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

SocTech Symposium 2025
社創及科技研討會 2025

生成式AI時代的私隱保障新里程

鍾麗玲
個人資料私隱專員

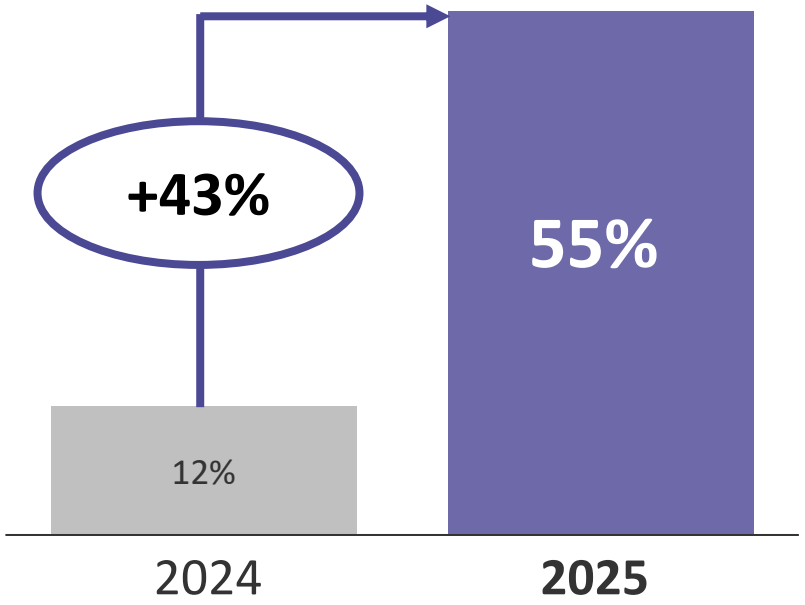
2025年10月20日

統計
AI使用越來越廣泛，機構關注數據安全

世界各地使用AI的非牟利機構數量急升

經常使用或正在試用AI的非牟利機構

1,229家非牟利機構

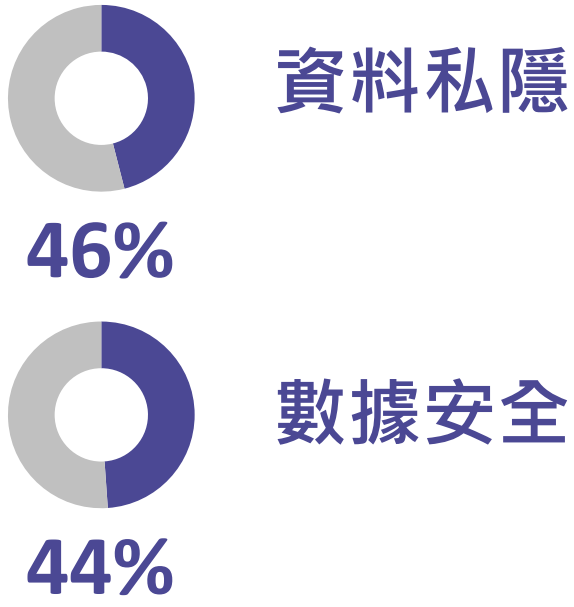


資料來源： Salesforce

非牟利機構對AI的最大關注與數據有關

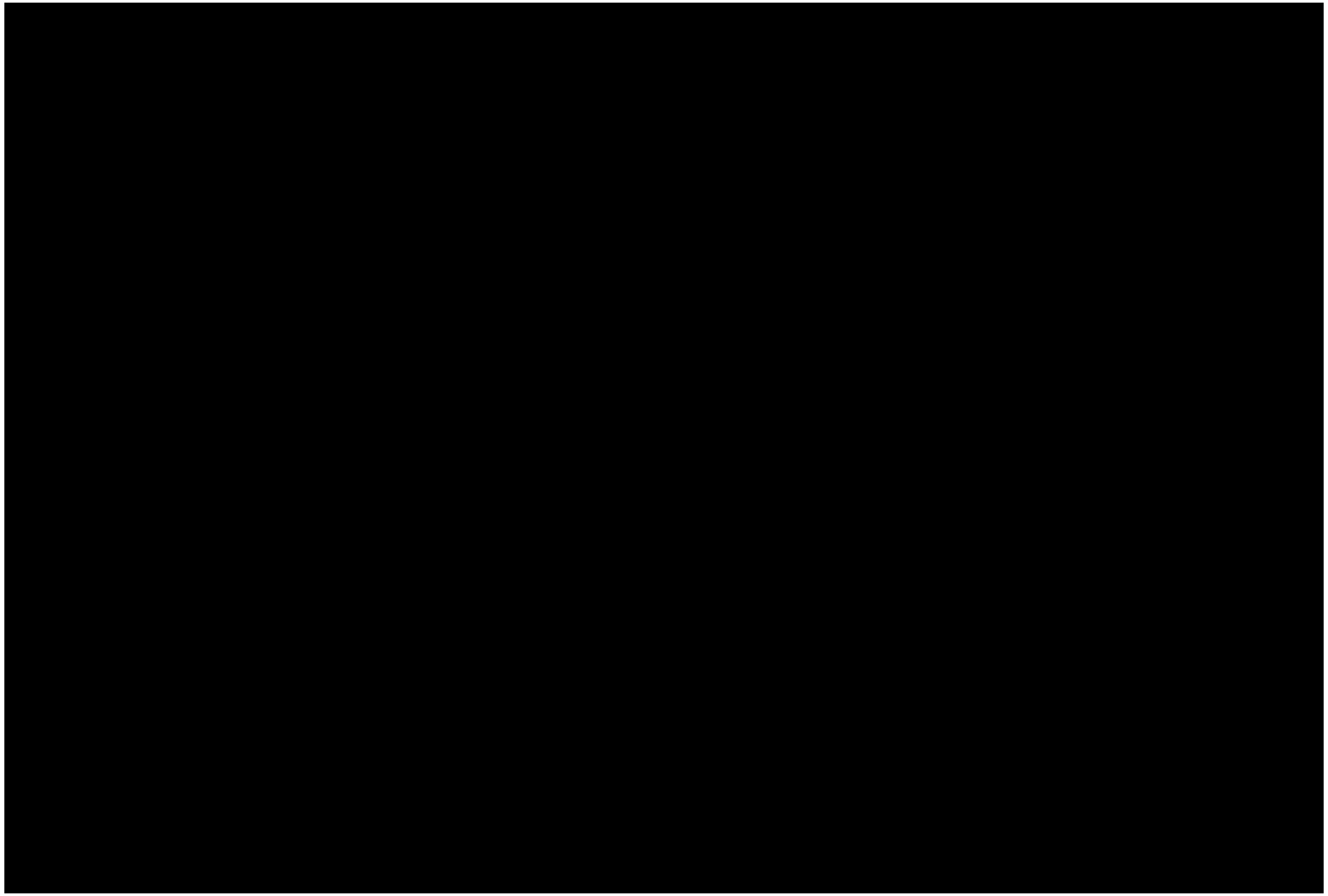
對AI的最大關注

1,229家非牟利機構



資料來源： Salesforce

眼見未為真？
製作深偽影片已非難事



風險
使用AI可能對個人資料私隱構成多重風險

風險	解釋	例子
資料外洩	如果用戶輸入個人資料至AI聊天機械人，該資料**可能被轉移至服務供應商**，繼而構成資料外洩風險	**荷蘭某診所**一名僱員被發現在沒有合理理由下，將**極為敏感的病人醫療資料輸入至AI聊天機械人，侵犯病人的私隱權**
資料收集過量	AI傾向**收集和保留盡可能多的數據**，包括個人資料	**某AI開發商被指從網上擷取了3,000億個詞彙**作模型訓練
資料的使用	AI開發者可能會在**資料當事人不知情或未給予同意**的情況下，**使用其個人資料訓練AI系統**	某**科技公司使用160萬名病人的醫療紀錄訓練AI模型**，而未事先取得病人的同意或提供任何「退出」的選項
資料準確性	即使AI系統包含**過時或不準確的個人資料**，開發者亦**未必能夠改正或刪除這些資料**	某AI聊天機械人**反複地提供錯誤的某位公眾人物的出生日期**，而開發者表示他們**無法**透過修改訓練數據**改正輸出結果**。

