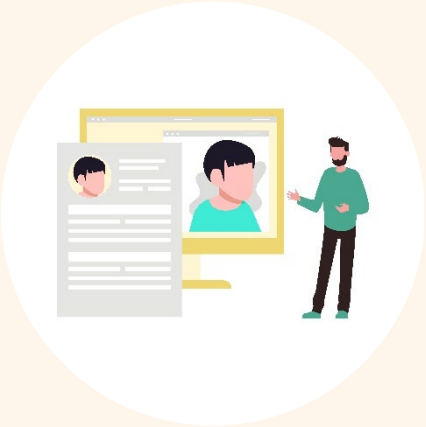
PCPD.org.hk

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

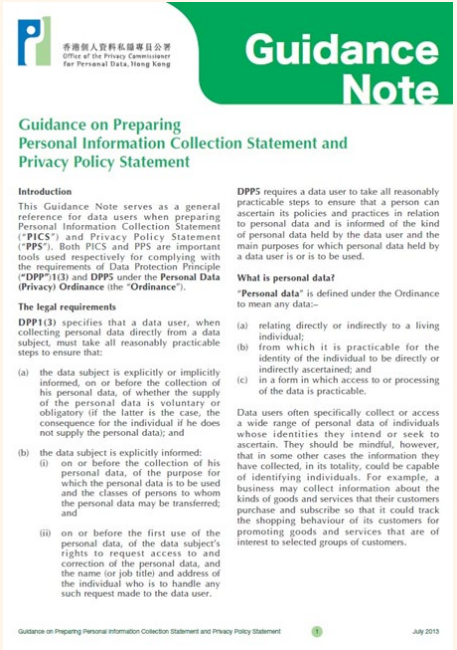
- When employing staff through sub-contracting (including through third parties), organisations should pay particular attention to the handling of personal data.
- **As these organisations do not have a direct employment contract with the individual concerned, in general, they would collect less personal 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**



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

Guidance Note

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement

Introduction

This Guidance Note serves as a general reference for data users when preparing Personal Information Collection Statement ("**PICS**") and Privacy Policy Statement ("**PPS**"). Both PICS and PPS are important tools used respectively for complying with the requirements of Data Protection Principle ("**DPP**")1(3) and **DPP5** under the **Personal Data (Privacy) Ordinance** (the "**Ordinance**").

The legal requirements

DPP1(3) specifies that a data user, when collecting personal data directly from a data subject, must take all reasonably practicable steps to ensure that:

(a) the data subject is explicitly or implicitly informed, on or before the collection of his personal data, of whether the supply of the personal data is voluntary or obligatory (if the latter is the case, the consequence for the individual if he does not supply the personal data); and

(b) the data subject is explicitly informed:
(i) on or before the collection of his personal data, of the purpose for which the personal data is to be used and the classes of persons to whom the personal data may be transferred; and
(ii) on or before the first use of the personal data, of the data subject's rights to request access to and correction of the personal data, and the name (or job title) and address of the individual who is to handle any such request made to the data user.

DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can ascertain its policies and practices in relation to personal data and is informed of the kind of personal data held by the data user and the main purposes for which personal data held by a data user is or is to be used.

What is personal data?

"**Personal data**" is defined under the Ordinance to mean any 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.

Data users often specifically collect or access a wide range of personal data of individuals whose identities they intend or seek to ascertain. They should be mindful, however, that in some other cases the information they have collected, in its totality, could be capable of identifying individuals. For example, a business may collect information about the kinds of goods and services that their customers purchase and subscribe so that it could track the shopping behaviour of its customers for promoting goods and services that are of interest to selected groups of customers.

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement 1 July 2013

DPP2: Accuracy & Retention

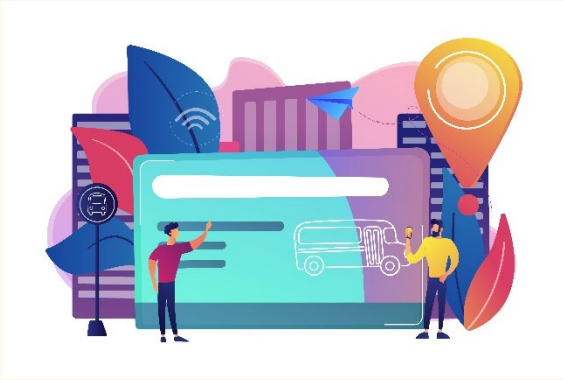
Data users should take all practicable steps to ensure:

- 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.

