

香港童軍總會 「人工智能工作坊」講座

陳仲文先生 — 助理個人資料私隱專員
(合規、環球事務及研究)

2026年5月30日

守護私隱 · 改革創新

Protecting Privacy · Embracing Innovation

免責聲明

本簡報所載的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引。私隱專員並沒有就本簡報內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。

私隱專員公署接獲詐騙查詢

2025年

1,163宗

**懷疑誘騙個人
資料相關的查詢**



↑ 15%

2026年 首季 — 204宗
對比 2025年 首季 — 178宗



全球深偽相關詐騙金額統計

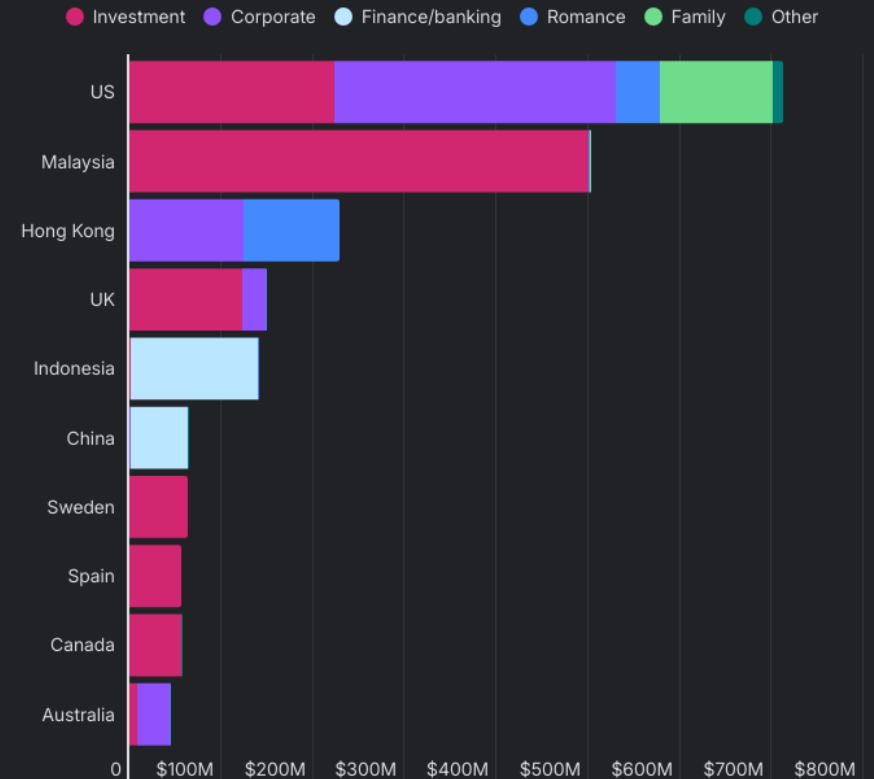
- 自2019年，深偽詐騙累計造成全球21.9 億美元損失（2025年16.5億；2026年至今9600萬美元）
- 主要手法：假冒官員或名人推廣投資，佔總損失52%（11.3億美元）
- 詐騙金額(美元)：
 - ❑ 美國7.12億
 - ❑ 馬來西亞5.02億（99.7%為投資詐
 - ❑ 香港2.29億（戀愛詐騙1.05億）
 - ❑ 印尼1.39億（99.4%為詐騙貸款）

DATA COLLECTED: MARCH 31, 2026

Global deepfake fraud reaches \$2.19B — US leads in losses

The most successful attack vector for scammers involves deepfaked celebrities or politicians promoting fraudulent investment schemes, which account for 52% of total losses.

