Introduction to the Personal Data (Privacy) Ordinance

PDPO Overview

Offences and Compensation

Six Data Protection Principles

Q&A

Direct Marketing

1. Introduction to the Concept of Privacy and the PDPO

What is “Privacy”?

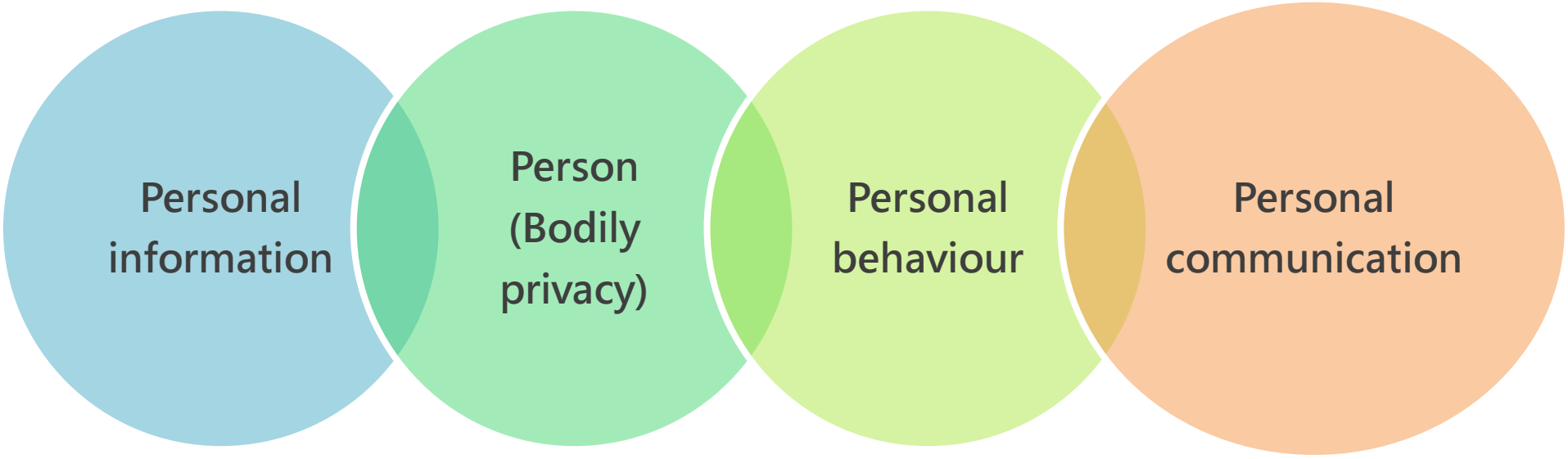
the right to be let alone, or freedom from interference or intrusion

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

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

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

Privacy covers...



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

One of the earliest comprehensive data protection laws in Asia

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

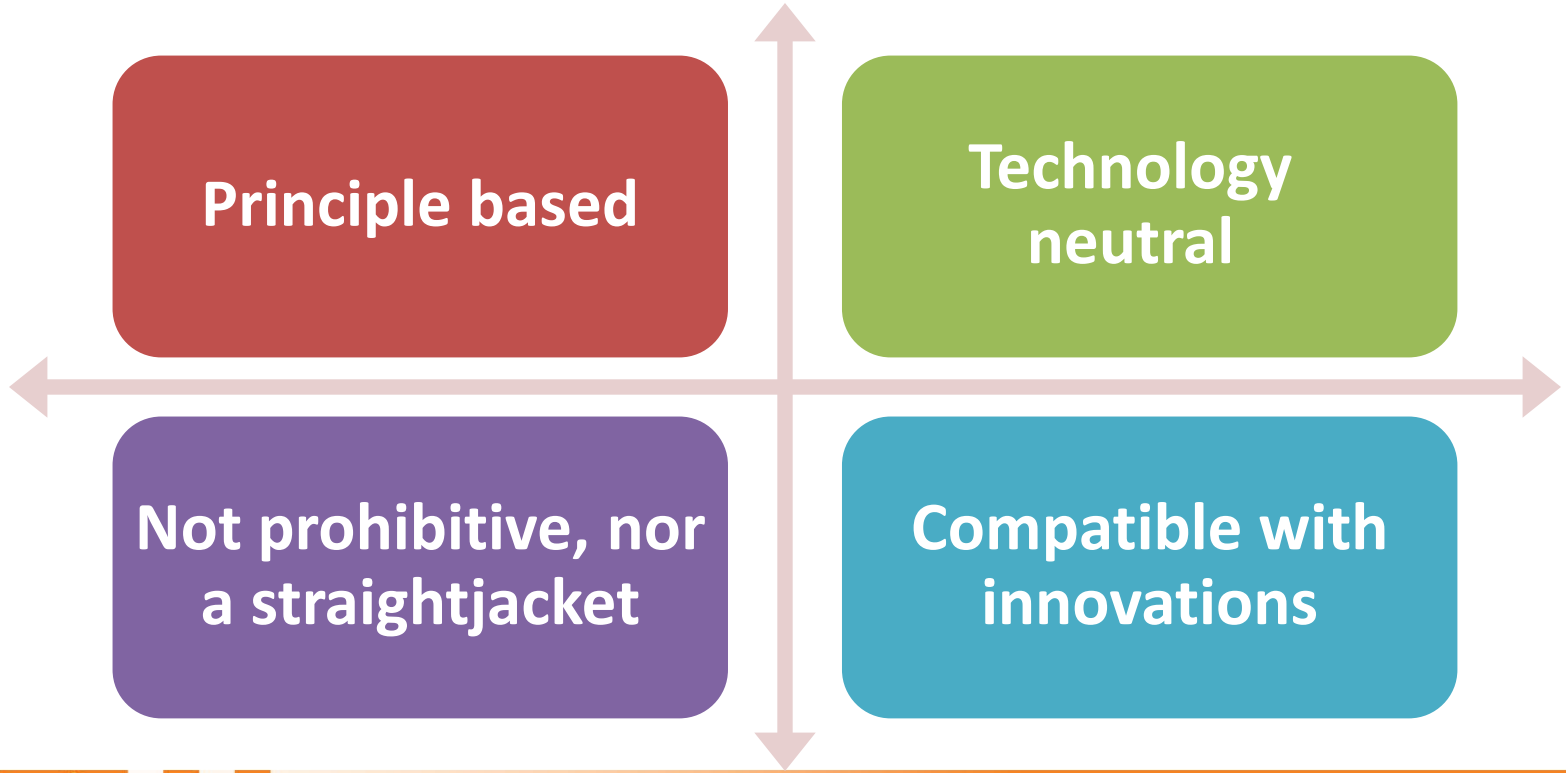
Established an independent authority, the Office of the Privacy Commissioner for Personal Data (PCPD)

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



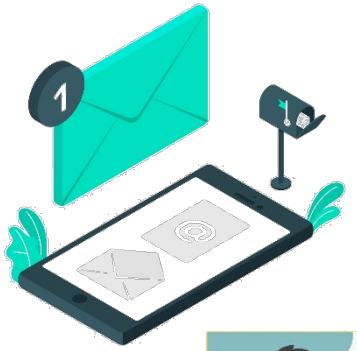
What is “Personal Data”?

