PCPD.org.hk

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

香港國際數據私隱學院
Hong Kong International Data Privacy Academy

政府資助機構
Government-funded organisation

Seminar on Cyber Security and Personal Data Privacy Protection in eHealth

The Digital Healthcare Era, Fortifying Privacy Safeguards
數碼轉型新時代，醫療私隱築防線

29 October 2026

守護私隱·改革創新

Protecting Privacy · Embracing Innovation

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.

What is “Personal Data”?

According to Section 2(1) of the Personal Data (Privacy) Ordinance, personal data means any data —

a) Relating directly or indirectly to a living individual;

a) Practicable for the identity of the individual to be directly or indirectly ascertained; and

a) In a form in which access to or processing of is practicable

Pop Quiz:

Which one of the following is personal data?

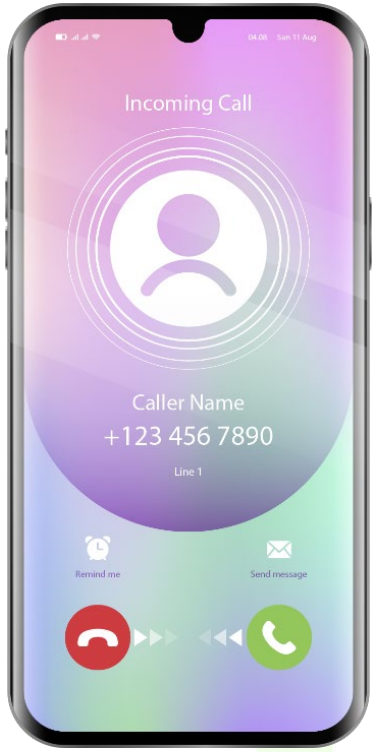
A. Vaccination records 

B. HKID Card copy 

C. Mobile number 

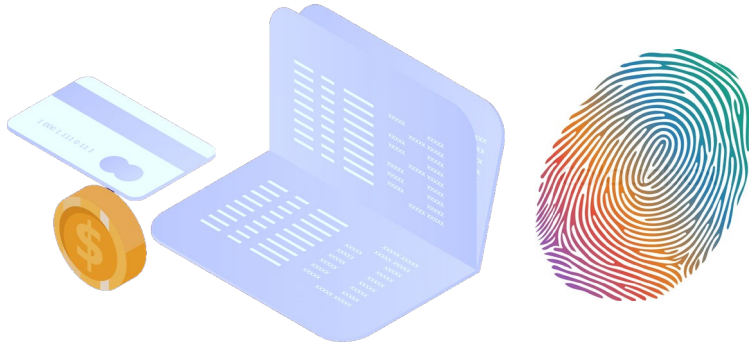
D. Fingerprint 

Examples of Personal Data

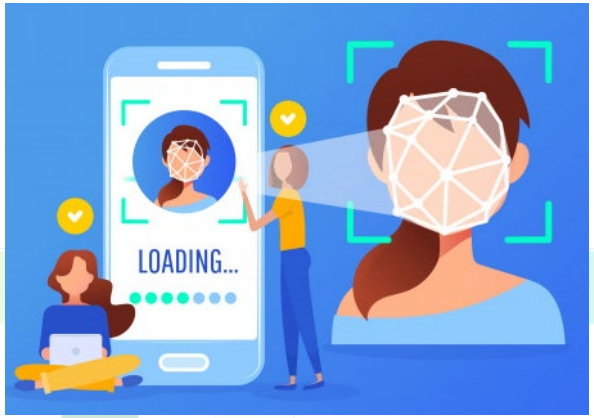


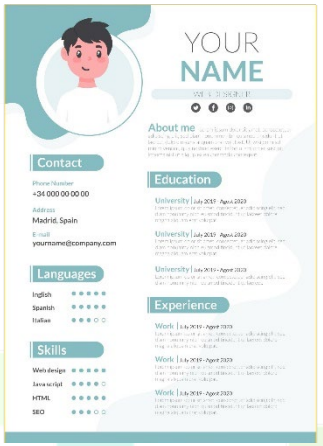


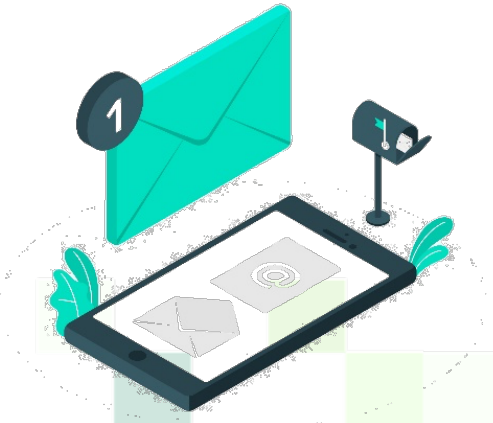












Who are involved?