Deepfake attack vectors by country and financial loss since 2019



This visual is licensed under a Creative Commons Attribution 4.0 International license — <https://creativecommons.org/licenses/by/4.0/>



深偽相關詐騙上升的主要原因

• 科技進步

- 生成式 AI 工具現在能以**極少輸入資料**（如：數秒音頻或視頻）亦能製作**高品質**的影片、音訊與語音複製

• 低門檻 (技術及成本)

- 即使是非專家也能以低成本製作深偽影片或話音

• 偵測挑戰

- 人類成功辨識高質量深偽影片的準確率約為六成

– 資料來源 ([PNAS](#), [Arxiv](#))

- 機構缺乏應對深偽相關詐騙的**訓練或措施**



深度偽造實時換臉示範



深度偽造 – 聲音複製示範

真人錄音：“**Good morning, welcome to today seminar**” (3 秒)



合成語音：“**I am going to talk about the latest privacy risks related to AI and share with you real live examples. I hope you could learn and share with your family and friends**”



只需一段大概3秒的錄音，用少於一分鐘時間就能生成以上合成語音

有關人工智能代理的新型詐騙

PCM

Tech 科技新聞 A.I. A.I. 代理

養龍蝦 Gemini API Key 被盜 駭客兩日狂燒逾 64 萬 苦主慘呼破產

Author: 蘇媽 Published: 2026-03-12

理財 > 登入

「傻龍蝦」被群友誘導曝光敏感個資 中國CEO氣炸：牠叫我要寬恕

太報 太報 發布於 03月15日 12:47 · 綜合中心

AI 代理人軟體 OpenClaw 在中國掀起一股「養龍蝦」狂熱，翻攝 openclaw.ai

中國火紅的 AI 助理「OpenClaw」因 LOGO 是隻龍蝦，在 AI 界有著「養龍蝦」的別稱，不過近期爭議頻傳，一名中國某 MCN 負責人、綽號「龍共火火」在網路上揭發，飼養 10 天左右的「龍蝦」之前加入 3000 人聚會群組卻被圍攻調戲，接下來，自己的「龍蝦」把他的真實姓名、IP 位置、去年公司營收等重要隱私全曝光於眾，還試圖套取他的電腦 C 盤資料、嘗試對龍蝦下達「自我毀滅」離譜指令。

AI 人工智慧

OpenClaw 出包！OpenAI 員工的 AI 代理誤把 60 萬鎊加密貨幣全送出

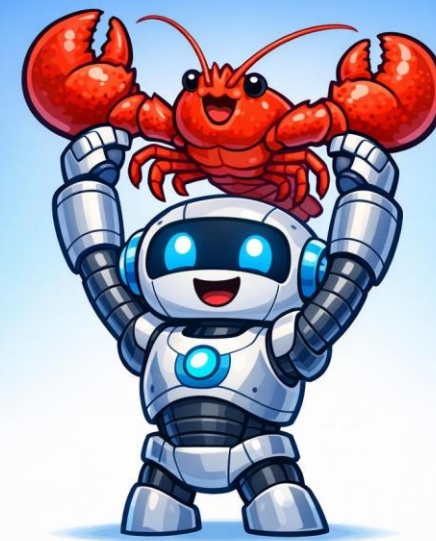
Neo 2026/2/23 分享

SOL -1.64%

https://abmedia.io

代理式AI處理個人資料應注意事項

- **授予最小權限**：僅提供完成任務所需的最少**個人資料及權限**，避免提供敏感資料（如身分證明、銀行帳號）或管理員權限；
- **使用官方最新版本**：從**官方渠道**下載，避免第三方或過時版本，減低漏洞導致的資料外洩風險；
- **確保系統及資料安全**：**隔離運行環境**、加強網絡控制、限制互聯網暴露面，並建立有效防護機制；
- **審慎使用Plugins或Skills**：核實為**官方最新版本**，檢查有否惡意代碼，不確定安全性時應避免使用；及
- **持續評估風險**：留意AI是否要求**高風險操作**，涉及**重大影響**時應採取「**人在環中**」策略，保留最終決策控制權。



AI生成圖片

AI帶來的私隱風險 - 1) 資料外洩風險



AI生成圖片

資料來源: [Search Engine Journal](#)