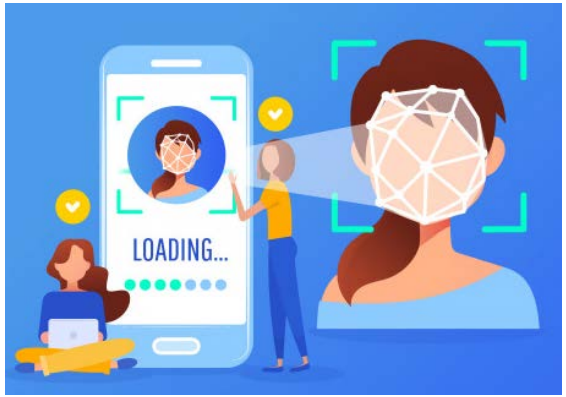
(a) relating directly or indirectly to a living individual

(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

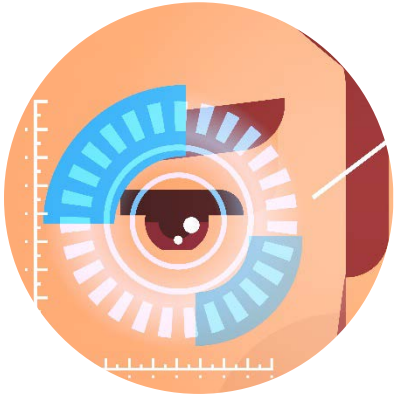




Applications of Biometric Data

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

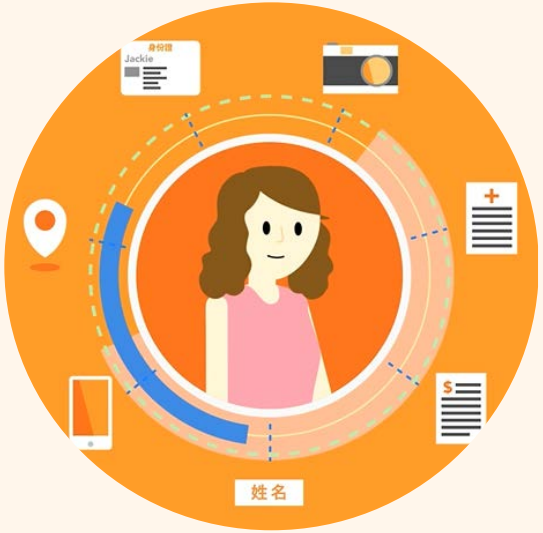
Is email address regarded as personal data?

- **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

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**

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

The *Eastweek* case

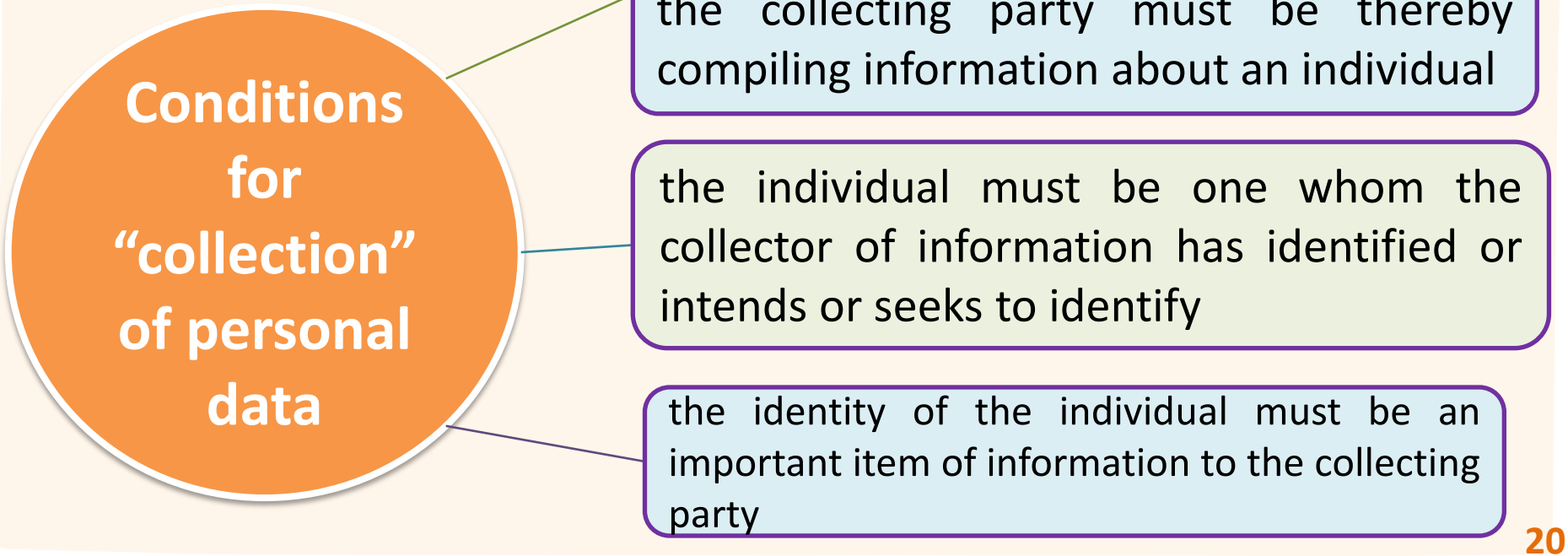
Eastweek Publisher Limited & Another v
Privacy Commissioner for Personal Data (CACV 331/1999)

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



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.

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:

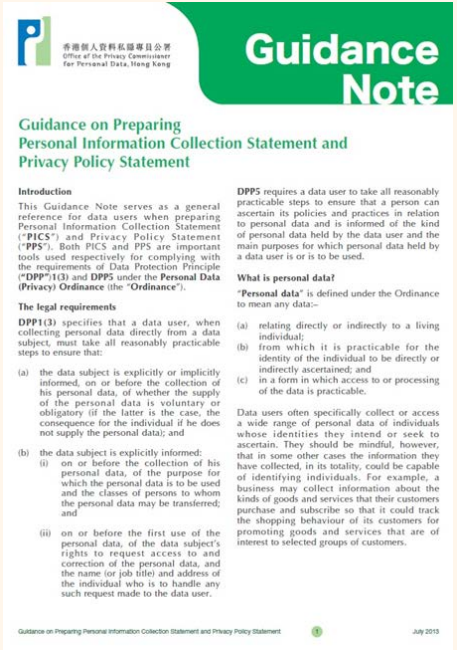
-may seek to identify the employer & information about purpose statement

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**



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

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

Case Sharing: Invalid address reported by the customer

Background:

The complainant was a customer of an insurance company. He was dissatisfied that after he had made a change of address request to the company, the insurance company still issued a letter to his invalid address to confirm the said request.

