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

2025年聖職人員學習營

收集及處理個人資料法寶

2025年1月8日

鍾麗玲女士 - 個人資料私隱專員
林港燕女士 - 私隱專員公署經理
（企業傳訊部）

1 六項保障資料原則

2 數據安全及人工智能安全

3 保護網上個人資料

何謂「個人資料」？

(a) 直接或間接與一名在世人士有關

(b) 從該等資料直接或間接地確定有關的個人的身分是切實可行的

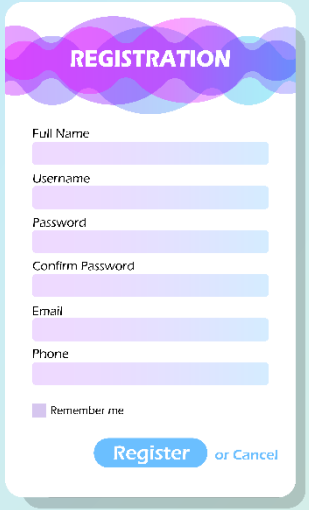
(c) 該等資料的存在形式令查閱及處理均是切實可行的

個人資料的例子


Incoming Call
Caller Name
+123 456 7890


HONG KONG PERMANENT IDENTITY CARD
SURNAME, NAME
0000 1111 2222
Date of Birth
DD-MM-YYYY SEX
*****
Date of Issue
(MM-YY)
DD-MM-YY
NUMBERS


LOADING...


REGISTRATION
Full Name
Username
Password
Confirm Password
Email
Phone
Remember me
Register
or Cancel


TRACKING
HEALTH

六項保障資料原則是.....

- 《個人資料（私隱）條例》的**基本規定**
- 涵蓋由**收集**、**保存**、**使用**以至**銷毀**個人資料的整個**生命周期**
- 資料使用者必須遵從

6 保障資料原則 Data Protection Principles

PCPD.org.hk

PCPD HK

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性、儲存及保留 Accuracy & Retention

資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述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 practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

個案分析（一）收集個人資料

個案背景

- 投訴人委託一間教友服務中心辦理其母親的後事時，向該中心提供了包括電話號碼及地址等個人資料，並曾在與該中心職員會面時出示身份證。其後投訴人發現該中心將其個人資料轉移予一間殯儀公司，投訴人遂向公署投訴該中心**在未有通知他的情況下轉移其個人資料**。
- 該中心表示就投訴人的服務申請，他們在服務申請表上登記了投訴人的姓氏及電話號碼，而沒有從其出示的身份證記錄任何其他資料。在該個案中，該中心按一貫做法將投訴人的服務申請表副本交予提供殯儀服務的承辦商，以安排有關服務。

個案分析（一）收集個人資料

《私隱條例》的規定

- 保障資料第1(3)原則規定，資料使用者在直接向資料當事人收集個人資料時，須採取所有合理地切實可行的步驟，以確保在收集個人資料之時或之前，告知資料當事人個人資料將會用於甚麼目的及個人資料可能轉移予甚麼類別的人等資訊。

結果

- 該中心修訂了服務申請表，在表格中加入《收集個人資料聲明》，述明服務申請人提供的個人資料會被轉移予該中心的服務承辦商以提供殯儀服務。

個案分析（二）使用個人資料

個案背景

- 投訴人是一間教堂的教友，於該教堂領洗後向其提供包括姓名、身份證號碼、出生日期、地址及婚姻狀況等個人資料。一日，投訴人與該教堂的一名執事傾談期間，該執事向投訴人表示他曾查看該教堂的電腦系統，得悉投訴人未有向該教堂更新婚姻狀況，並指投訴人的領洗紙並無其婚姻紀錄。
- 投訴人表示該執事在該教堂的職責範圍並不包括處理會友的個人資料，故相信他曾在未獲授權及未經投訴人的同意下，登入該教堂的電腦系統或記錄冊查閱其個人資料，投訴人遂向公署提出投訴。

結果

公署提醒該教堂須緊遵《私隱條例》下有關個人資料的使用及保安之規定，以保障及尊重他人在私隱方面的期望。

2 數據安全及人工智能安全

《私隱條例》的相關規定

資料外洩事故可構成違反《私隱條例》 附表1的保障資料第4原則

保障資料第4(1)原則

資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響

保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料處理者作處理的個人資料被未獲准許或意外地被查閱、處理、刪除、喪失或使用