Data subject	Data user	Data processor
The individual who is the subject of the data (e.g. Patients)	A person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data (e.g. Healthcare providers)	A person who – a) Processes personal data on behalf of another person; and b) Does not process the data for any of his/her own purposes

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



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.



DPP1: Collection Purpose & Means



Practical Guidance for Healthcare Providers

1. Patiently explain the use of the eHealth System to patients in detail to ensure that patients understand the benefits of sharing their health records;

2. Ensure that their staff will remind patients, before giving joining consent and/or sharing consent, to read carefully the "Personal Information Collection Statement", "Privacy Policy Statement", and "Participant Information Notice" issued by the Commissioner for the Electronic Health Record; and

3. Explain to patients in detail how withdrawing from the eHealth System and/or revoking consent to share information with any healthcare provider may affect the healthcare services patients receive.

DPP2: Accuracy & Retention

Data users should take all practicable steps to ensure:

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



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

DPP3: Use of Personal Data

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

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

- **Under certain circumstances, a relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using the data subject's personal data for a new purpose**



DPP3: Use of Personal Data

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: Use of eHealth record for other purpose

Background:

- A patient was dissatisfied with the medicine prescribed to him by a doctor of a medical centre, hence lodged a complaint to the Medical Council of Hong Kong. The complaint was dismissed by the Medical Council on the ground that there was insufficient evidence as proof of any misconduct.

- The patient subsequently **received a SMS notification which stated that the doctor had accessed his electronic health record on the Electronic Health Record Sharing System**. As a result, the patient lodged the second complaint to the Medical Council for an alleged violation of his privacy by the doctor, which was referred to the PCPD for follow-up upon the patient's consent.



Case Sharing: Use of eHealth record for other purpose

Findings:

- the Privacy Commissioner found that when the doctor accessed to the patient's electronic health record, he was not providing medical treatment to him, but **the access was made for refreshing his memory to deal with enquiry from Medical Council**.
- In this connection, the purpose of the doctor's access and use of the patient's health records at the material time was **inconsistent with the original purpose for which the data was collected, thereby contravening DPP3**. Hence, the Privacy Commissioner issued a written warning to the doctor.



DPP4: Security of Personal Data

Data Breach – Common Categories



Cyberattack or hacking



Improper/wrongful disposal of personal data



Loss of documents or portable devices



Staff misconduct

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**



- **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**

DPP4: Security of Personal Data



Practical Guidance for Healthcare Providers

Healthcare providers shall adopt all practicable steps to protect the personal data in the eHealth System. For example:

- **Ensure that when authorised staff log into the eHealth System, electronic health records shown on the computer screen will not be seen by unrelated third parties (e.g. consider configuring screen orientation and/or using a privacy filter)**

- **Conduct risk assessment for devices if patients' electronic health records in the eHealth System are accessed through notebook computers at non-registered locations for provision of healthcare services (e.g. consultation at patients' homes)**

DPP4: Security of Personal Data



Practical Guidance for Healthcare Providers

- Keep electronic health records downloaded or printed from the eHealth System (in paper or electronic form) safely, and formulate guidelines on the use of portable storage devices to minimise the risk of personal data leakage

- Adopt appropriate measures to ensure that healthcare providers' information systems are adequately safeguarded and properly functioning to avoid jeopardising patients' electronic health records in the eHealth System

If there is a data breach of the eHealth System, healthcare providers should notify both the Commissioner for the Electronic Health Record and the Privacy Commissioner as soon as possible.

Case Sharing: Ransomware Attack

Background:

- A clinical centre's servers containing patients' personal data were attacked by ransomware, resulting in the malicious encryption of files containing personal data of around 100,000 patients, including names, identity document numbers, telephone numbers, dates of birth, addresses, and medical records.

- The incident was likely caused by the use of firewall firmware that was not up to date, which allowed the hacker to exploit an unpatched vulnerability in the firewall to remotely execute commands or programs through SSL VPN to acquire the credentials of an administrative account, and subsequently deployed ransomware. There was no policies or procedures in place relating to vulnerability and patch management.



PCPD commenced an investigation and served an Enforcement Notice on the clinical centre.