The insurance company stated:

- **Usual practice to confirm customers' change of address requests by sending letters to both the new and former addresses**
- **Such practice was designed for fraud prevention and avoiding change of address requests being made by third parties without the knowledge of the customers.**

Case Sharing: Invalid address reported by the customer

After the PCPD's intervention:

- **The insurance company revised its practice**
- **Whenever it received address update requests, instead of using the former addresses, the insurance company would contact the customers by other means, such as SMS to confirm the requests.**
- **The insurance company undertook not to issue letter to the complainant's former address.**

Case Sharing: Data Retention

Background：

- A telecommunications company's inactive database had been intruded which caused leakage of personal data of about 380,000 customers and service applicants.
- 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.**
- 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.

Case Sharing: Data Retention

PCPD's recommendation：

- **devise clear procedures** to specify the steps, time limits and monitoring measures for deleting personal data in obsolete database(s) after system migration;
- **devise a clear data retention policy** to specify the retention period(s) of personal data of customers and service applicants, which is no longer than is necessary for the fulfillment of the purpose;
- **erase all the personal data of customers and service applicants which is retained longer than the retention period(s)** as specified in the data retention policy devised.
- devise a clear data security policy to cover regular review of user privileges and security controls of remote access service; and
- implement effective measures to ensure that the policies and procedures would be expressly informed to relevant staff members and effectively executed.

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

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

Case Sharing: Disclosure of Personal Data

- The Complainant was an executive staff of an academic department and the secretary of a specific management committee in a university
- The Complainant needed to report to the head of department and the head also acted as the chairman of the Committee
- The head sent a warning email to the Complainant and, without the Complainant's consent, copied the full contents of the warning email to all members of the Committee

Case Sharing: Disclosure of Personal Data

Explanation by the University:

- one of the purviews of the Committee was to give advice on “deployment of human and other resources”
- disclosure of the warning email enabled the Committee members to ascertain the deficiency found on the Complainant's work performance

Case Sharing: Disclosure of Personal Data

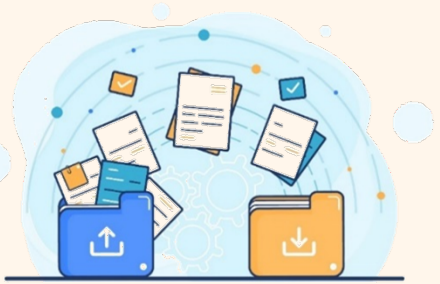
Findings:

- There was insufficient evidence indicating that the Committee members were empowered to review the work performance of the Complainant
- The Complainant's supervisor mere forwarded the warning email to the Committee members without requesting the recipients to render their advice and views on the Complainant's performance
- The university's disclosure of the warning email to the members of the Committee was not on a "need-to-know" basis and hence contravened the requirements of DPP3

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

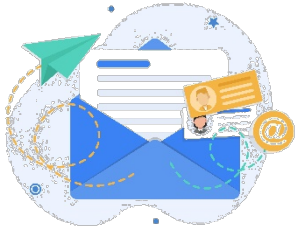
Data Breach – Common Categories

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

Case Sharing : Inadvertent disclosure of students' personal data via email by a university

Background

- A faculty staff member intended to email the faculty's non-local students about the university's quarantine arrangements. However, when retrieving the email addresses of the non-local students from the faculty's master list of students, the staff member mistakenly attached the master list in the email
- The master list contained names, dates of birth, nationalities, email addresses, correspondence addresses and contact numbers of about 2,500 students of the faculty. As a result, the personal data was unnecessarily disclosed to the recipients of the email concerned
- The university reported the incident to the PCPD

Case Sharing : Inadvertent disclosure of students' personal data via email by a university

Remedial Measures

- The university now requires all outbound emails containing personal data be checked by another staff member before they are sent
- Work files containing personal data must be encrypted

Case Sharing : Inadvertent disclosure of students' personal data via email by a university

Lesson Learnt

- Universities possess a large volume of students' personal data and should therefore take reasonably practicable measures to ensure that staff handling such data are properly trained
- Staff should observe relevant personal data privacy policies and exercise due diligence in applying those policies
- Universities should establish procedures to ensure staff's compliance with those policies

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

Case Sharing: Improper Password Management

- **An educational institution reported to the PCPD that a hacker had acquired the administrator password of its information management system through a brute force attack and created a new account with administrative rights to access the personal data stored in it.**
- **The incident affected the personal data of more than 24,000 parent and student users. Investigation revealed that the incident was due to improper password management, which failed to protect the administrator account in accordance with industry best practices.**

Remedial measures:

1. two-factor authentication for its information management system to provide an additional layer of protection for system accounts
2. strong passwords
3. regular purging of unnecessary accounts
4. enhanced training programme to raise employees' awareness of data privacy protection.

How Much is Your Data Worth?

Product	Avg. dark web price (USD)
Credit card data (Credit card details, account balance up to 5,000)	$110
50 hacked PayPal account logins	$120
Hacked Gmail account	$60
Hacked Instagram account	$25
Netflix account (1-year subscription)	$20

Source:
Privacy Affairs – Data Web Price Index 2023

Data Breach Handling – Action

Collecting Information Immediately

Immediate gathering of essential information for assessing the impact on data subjects including:

- When and where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of personal data was involved?
- How many data subjects were affected?