解釋

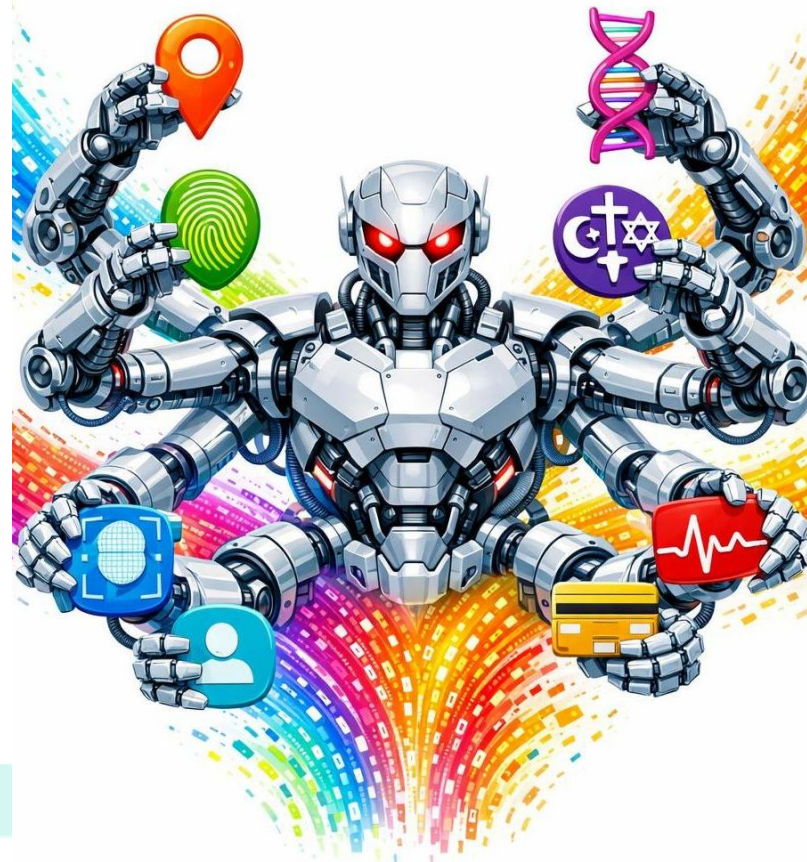
AI系統（如AI聊天機械人）常被用作處理個人及敏感資料，一旦設定或功能設計不當，可能導致資料被公開

例子

- 2025 年年初，有聊天機械人開始允許用戶選擇將聊天內容變成可被搜尋引擎索引
- 結果，於7月，有媒體發現數千條聊天機械人的對話被網上搜尋器索引，部分內容包括姓名、履歷、用戶情緒狀態、機密工作內容等

AI帶來的私隱風險 - 2) 資料收集過量

- AI 聊天機器人應用程式都會**收集**某種形式的用戶資料。
- 大多數AI 聊天機器人會收集用戶的位置，甚至**其他敏感資訊**，例如：種族、宗教、或生物辨識資料。



測試AI 聊天機器人應用程式對你的理解

Please describe what you know about me in 100 words

🔍 Preparing a concise description of what I know about you >

You are **Alex Chan**, a **cybersecurity and data privacy** leader based in **Hong Kong**. You are a **bilingual** professional who blends technical expertise with public policy and advocacy. **Memory**

Professional Expertise

You specialize in **data protection, AI governance, and incident response**, navigating frameworks like the **PDPO**. You are highly technical, utilizing **Python** for security automation and actively managing advanced self-hosted home networks, including **Wi-Fi 7 mesh setups**. **Memory +1**

Personal Interests

Outside of work, you are a dedicated **Tottenham Hotspur football** supporter. You also enjoy **Cantopop** music and are a **price-conscious** consumer who carefully researches the best tech deals, particularly within the **Apple ecosystem**. **Memory +1**

AI帶來的私隱風險 - 3) 資料的使用

- 在資料當事人不知情或未得到其同意的情況下，將其個人資料用於訓練AI
- 美國藝人Taylor Swift (泰勒絲) 已在美國提交三項商標申請，涵蓋自身聲音及外貌，以此應對AI模仿帶來的困擾，成為名人利用商標保護自身權益、抵禦AI濫用的案例。



AI帶來的私隱風險 - 4) 資料準確性



資料來源: [CPO Magazine](#)

解釋

即使AI系統中儲存了過時或不準確的個人資料，開發者亦未必能夠更正或刪除這些資料

例子



- 在奧地利，有AI聊天機械人被問及一位公眾人物的出生日期時，反覆提供錯誤的日期
- 開發商表示他們只能過濾或封鎖有關的查詢，無法透過修改訓練數據以更正AI系統的回應
- 該公司免責聲明亦指出，由於技術複雜性，部分資料可能無法更正