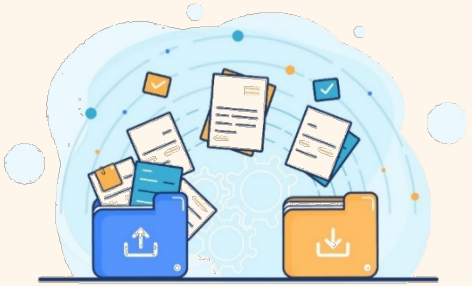
Case Sharing: Use of Personal Data

- 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



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.**

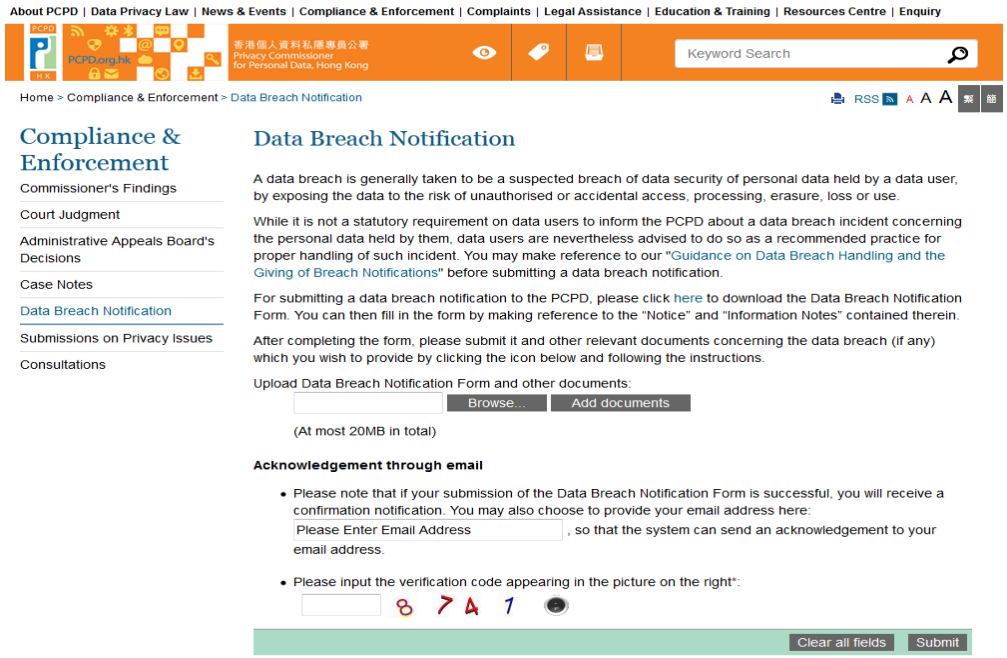
The Incident was caused by the following deficiencies:

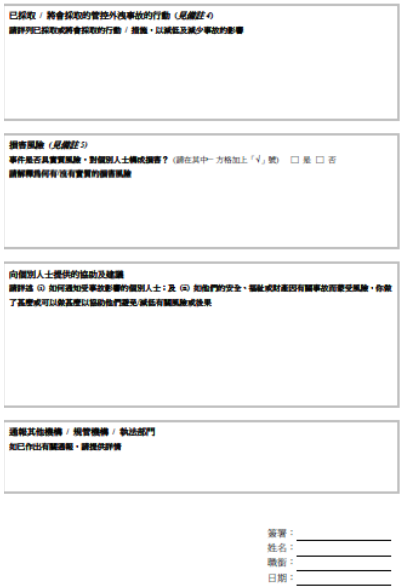
1. Lack of effective detection measures in its information systems
2. Failure to enable multi-factor authentication for remote access to data
3. Insufficient security audits of the information systems
4. Lack of specificity in the information security policy
5. Unnecessary retention of personal data