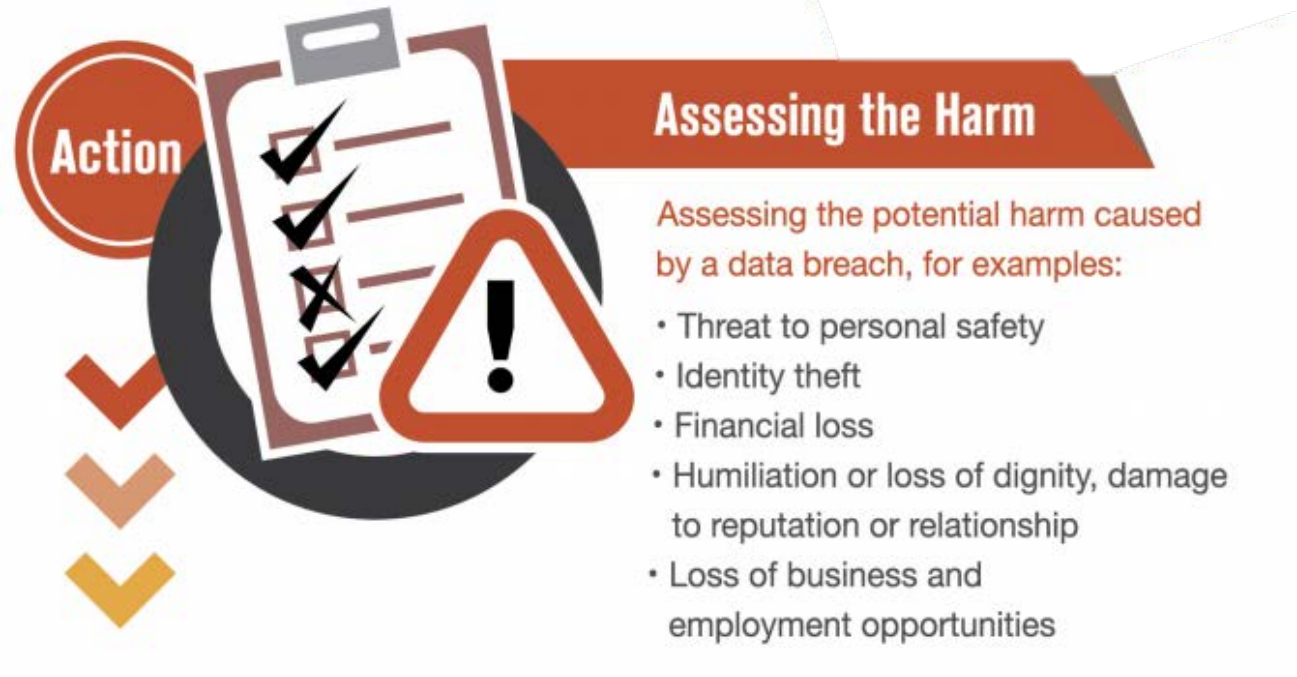
Data Breach Handling – Action

Contacting the Interested Parties & Adopting Containment Measures

Interested parties may include:

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

Data Breach Handling – Action

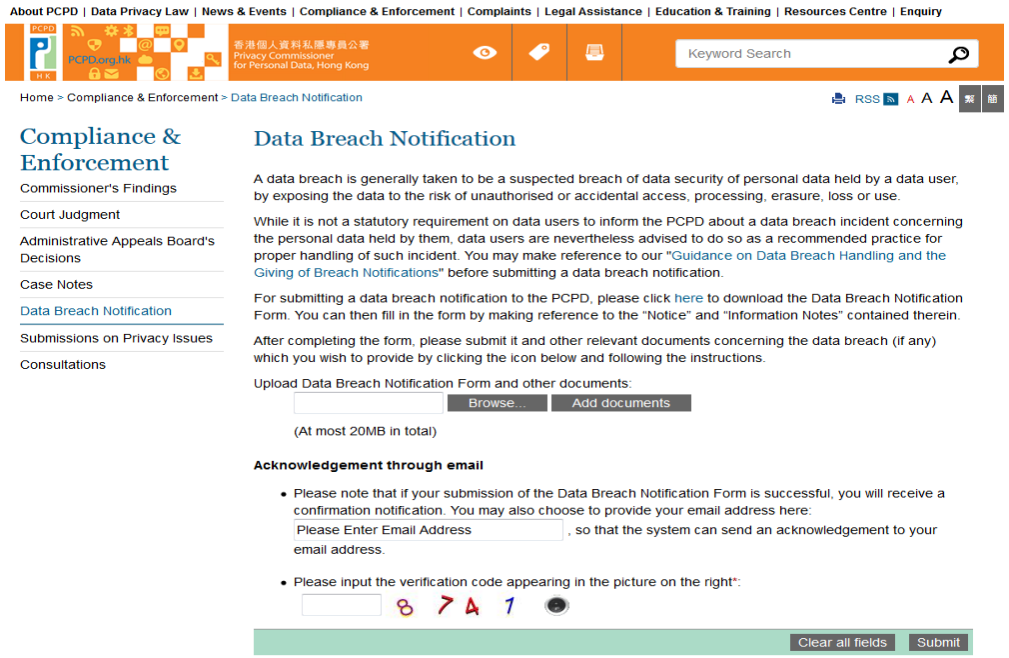


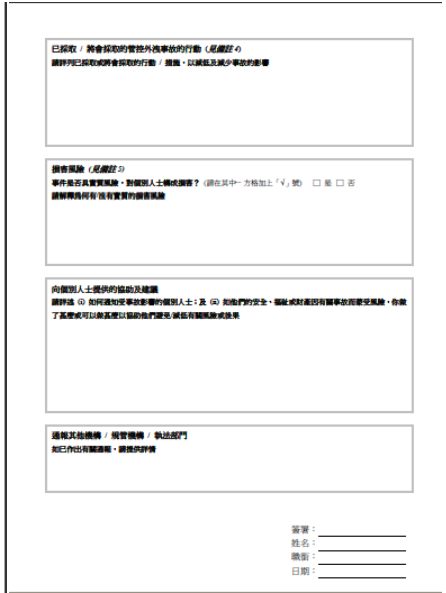
Data Breach Handling – Action

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





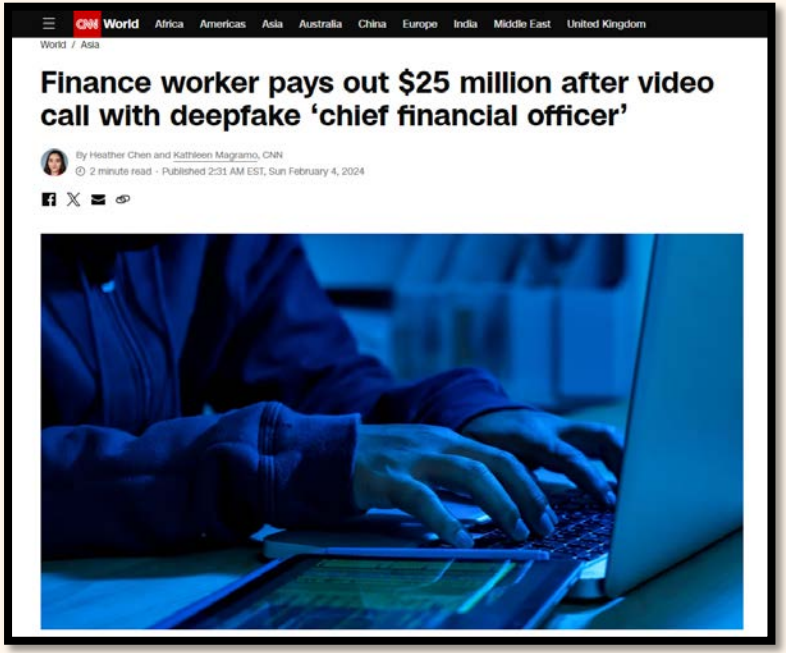
(Website：https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html)

Deepfake scams

- An employee received a message who claimed to be the "CFO", asking to join a virtual meeting.
- 4 – 6 staff also joined the meeting. The "CFO" asked the employee to transfer funds to different accounts. The meeting was ended in a hurry.