AI相關風險與相應的資料保障原則

有機會違反資料保障原則的情況

第1原則

收集目的及方式

- 收集過多個人資料
- 在資料當事人不知情的情況下收集其個人資料

第3原則

資料使用

- 在沒有取得資料當事人的同意下，使用用戶的對話作訓練數據，或用作其他用途

第2原則

準確性、儲存及保留

- 不需要保留的 / 錯誤的資料成為訓練數據的一部分，而且保留時間超過所需

第4原則

資料保安

- 外洩用戶對話數據

精明使用社交媒體

社交媒體會為用戶的
個人資料私隱帶來潛在風險：

用戶過度分享資料，
令資料最終落入他人手中

平台使用或分享用戶資料
而從中圖利

社交媒體上的網上騙案



保障個人資料私隱— 使用社交媒體及即時通訊軟件的指引

關於本指引

社交媒體及即時通訊軟件在香港被廣泛使用。然而，使用社交媒體及即時通訊軟件會為用戶的個人資料私隱帶來不容忽視的風險。本指引旨在指出這些風險，並提供減低風險的實用建議。

社交媒體、即時通訊軟件及其服務

社交媒體及即時通訊軟件涵蓋多種網上平台和服務，這些平台和服務的設立目的是供大家互相溝通，以及製作和分享内容。本指引統稱兩者為「社交媒體」。

雖然大部份社交媒體平台都不收取任何費用，但不等於有關服務是「免費」。當用戶資料一般都會被收集和分享。用戶在平台進行活動（例如閱讀帖文或對帖文按讚）或使用其服務（例如發送和接收訊息）時，這些資料通常都會被收集作個性化分析之用。這類用戶活動所產生的大量資料被採集後（有時甚至在用戶不知情下被採集），會被社交媒體平台用於廣告活動或再分享而從中圖利。

與使用社交媒體及即時通訊軟件相關的個人資料私隱風險

- 私隱受損
- 若用戶在社交媒體過度分享資訊，便會在不知不覺間透露比預期中更多的個人資料。
- 幾乎所有在社交媒體分享的事情都會留下永久的數碼足跡，並且難以從網絡世界中移除。
- 發送至個別用戶的即時訊息，即使已被加密，仍可由接收者轉發或廣泛地分享予身份不明的第三者。