資料外洩的常見原因

主要技術風險

網絡釣魚

未修補保安漏洞

低強度密碼

過時的操作系統
和應用程式

植入惡意軟件

個案分析（三）遺失便攜式電腦硬碟

個案背景

- 一名牧師乘坐專線小巴時，遺失一個載有65名會眾個人資料的便攜式電腦硬碟，當中包括姓名、地址、電話號碼及電郵地址

- 在公署的查詢過程中，該教會及牧師表示，他把會眾的個人資料儲存至未經加密的私人電腦硬碟以便聯繫會眾，惟事發時並無必要將該硬碟攜離教會。教會在事發前未有就使用便攜式裝置儲存個人資料制定任何指引。

補救措拖：

1. 制定「保障個人資料私隱措施」指引，明確規定未經教會的董事局授權，不可將個人資料儲存於便攜式裝置內
2. 規定同工如獲准使用便攜式裝置儲存個人資料，必須使用由教會提供具備密碼保護功能的便攜式裝置，並在使用後立即刪除內存的個人資料及交還有關裝置
3. 透過例會向董事及同工說明該指引及使用便攜式裝置的安排，並承諾每年傳閱該指引

個案分析（四）勒索軟件攻擊

個案背景

- 2024年，非牟利機構A向私隱專員公署作出資料外洩通報，表示其伺服器遭**勒索軟件攻擊及惡意加密**。有關的勒索軟件屬**Trigona的變種**，合共八台伺服器、一台數據儲存器及18台電腦遭受勒索軟件攻擊及加密。黑客曾要求機構支付贖金，為已被加密的檔案解鎖。

- 事件涉及**超過72,300名**會員的個人資料，當中包括姓名、香港身份證號碼、護照號碼、相片、出生日期、地址、電郵地址、電話號碼及緊急聯絡人的姓名及電話號碼。

調查結果發現六項缺失：

1. 伺服器被意外地**曝露於互聯網**
2. 資訊系統欠缺有效的**偵測措施**
3. 沒有為管理員帳戶啟用**多重認證**功能
4. 欠缺資訊**保安政策**及指引
5. 沒有定期進行**風險評估**及**保安審計**
6. 欠缺離線**數據備份**方案

個案分析（五）即時通訊軟件帳戶遭騎劫

個案背景

- 於2023年，私隱專員公署接獲23宗有關社福機構及學校（包括天主教機構)的資料外洩事故通報，表示用作與服務使用者、學生及／或學生家長通訊的**即時通訊軟件帳戶遭騎劫**，騙徒繼而盜用有關即時通訊軟件帳戶**假冒受害機構**，向通訊錄的聯絡人發送訊息企圖騙取金錢。有關事件涉及近**2,600名服務使用者、學生、學生家長及／或職員**的姓名及手提電話號碼等個人資料。

騎劫WhatsApp帳戶的常見手法

釣魚訊息	騙徒已騎劫受害人的親友的WhatsApp帳戶，並假扮該親友發送WhatsApp訊息予受害人，誘騙受害人轉發其WhatsApp帳戶的驗證碼
假冒短訊	假冒WhatsApp官方發出短訊，誘騙受害人按下連結至假網頁，騙取其電話號碼及WhatsApp帳戶驗證碼
假冒網站	於搜尋網站放置假冒的WhatsApp網頁版，誘騙受害人掃瞄假冒二維碼，騙取其電話號碼及WhatsApp帳戶驗證碼

保障WhatsApp帳戶的措施

啟用WhatsApp雙重認證功能

定期在WhatsApp設定中檢查已連結裝置

切勿向他人透露任何密碼或驗證碼

一旦收到可疑訊息，先確認發送者的身分

切勿從非官方渠道下載及使用WhatsApp應用程式

切勿隨意打開連結或披露個人資料

小心誤按虛假的WhatsApp網頁版

資訊及通訊科技的保安措施

資料保安建議措施 *七大建議措施一覽*

1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

下載指引

下載小冊子

資料保安建議措施

技術上及操作上的保安措施

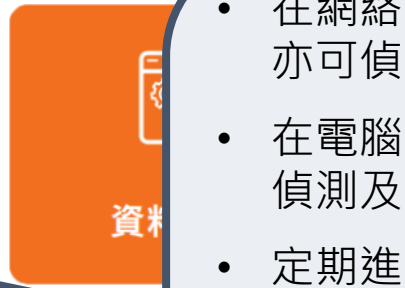
資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

- 保護電腦網絡
- 資料庫管理
- 存取管控
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 電郵及檔案傳送
- 資料備份、銷毀及匿名化