Source: The Standard

Deepfake scams



- A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

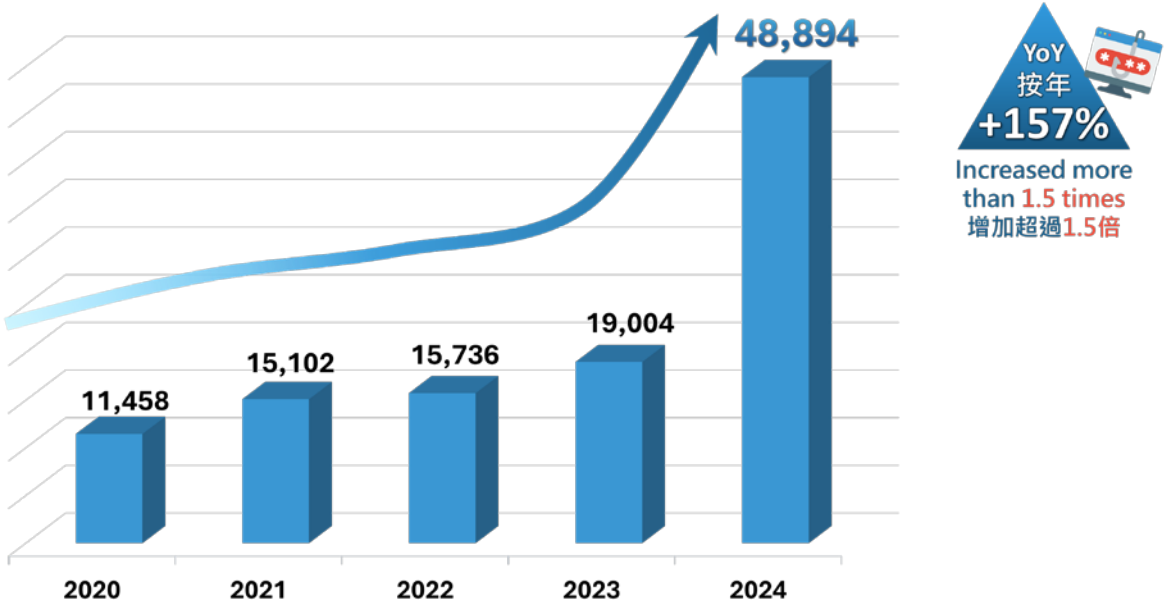
Source: CNN World

Data Governance and Organisational Measures

Training

Source: HKCERT

Trend of Phishing URL
網絡釣魚所涉及的URL走勢



New Phishing Attacks

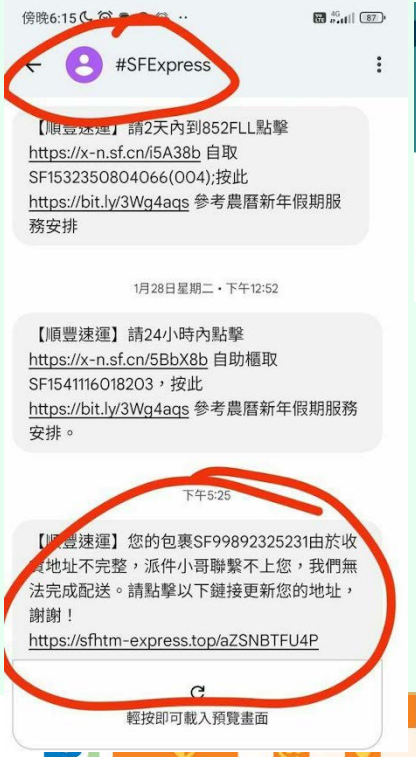
Quishing (QR Code)

Zishing (Zoom)

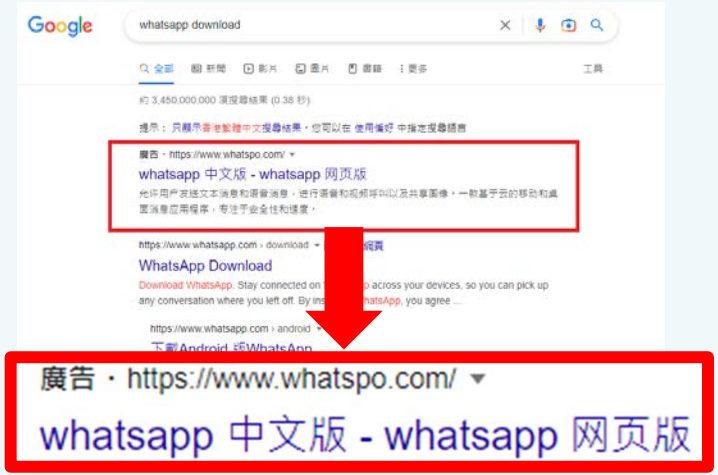
Vishing (Voice)

New Phishing Attacks

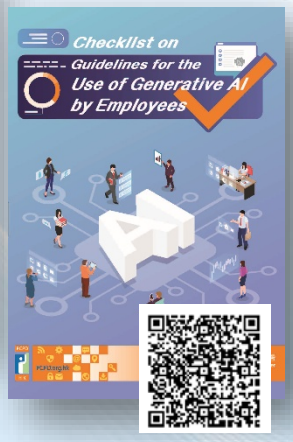
Smishing (SMS)

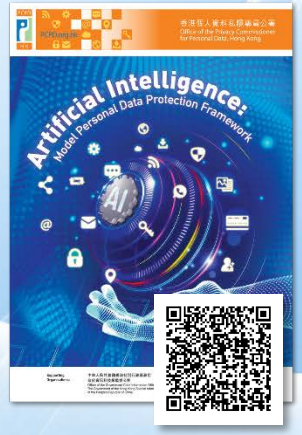


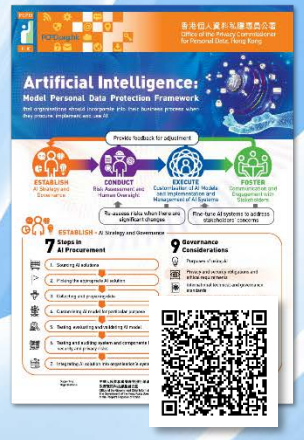
SEO Poisoning（搜尋器優化中毒）



《人工智能 (AI)：個人資料保障模範框架》
Artificial Intelligence: Model Personal Data Protection Framework