Case Sharing: Ransomware Attack

Remedial Measures

- The clinical centre implemented remedial measures, including
  - upgrading the firewall firmware and patching the vulnerability in question;
  - implementing a series of security enhancements on its information systems;
  - devising policies and procedures related to application vulnerability and patch management; and
  - implementing multi-factor authentication for all remote access users accessing personal data.



DPP4: Security of Personal Data

Recommended Data Security Measures for ICT in 7 Areas

1. Data Governance and Organisational Measures
2. Risk Assessments
3. Technical and Operational Security Measures
4. Data Processor Management
5. Remedial Actions in the event of Data Security Incidents
6. Monitoring, Evaluation and Improvement
7. Other Considerations



DPP4: Security of Personal Data

Data Governance and Organisational Measures — *Policy and Procedures*



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



NOTE

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

DPP4: Security of Personal Data

Technical and Operational Security Measures



DPP4: Security of Personal Data

Data Governance and Organisational Measures — *Training*

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





DPP4: Security of Personal Data

Data Governance and Organisational Measures — *Training*

Enhance staff's awareness on phishing attack

- According to the Cybersecurity and Infrastructure Security Agency, CISA, ransomware is mainly transmitted through online phishing emails or drive-by downloads.

Hong Kong / Law and Crime

'Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting

- Employee fooled after seeing digitally recreated versions of company's chief financial officer and others in video call
- Deepfake technology has been in the spotlight after fake explicit images of pop superstar Taylor Swift spread on social media sites

YP / Discover / News / Hong Kong

Hong Kong sees drop in email phishing cases, but scam drill shows cybersecurity awareness 'still lacking'

- *City reports 54.2 per cent drop in cases compared with same period last year*
- *But police say more public awareness is needed, as participants in anti-scam drill fell for fake online meeting invites, AI chatbot subscriptions*

Listen to this article

by **SCMP** | Published: 10:47am, 2 Aug, 2023

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

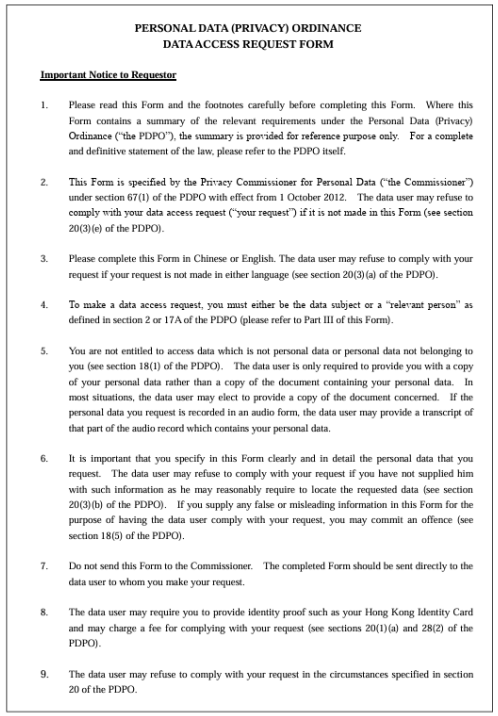
A data subject shall be entitled to :

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



PERSONAL DATA (PRIVACY) ORDINANCE
DATA ACCESS REQUEST FORM

Important Notice to Requestor

1. Please read this Form and the footnotes carefully before completing this Form. Where this Form contains a summary of the relevant requirements under the Personal Data (Privacy) Ordinance ("the PDPO"), the summary is provided for reference purpose only. For a complete and definitive statement of the law, please refer to the PDPO itself.

2. This Form is specified by the Privacy Commissioner for Personal Data ("the Commissioner") under section 67(1) of the PDPO with effect from 1 October 2012. The data user may refuse to comply with your data access request ("your request") if it is not made in this Form (see section 20(3)(e) of the PDPO).

3. Please complete this Form in Chinese or English. The data user may refuse to comply with your request if your request is not made in either language (see section 20(3)(a) of the PDPO).

4. To make a data access request, you must either be the data subject or a "relevant person" as defined in section 2 or 17A of the PDPO (please refer to Part III of this Form).

5. You are not entitled to access data which is not personal data or personal data not belonging to you (see section 18(1) of the PDPO). The data user is only required to provide you with a copy of your personal data rather than a copy of the document containing your personal data. In most situations, the data user may elect to provide a copy of the document concerned. If the personal data you request is recorded in an audio form, the data user may provide a transcript of that part of the audio record which contains your personal data.