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





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

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

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

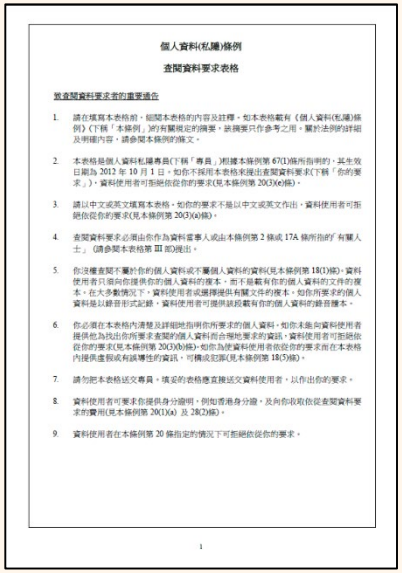
A data subject shall be entitled to：

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

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)

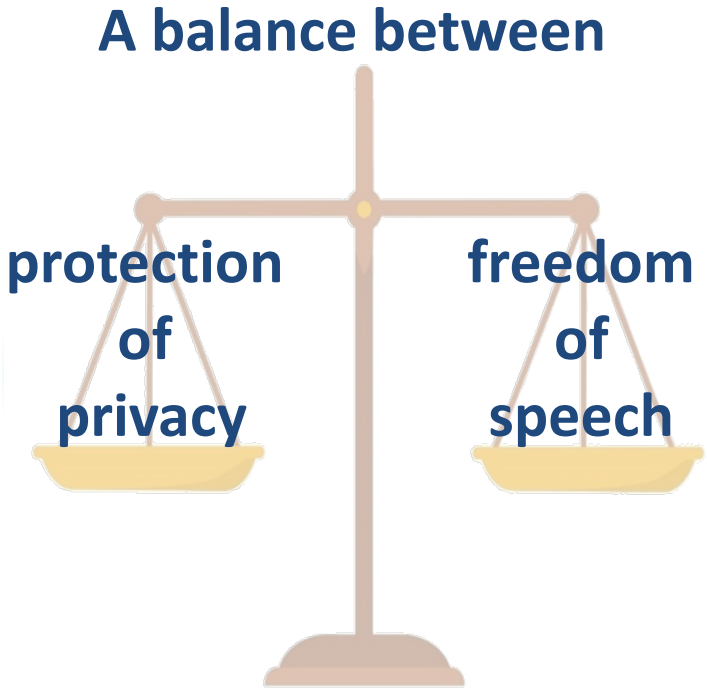
- Under Section 64 (1) of the PD(P)O, a person commits an offence if he discloses any personal data of a data subject which was obtained from a data user **without the data user's consent**, with an intent –
  a) to **obtain gain** in money or other property, whether for the benefit of the person or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



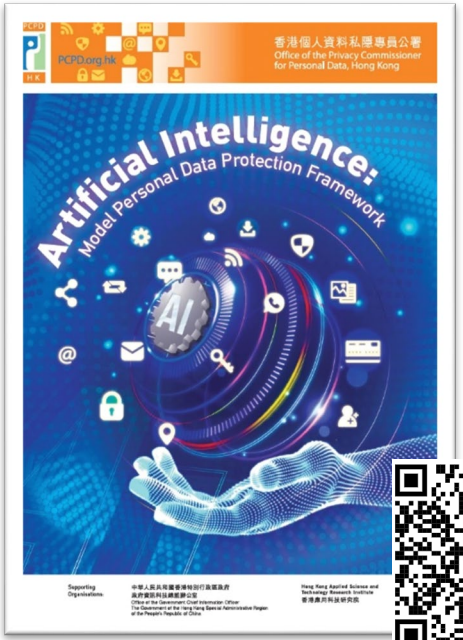
A two-tier structure of the doxxing offence

	Prosecution means	Threshold for conviction	Maximum penalty
First Tier	Summary offence	• 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	Fine of $100,000 Imprisonment for 2 years
Second Tier	Indictable offence	• 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	Fine of $1,000,000 Imprisonment for 5 years

“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 persons safety or well-being; or
- Damage to the property of the person.