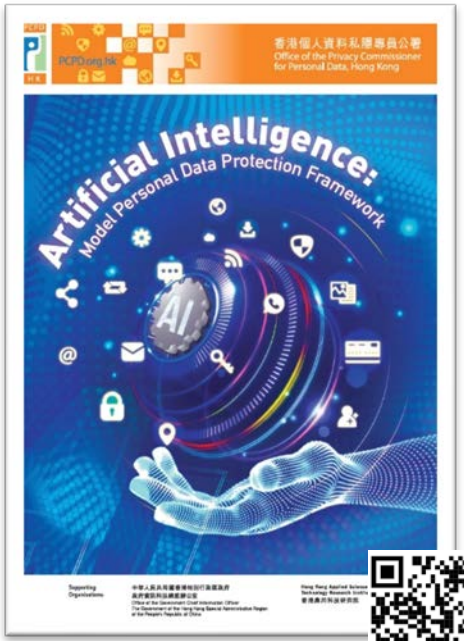






《僱員使用生成式AI的指引清單》
Checklist on Guidelines for the Use of Generative AI by Employees

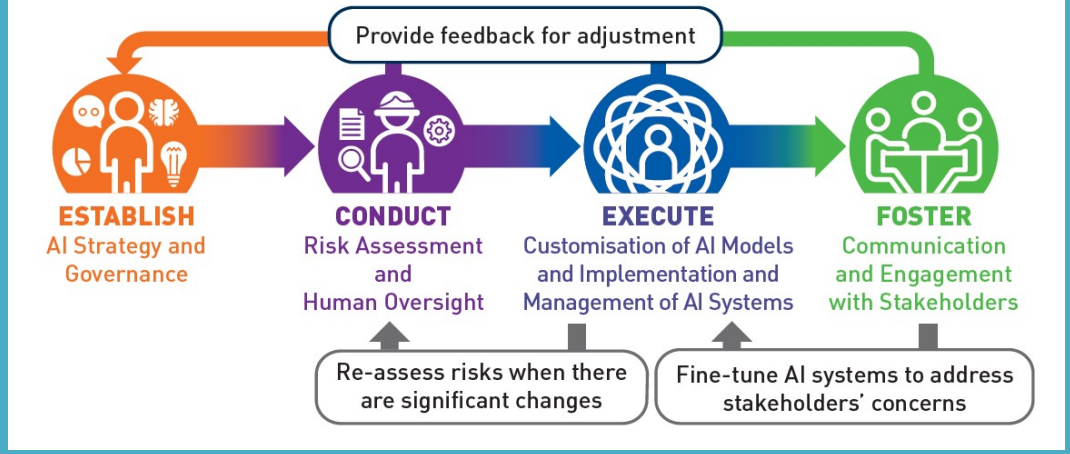
Artificial Intelligence: Model Personal Data Protection Framework



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

57

Artificial Intelligence: Model Personal Data Protection Framework

ESTABLISH
AI Strategy and Governance

- AI Strategy
- Governance Considerations
- Governance Structure
- Training and Awareness Raising

CONDUCT
Risk Assessment and Human Oversight

Lower — ***Risk level of AI system*** — *Higher*

Human-out-of-the-loop
AI makes decisions without human intervention

Human-in-command
Human actors oversee the operation of AI and intervene whenever necessary

Human-in-the-loop
Human actors retain control in the decision-making process

58

Artificial Intelligence: Model Personal Data Protection Framework

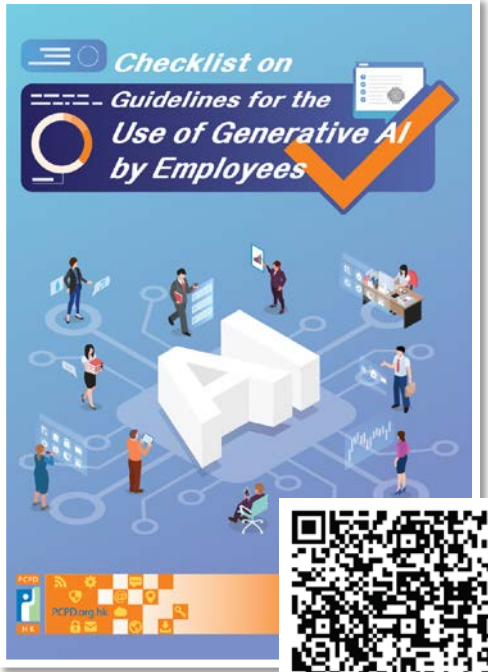
Data Preparation

Customisation and Implementation of AI

Management and Continuous Monitoring of AI

- Information Provision
- Explainable AI
- Data Subject Rights and Feedback
- Language and Manner

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

- Permitted tools
- Permissible use
- Policy applicability

02 Protection of Personal Data Privacy

- Permissible types and amounts of input information
- Permissible use of output information
- Permissible storage of output information
- Compliance with other relevant internal policies

PCPD.org.hk

Checklist on Guidelines for the Use of Generative AI by Employees

03 Lawful and Ethical Use and Prevention of Bias

- Not use Gen AI tools for unlawful or harmful activities
- Importance of employees acting as human reviewers
  - Accuracy and verification
  - Prevention of bias and discrimination
  - Watermarking / labelling

04 Data Security

- Permitted devices
- Permitted users
- Robust user credentials
- Security settings
- Response to AI incident and data breach incident

05 Violations of the policies or guidelines

- Consequences

+ Practical tips on supporting employees

61

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

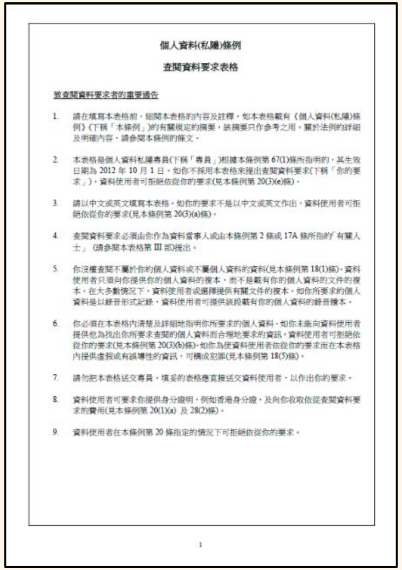
A data subject shall be entitled to：

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



Who could make a DAR?