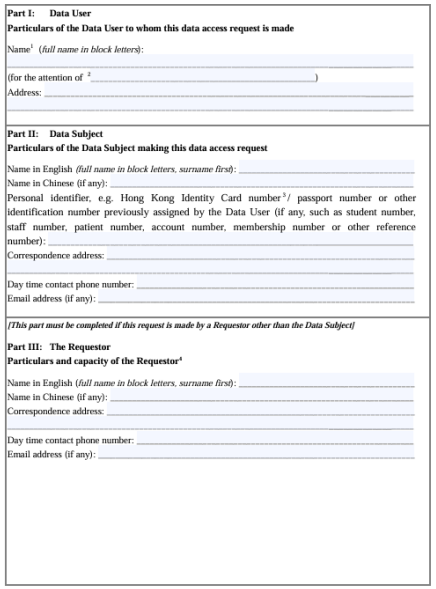
6. It is important that you specify in this Form clearly and in detail the personal data that you request. The data user may refuse to comply with your request if you have not supplied him with such information as he may reasonably require to locate the requested data (see section 20(3)(b) of the PDPO). If you supply any false or misleading information in this Form for the purpose of having the data user comply with your request, you may commit an offence (see section 18(5) of the PDPO).

7. Do not send this Form to the Commissioner. The completed Form should be sent directly to the data user to whom you make your request.

8. The data user may require you to provide identity proof such as your Hong Kong Identity Card and may charge a fee for complying with your request (see sections 20(1)(a) and 28(2) of the PDPO).

9. The data user may refuse to comply with your request in the circumstances specified in section 20 of the PDPO.

1



Part I: Data User
Particulars of the Data User to whom this data access request is made

Name[1] (*full name in block letters*):
(for the attention of [2])
Address:

Part II: Data Subject
Particulars of the Data Subject making this data access request

Name in English (*full name in block letters, surname first*):
Name in Chinese (if any):
Personal identifier, e.g. Hong Kong Identity Card number[3] / passport number or other identification number previously assigned by the Data User (if any, such as student number, staff number, patient number, account number, membership number or other reference number):
Correspondence address:
Day time contact phone number:
Email address (if any):

[This part must be completed if this request is made by a Requestor other than the Data Subject]

Part III: The Requestor
Particulars and capacity of the Requestor[4]

Name in English (*full name in block letters, surname first*):
Name in Chinese (if any):
Correspondence address:
Day time contact phone number:
Email address (if any):

1 Please fill in the full name of the Data User to whom the data access request is addressed.
2 If you have previously been informed by the Data User of the name and/or job title of the person to whom such a data access request may be made, please fill in here the name and/or job title of such person.
3 For Data Subject who is Hong Kong Identity Card holder. Please note that the information may assist the Data User to retrieve or locate the Requested Data. The identity card number needs not be provided in this Form if you have reasonable grounds to believe that this will not be necessary for the unique identification of the Data Subject by the Data User in the circumstances.
4 The Data User may require reasonably sufficient personal information from you to satisfy itself as to your identity before it can comply with this data access request.

4

Practical guidance for healthcare providers and healthcare professionals

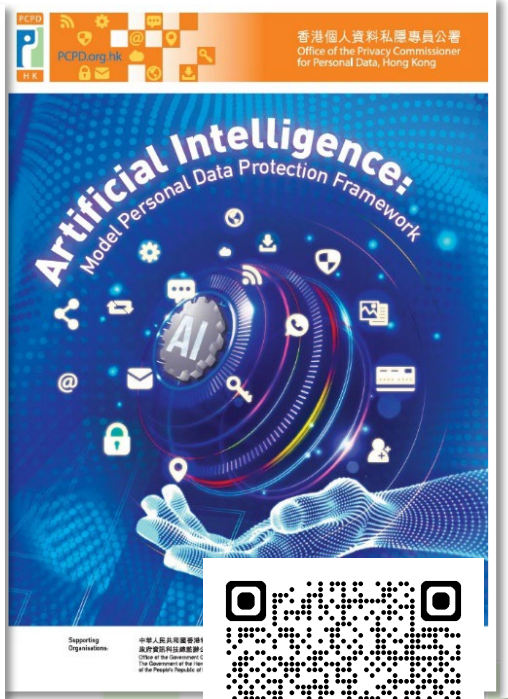
Personal Data (Privacy) Ordinance and the Electronic Health System: Points to Note for Healthcare Providers and Healthcare Professionals