資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取足夠及有效的保安措施，以保護其控制或所持有的個人資料和資訊及通訊系統：



- 在網絡安裝**防火牆**，以防止未經許可的網絡連接，亦可偵測網絡攻擊
- 在電腦及伺服器安裝**防毒軟件**（反惡意軟件），以偵測及防止病毒及威脅
- 定期進行**保安漏洞評估**及**滲透測試**
- 使用**網站安全掃描服務**，定期掃描以偵測最新的已知或潛在的網絡安全風險
- 及時更新正在使用的系統及軟件，可以**修補保安漏洞**，減少被攻擊的機會

資料保安建議措施

資料保安事故發生後的補救措施

資料使用者在資料保安事故發生時可採取的補救措施：

- 停止並中斷連接受影響的系統
- 更改密碼或中止權限
- 更改系統配置
- 通知受影響人士並提供建議
- 通知私隱公署及其他執法或監管機構
- 修補保安漏洞
- 在可行情況下掃瞄系統
- 汲取經驗及教訓

NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料管治和資料保安措施

AI的私隱風險

風險	闡釋	例子
資料外洩 	AI系統（如聊天機械人）可能會保留大量的用戶紀錄，使其成為黑客的目標，導致潛在的資料外洩。	2023 年 3 月，ChatGPT 發生重大資料外洩事故，洩露了用戶的對話標題、姓名、電子郵件地址以及信用卡號碼的後四位數字。
資料使用 	AI模型非常先進，以至於人們難以理解他們的個人資料將如何被使用。	一些AI模型可以識別某些患者的種族，即使這不是模型的原有目的。
過度收集資料 	AI應用程式傾向收集和保留越多的數據，包括個人資料。	據報道， OpenAI在網上擷取了 3,000 億個單字來訓練ChatGPT。
資料準確性 	訓練AI模型需要大量數據。但當數據的品質和準確性參差時，AI系統就有可能提供錯誤的分析。	一家跨國公司的AI招聘系統使用有偏見的數據進行訓練，分析結果較偏向男性申請人。