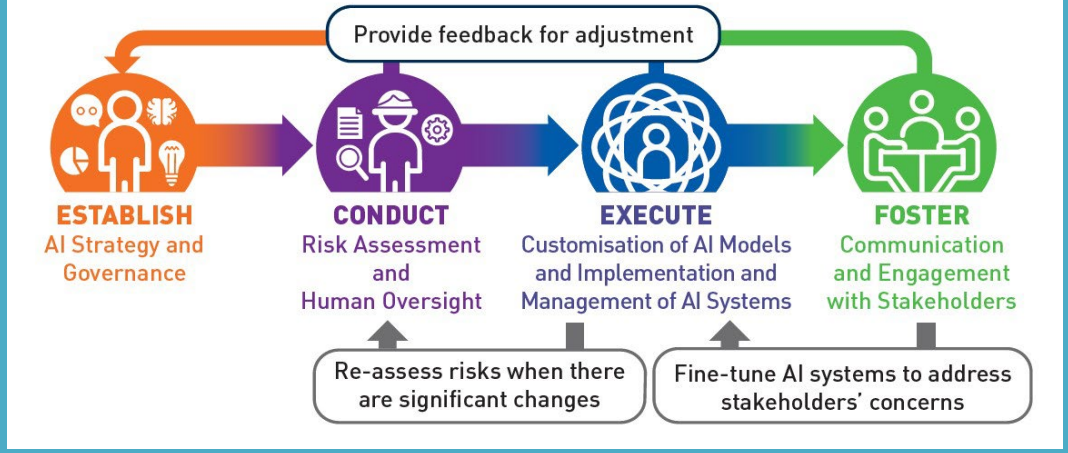
Artificial Intelligence:
Model Personal Data Protection Framework



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



PCPD.org.hk

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

01 Scope

02 Protection of Personal Data Privacy

03 Lawful and Ethical Use and Prevention of Bias

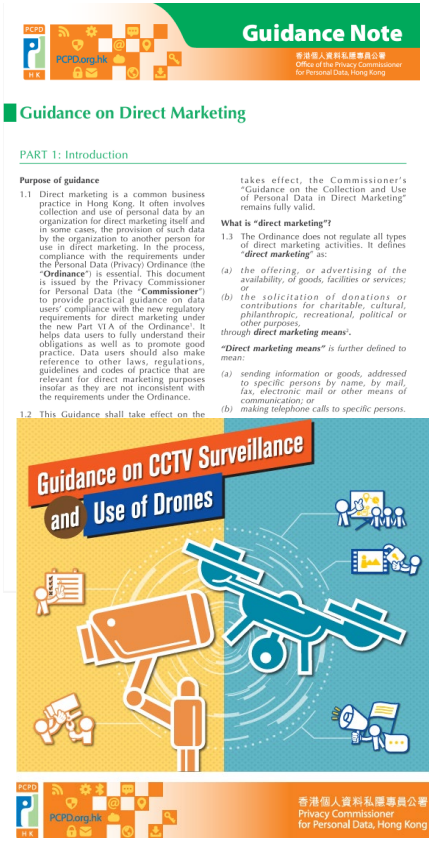
04 Data Security

05 Violations of the policies or guidelines

PCPD HK PCPD.org.hk

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



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 | --By Topic/Subject Matter-- | Please Enter Keyword | Go

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

2020-2021

2019-2020

2018-2019

Thematic webpages

PCPD.org.hk

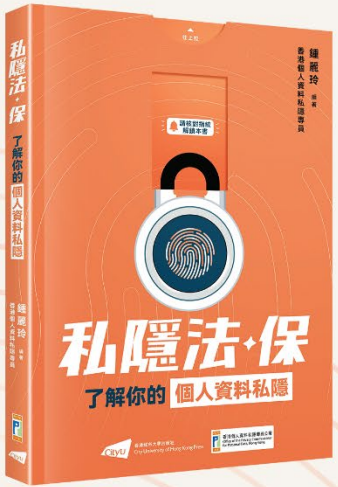
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

"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



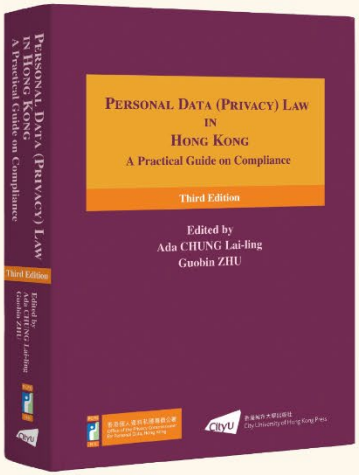
Buy Now

Personal Data (Privacy) Law in Hong Kong

A Practical Guide on Compliance (Third Edition)

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

Professor ZHU Guobin
Professor ZHU Guobin
City University of Hong Kong



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.