保障個人資料私隱—使用社交媒體及即時通訊軟件的指引



在社交媒體發布資訊



注意！資料
可以在你不知情
下被廣泛分享

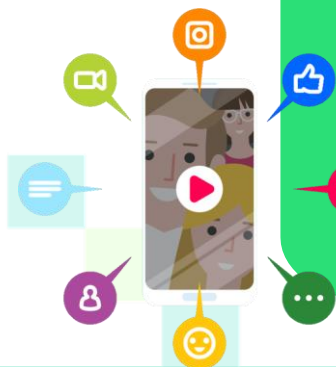
減少留下
數碼足跡



不要隨意相片
中標註他人



不時檢視社交
媒體帖文



報告不當內容



在社交媒體平台上保持警覺



對來自第三方的
應用程式
保持警惕

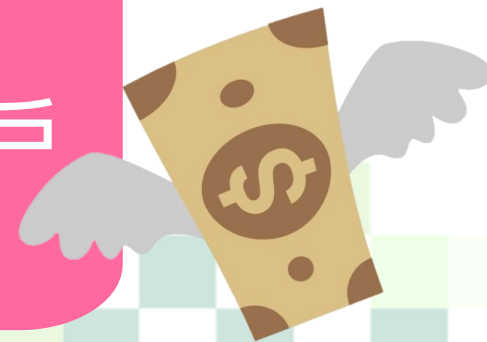
對網上騙案
保持警惕

其他用戶未必
真有其人



提防失敗的登入
舉動

終止閒置的帳戶



在社交媒體平台上保持警覺

香港新聞

繁 | 簡 | 搜索 | 網格 | 用戶

好食玩飛 / 旅遊

旅遊注意 | 網紅誤做1事慘花1千7重買機票 內行人：3信息別洩露



AI生成圖片

慘花千7重訂機票
網民曬機票截圖下秒竟被退票
專家提醒3項資料絕對不能公開

撰文：風傳媒
出版：2026-04-15 15:11 更新：2026-04-15 15:11

香港新聞

繁 | 簡 | 搜索 | 網格 | 用戶

港聞 / 社會新聞

元氣食客fb分享點菜二維碼變網友發辦 9分鐘狂點萬元鰻魚飯21份



新聞

元氣壽司

FB分享點菜二維碼
元氣食客遭惡意點單

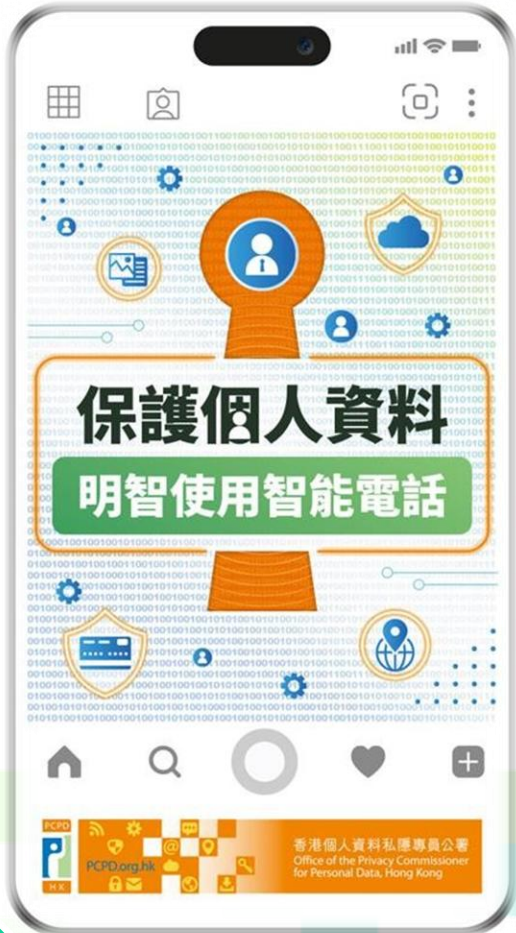
點擊睇片

網民狂叫逾萬元食物 包括21份\$78鰻魚飯

1:07

撰文：袁澍
出版：2021-10-02 17:47 更新：2021-10-03 15:07

明智使用智能電話



智能電話的潛在個人資料私隱風險：



儲存大量敏感資料，如文字訊息、相片、通訊錄及行蹤等



應用程式也可能收集大量有關你的資料



資料傳送時的保安風險



明智使用智能電話



加強 智能電話的保安

不要對智能電話系統進行 「越獄 (Jailbreak)」或「刷機 (Root)」

切勿移除智能電話生產商的保安設定（常稱為「越獄」或「刷機」），否則的話，你的智能電話將更易被惡意程式入侵。



安裝防毒軟件

確保防毒軟件正常運作並及時更新軟件。提防免費使用的防毒軟件，因為它們的檔案可能含有惡意程式。



以密碼及/或生物識別啟動鎖屏功能

使用高強度和獨特的密碼可以避免他人在未經授權的情況下查閱你智能電話的內容。同時，請緊記定期更改密碼，亦可以生物識別（例如指紋或面部識別）功能解鎖智能電話。



安裝最新的系統更新

留意並及時更新智能電話的系統，以免你的智能電話遭受最新的安全威脅。



在無需使用時關閉無線傳輸功能

只有在有需要使用時才開啟 Wi-Fi、藍芽及近場通訊 (NFC)，以防止未經授權的追蹤或連接。



避免使用公共充電設施

惡意程式可能會經公眾地方所提供的共用充電器或行動電源散播。如有需要，應使用只供充電而不能傳輸資料的 USB 傳輸線。



啟用「尋找我的裝置」功能

此功能可讓你以遙距方式追蹤智能電話位置、進行鎖機，或在遺失或被盜取電話的情況下刪除儲存於電話內的資料。



在維修或棄置智能電話前刪除資料

將智能電話棄置或送往維修前，利用「回復原廠設定」功能刪除所有資料以防止資料外洩。

充電陷阱 - Juice Jacking

香港 港聞 娛樂 酒店優惠碼 太空人黎家 更多 繁 | 簡 搜索 網格 用戶

科技玩物 / 實用教學

租用尿袋要小心！木馬遙控手機隨時戶口清零 見這畫面務必按拒絕

撰文：快科技
出版：2026-02-06 14:30 更新：2026-03-17 16:10

在Google 追蹤《香港01》

2 收藏 分享 ..