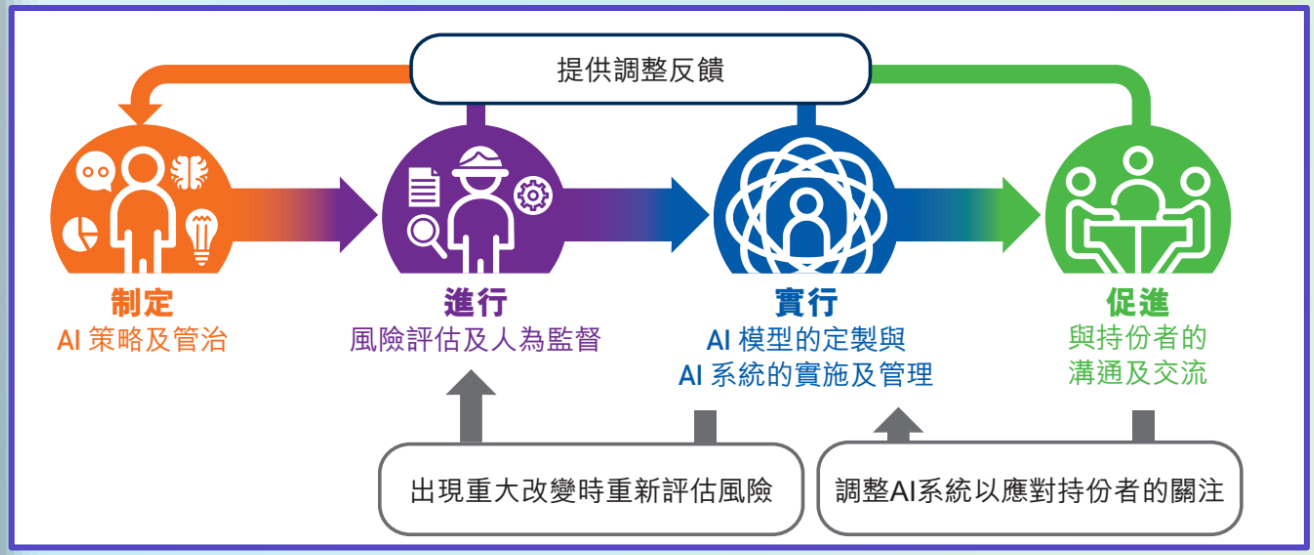
深度偽造（Deepfake）

製作詐騙影片

偽冒官員及名人

深度偽造（Deepfake）

《人工智能 (AI)：個人資料保障模範框架》



「數據安全」套餐 “Data Security” Package

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

免費名額參加研習班及講座
Free quotas to join professional workshop and seminars

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

3 保護網上個人資料

網上個人資料私隱風險

免費服務有「代價」

私隱受損

- 過度分享資訊
- 永久**數碼足跡**
- 被轉發予第三者

個人資料被濫用

- 被網絡平台及商戶「**追蹤**」
- 被第三方透過「**數據擷取**」大規模收集

身分「盜用」及騙案

- 身分被「**盜用**」作不當行為
- 被**誘騙個人資料**以作詐騙、其他犯罪活動或不當行為

謹慎使用網購平台

私隱專員公署檢視了10個本地消費者常用的網購平台的私隱設定，以了解這些網購平台收集及使用用戶個人資料的情況，並發表報告

- *Bkmall*
- *Carousell*
- *eBay*
- *Fortress*
- *HKTVmall*
- *JD.COM*
- *PlayStation App*
- *Price.com.hk*
- *Samsung*
- *Taobao*

謹慎使用網購平台

檢視結果重點（只列部分）

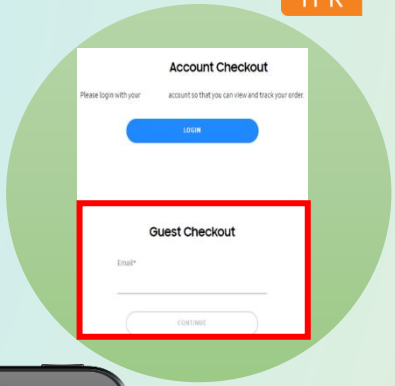
- 所有被檢視的平台都有進行**用戶追蹤**，涉及的資料包括**位置資料**、**瀏覽紀錄**、**交易紀錄**及**裝置資料**等

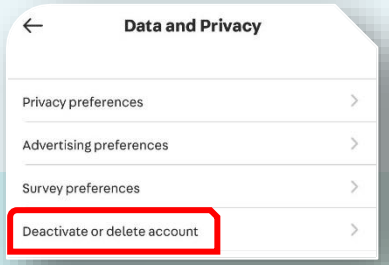
- 所有被檢視的網購平台均在私隱政策中表示會將用戶個人資料**轉移至第三方**，例如業務合作夥伴、附屬或關聯公司、廣告及促銷合作夥伴、外部服務供應商等

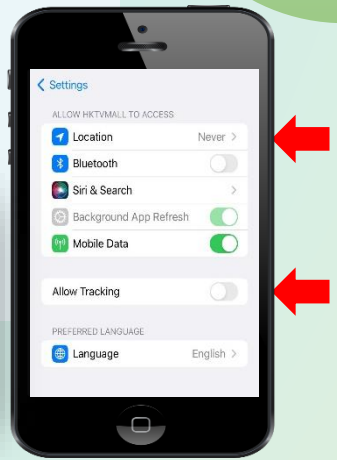
使用網購平台的保障私隱貼士

保障個人資料私隱

- 僅提供完成註冊及交易所需的**最少量資料**
- 注意有關**直接促銷**的設定
- 考慮使用**第三方支付平台**
- 閱讀**私隱政策**
- 調整**私隱設定**
- **刪除**不再使用的帳戶







使用網購平台的保障私隱貼士

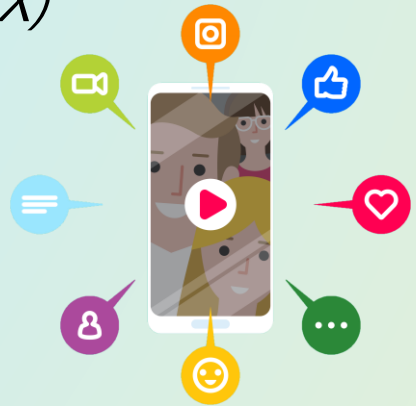
安全網購

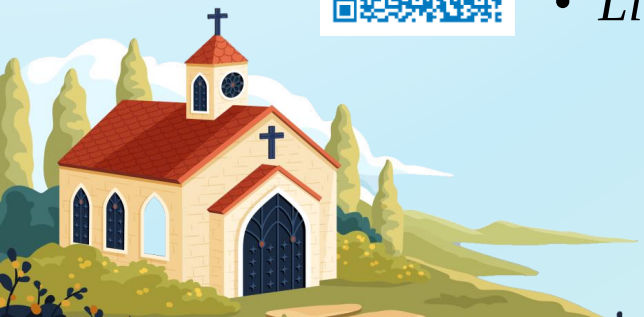
- 檢查平台的真確性
- 避免使用公眾Wi-Fi進行交易
- 使用高強度的密碼
- 點擊前先「停一停、諗一諗」
- 定期查看網上購物帳戶並報告問題