- Data subject
- Relevant person on behalf of the data subject

"relevant person" means

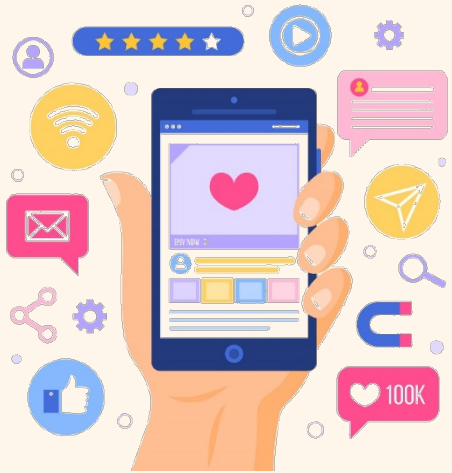
- where the individual is a minor, a person who has parental responsibility for the minor
- where the individual is incapable of managing his own affairs, a person who has been appointed by the court to manage those affairs
- guardian of a mentally incapacitated person under Part IIIA or Part IVB of 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,

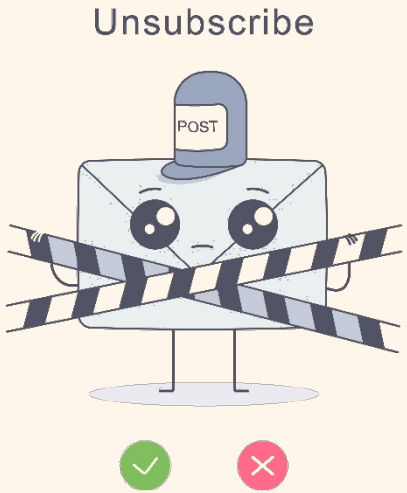
through direct marketing means (s.35A(1)).



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

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.

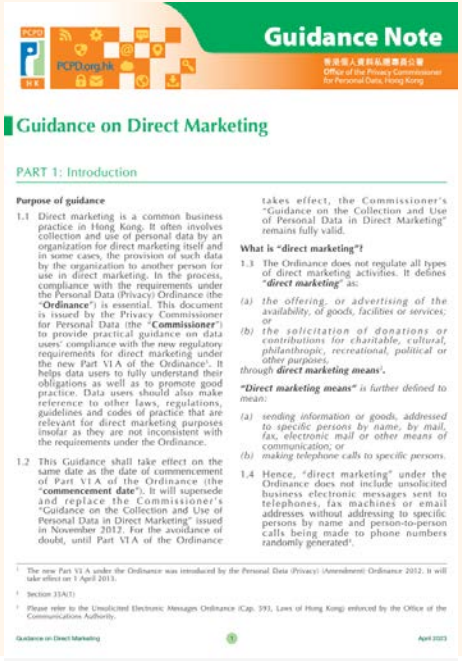
☐ The customer named objects to the proposed use of his/her personal data in direct marketing.

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

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

Guidance to Help Data Users

- **New 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

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[1]. 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 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***[2].

"***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.

1.4 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[3].

[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] Section 35A(1)

[3] 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 — April 2013 — 1


指引資料

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，一般是指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。在上述直銷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，以協助條例下新增的第VI A部（有關直接促銷的新規定），並協助資料使用者全面了解其責任和推廣良好行事方式。資料使用者亦應參考其他不抵觸條例規定而關乎直接促銷的法例、規例、指引及實務守則。

1.2 本指引將於條例第VI A部實施日期起同日生效（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》。為免生疑問，在條例第VI A部生效日前，專員的《收集及使用個人資料作直接促銷指引》仍繼續有效。

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) 要約提供貨品、設施或服務，或為該等貨品、設施或服務可予提供而進行廣告宣傳；或

(b) 為慈善、文化、公益、康體、政治或其他目的要求捐贈或貢獻[1]。

另外，「**直接促銷方法**」指：

(a) 藉郵件、圖文傳真、電子郵件或其他形式的傳訊，向指名特定人士送交資訊或貨品；或

(b) 以特定人士為致電對象的電話通話。

1.4 因此，條例下的「直接促銷」並不包括非應邀的商業電子訊息及隨打隨機抽出電話號碼的人對人電話通話[2]。

例子：

✓ 發送至具名人士的流動電話號碼的促銷短訊屬於直接促銷。

✓ 電訊服務供應商以電話聯絡現有客戶要約提供升級服務屬於直接促銷。

✗ 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送交。

✗ 捐款與邀門內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當面介紹產品／服務並不屬於直接促銷（但是其後使用這客戶的個人資料向他寄發推廣資料，則屬直接促銷）。

✗ 向非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，該部將於2013年4月1日生效。

[2] 第35A(1)條

[3] 請參考通訊事務管理局辦公室的《非應邀電子訊息條例》（香港法律第593章）。

直接促銷指引 — 1 — 2013年4月

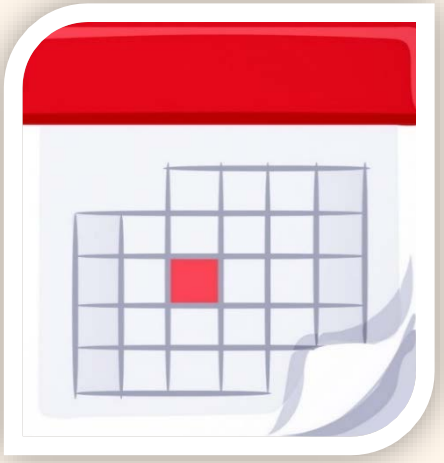
4. Offences and Compensation

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.