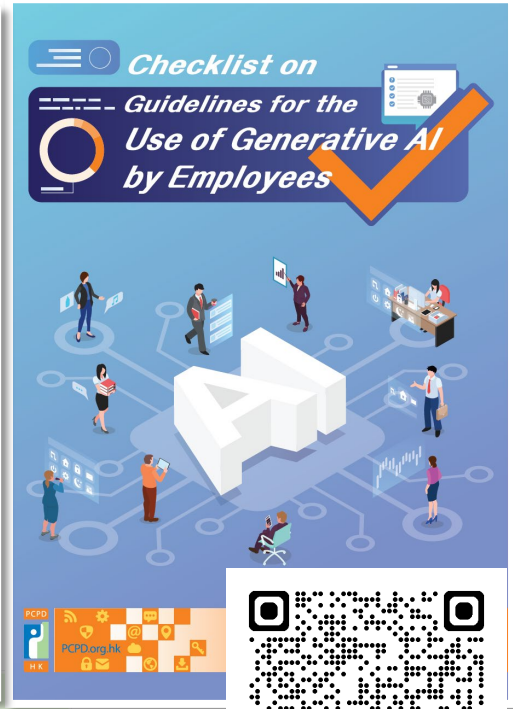
The Information Leaflet provides practical guidance on matters that healthcare providers and healthcare professionals should note, as well as recommended good practices when they use the eHealth System in handling patients' personal data.

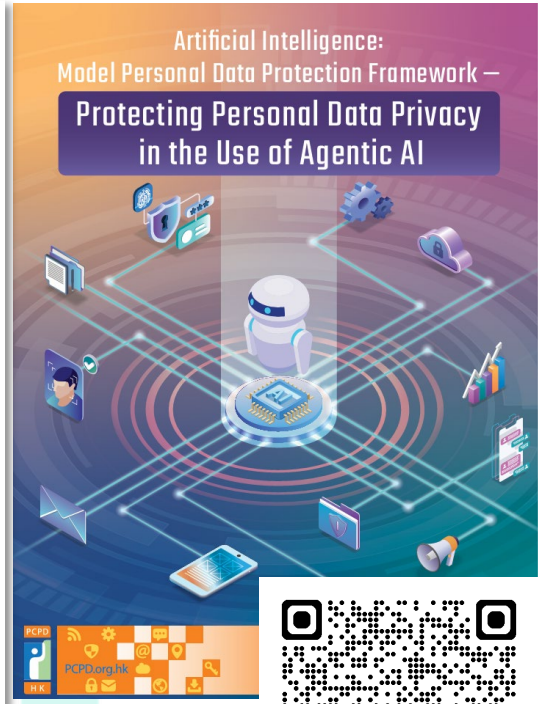


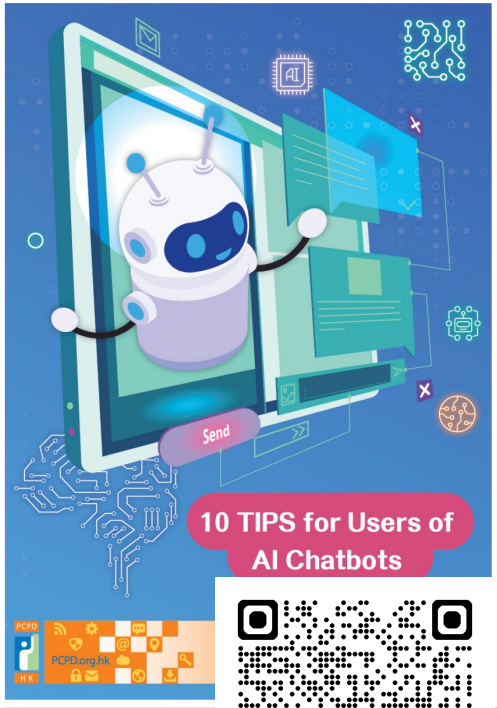
PCPD's AI Guidance







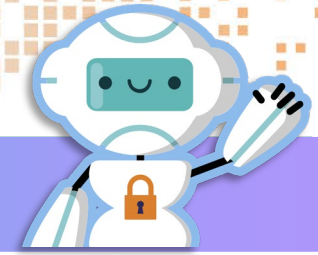




PCPD.org.hk

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

守護私隱・改革創新
Protecting Privacy・Embracing Innovation



Contact Us

Telephone: 2827 2827 Fax: 2877 7026

Website: www.pcpd.org.hk

Email: communications@pcpd.org.hk

Address: Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wan Chai, Hong Kong

Follow Us

私隱公署PCPD

香港个人资料私隐专员公署

Office of the Privacy Commissioner for Personal Data, Hong Kong