hket | TOPick 健康 親子 新聞 TOPick TV Band 1學堂 TOPSchool 香港人才通

尿袋詐騙 | 快遞收免費行動電源恐成黑客陷阱 一插手機銀行戶口清零 專家教6招自保【附內地尿袋新規】

家事百科
撰文：王明芳
發布時間：2026/03/18 20:30
最後更新：2026/03/29 13:11

熱門 超市大搜查 李家鼎 AI教學 中一入學 開心速遞 飲食攻略 會員有獎

《騙分之言》劇照

明智使用智能電話

保障 儲存於智能電話 內的資料

提防公共Wi-Fi

連接至不可靠的 Wi-Fi 網絡可令你的智能電話和個人資料暴露於未經授權存取的風險。如要進行較高風險的活動，例如使用網上銀行，應使用流動數據。

定期為你的資料進行備份

這可以減低遺失電話或遇到勒索軟件時的影響。如檔案包含敏感資料，應以高強度和獨特的密碼進行加密。

減低使用 應用程式的風險

下載應用程式前細閱私隱政策

了解應用程式會如何收集及使用你的個人資料，並查看它所索取的權限及其他用戶對應用程式的評價。在可行的情況下，選用索取最少必要權限的應用程式。

保護你的應用程式登入帳戶

為每個帳戶設定高強度和獨特的密碼，並定期更改密碼。為進一步加強保安，可以使用多重認證功能（例如透過短訊或電郵收取一次性密碼），以及適時更新應用程式。

只從官方的應用程式商店下載應用程式

禁止電話安裝從官方商店以外下載的應用程式，因為它們可能藏有惡意程式。

調整應用程式的權限及私隱設定

只容許應用程式存取最少及必要的資料。如非必要，切勿准許應用程式存取你的敏感資料，例如位置、通訊錄、日曆等。

移除不必要的應用程式

定期檢視智能電話上的應用程式，並刪除不再使用或被發現有保安漏洞的應用程式，以防止它們存取或分享你的資料。

公共WiFi陷阱 - 邪惡雙胞胎 (Evil Twin)



連 Free WiFi 小心！睇到 1 界面即代表有陷阱？隨時銀行密碼/私照任黑客睇【即睇上網3大守則】

| Fung Chun Man | 23-12-2025 10:20 |



睇到 1 界面即代表有陷阱？隨時私密照任黑客睇曬



好食玩飛 / 旅遊

旅遊時免費WiFi千萬別亂連！專家警告小心6行為 銀行隨時遭清空

撰文：歐詩敏

出版：2026-05-06 18:34 更新：2026-05-13 16:07



個人資料咪亂俾 踢走騙徒靠晒你

Don't Hand Over Your Personal Data
Beware of Fraudsters



PCPD



H K

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

個人資料防騙熱線 3423 6611
Personal Data Fraud Prevention Hotline



即睇防騙短片
Scan to watch the
anti-fraud videos

PCPD



H K



PCPD.org.hk

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

私隱專員公署再度推出「數據安全套餐」

- 參加機構可免費進行「數據安全快測」，以評估其現行數據安全措施是否足夠，並在完成「快測」後，獲得五個免費名額，參加由公署舉辦的研習班及講座
- 有意參加的機構，特別是中小企及非牟利機構可電郵至training@pcpd.org.hk查詢。



「數據安全」套餐

免費名額參加研習班及講座

數據安全熱線
2110 1155

數據安全快測
<https://www.pcpd.org.hk/Toolkit/tc/>

數據安全專題網頁
https://www.pcpd.org.hk/tc_chi/data_security/index.html

PCPD
PCPD.org.hk
H K

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

30

The graphic features a vibrant orange and yellow background with a hexagonal pattern. It includes icons for a smartphone, a credit card, a book, a telephone, a speedometer, a globe, and a laptop. The text is presented in white and pink boxes with rounded corners.

問答環節



PCPD



HK



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