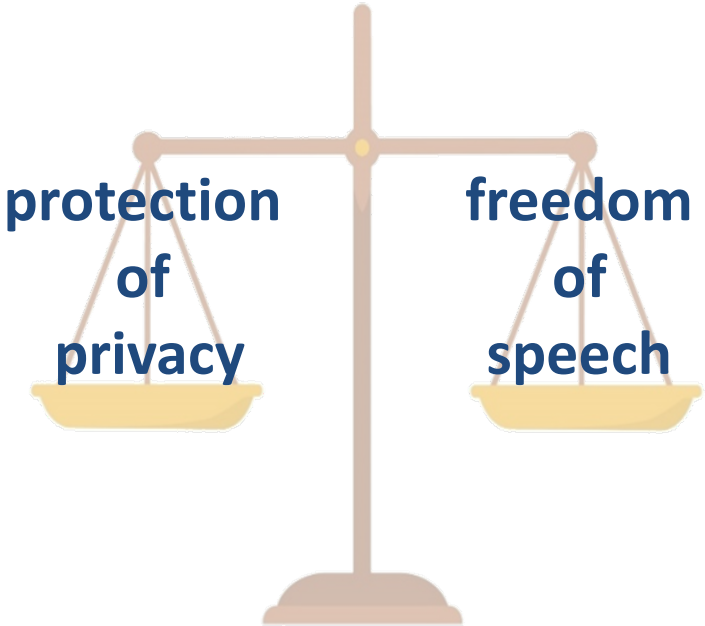


The Personal Data (Privacy) (Amendment) Ordinance 2021

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

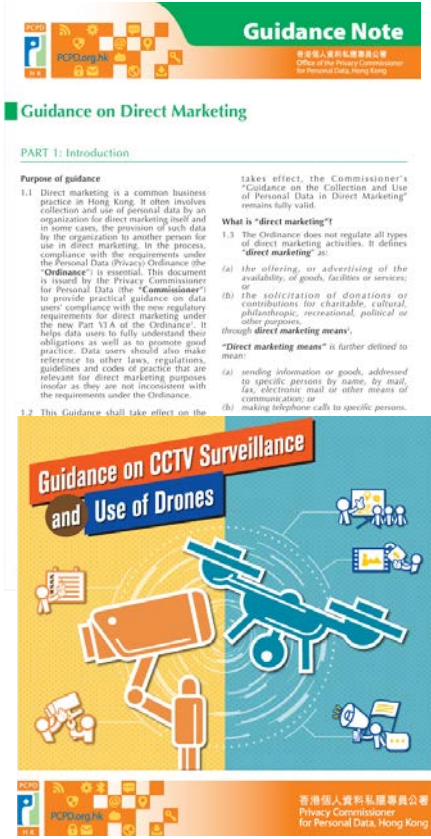
	Prosecution means	Threshold for conviction	Maximum penalty
First Tier	Summary offence	• Disclosing personal data without the data subject's consent; and • With intent to cause specified harm or being reckless as to whether specified harm would be caused	Fine of $100,000 Imprisonment for 2 years
Second 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

Compensation

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

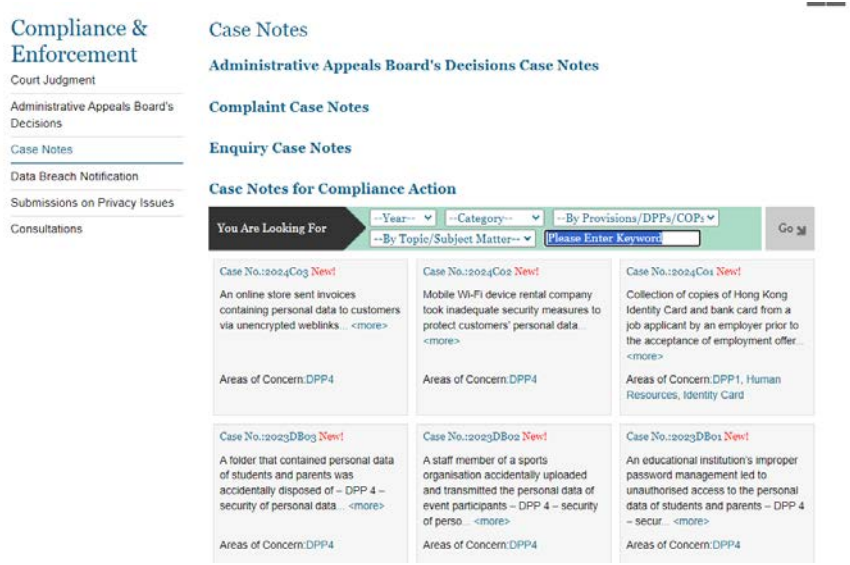
Publications

- 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

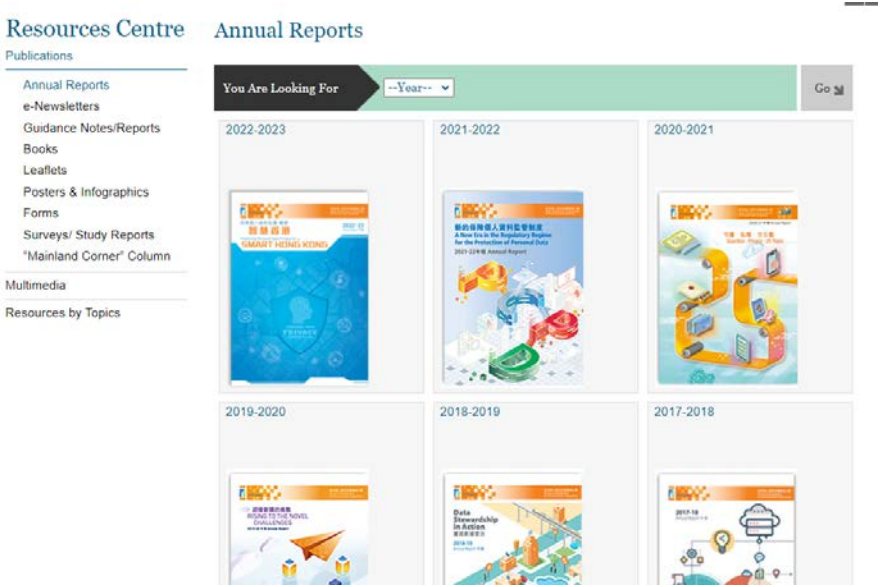


Thematic webpages

Case notes



Resources centre



PCPD.org.hk

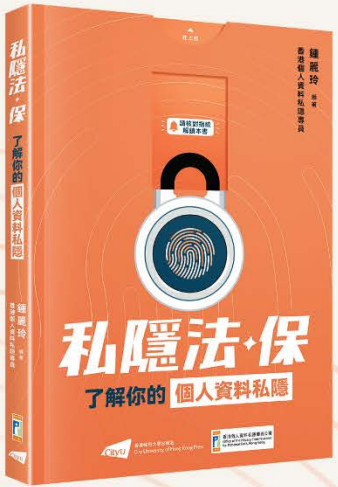
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

"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

PCPD.org.hk

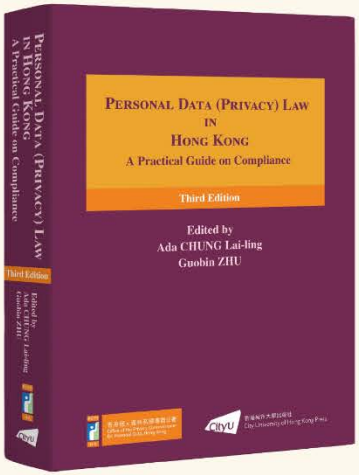
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Personal Data (Privacy) 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



Buy Now

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

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.


Q
A