小心使用社交媒體平台

私隱專員公署檢視了香港十大最常使用的社交媒體的**私隱功能、私隱政策及私隱版面易用性**，並發表報告

- *Facebook*
- *Facebook Messenger*
- *Instagram*
- *LINE*
- *LinkedIn*
- *Skype*
- *Twitter (現為X)*
- *WeChat*
- *WhatsApp*
- *YouTube*





小心使用社交媒體平台

檢視結果重點（只列部分）

- 被檢視的社交媒體均會收集用戶的**位置資料**
- 部分社交媒體預設**公開用戶的年齡、位置、電郵地址或電話號碼等個人資料**
- 大部分被檢視的社交媒體均會**儲存用戶的信用卡資料**
- 所有社交媒體均在私隱政策中列出會將用戶個人資料**轉移到其附屬公司**
- 個別社交媒體沒有在用戶傳送訊息時採用**端對端加密**

在註冊社交媒體帳戶前

查閱私隱政策

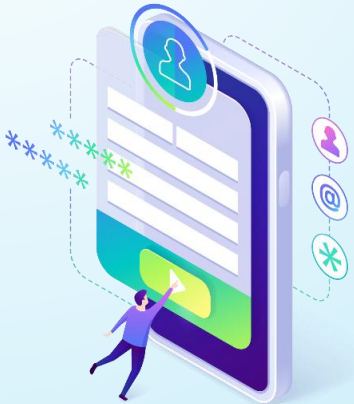
了解平台如何**處理**用戶的
個人資料

即時通訊軟件
有否提供
端對端加密

平台會否將
用戶的個人資料
分享予第三方

所分享的
資料種類和
*分享的**目的***

在註冊社交媒體帳戶前



減少提供個人資料

避免提供
敏感資料

開設專用電郵地址
作註冊之用

保障你的帳戶

設定高強度、
獨特的密碼

採用多重身份認證
功能（MFA）

完成註冊後

檢視及調整私隱設定

限制個人資料及帖文的**公開程度**

- *電郵地址*
- *電話號碼*
- *個人簡歷*

限制平台獲取的**權限**

- *臉容識別*
- *定位追蹤*
- *網上跨平台追蹤*

限制其他用戶利用你的電郵地址或電話號碼對你作出**搜尋**

使用社交媒體時

分享或發送任何資訊前應三思

限制所分享的資訊的公開程度

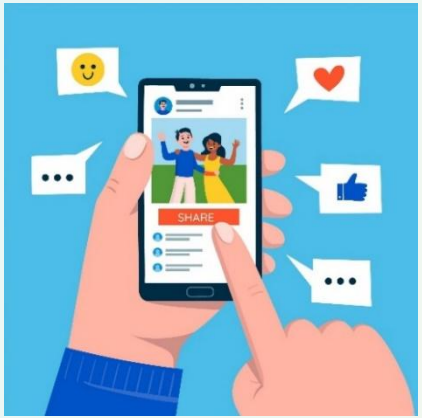
只限向朋友公開

謹慎分享位置資料：

- *住址*
- *工作地點*
- *慣常出行路線的資訊*

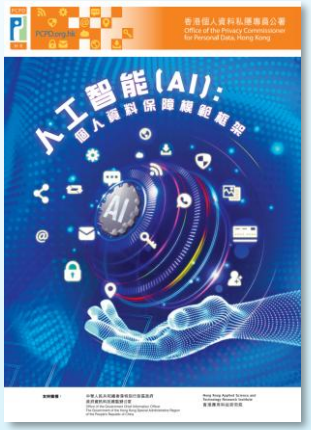
在標註或分享他人的個人資料時應謹慎

在獲得當事人的同意前不要作出分享



精明使用流動應用程式

資訊科技相關指引及報告



www.pcpd.org.hk

聯絡我們

查詢 2827 2827　傳真 2877 7026

網址 www.pcpd.org.hk

電郵 communications@pcpd.org.hk

地址 香港皇后大道東248號大新金融中心13樓1303室

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

追蹤我們最新資訊

PCPD
HK

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

謝謝！

Thank you!