資料來源：AP; Fortune; ICO, BBC; CPO Magazine

AI事故
負責保護兒童的社工使用AI聊天機械人導致嚴重問題

AI ban ordered after child protection worker used ChatGPT in Victorian court case

Investigation finds staffer's report referred to doll allegedly used by father for 'sexual purposes' as 'age-appropriate toy'

- Follow our Australia news live blog for latest updates
- Get our breaking news email, free app or daily news podcast

資料來源： The Guardian; 澳洲維多利亞省資訊專員辦公室

事故詳情

澳洲維多利亞省一名負責保護兒童的社工向法庭呈交一份由AI生成的報告

- 涉案**兒童的父母因性罪行被起訴**
- 該對父母、照顧者及兒童的**個人資料被輸入**至AI聊天機械人

相關資料保障機構發現以下違規行為：

- **未經授權披露**個人資料
- 呈交法庭的報告載有**不準確**的個人資料

《僱員使用生成式AI的指引清單》

🎯 目的

協助機構制定僱員在工作時使用生成式AI的內部政策或指引，以及遵從《私隱條例》有關處理個人資料的相關規定

✨ 特色

以清單形式呈現

作為良好的行事方式，機構可以制定與其價值觀及使命一致的內部政策或指引

僱員使用生成式AI的政策或指引的建議內容

01 範圍

02 保障個人資料私隱

03 合法及合乎道德的使用及預防偏見

04 數據安全

05 違反政策或指引

01 範圍

範圍	內容
獲准使用的工具	**清晰訂明機構內准許使用的生成式AI工具及應用程式**，例如： • 公眾可用的AI工具或應用程式 • 內部開發的AI工具或應用程式
獲准許的用途	**清晰指明僱員可以使用生成式AI工具處理甚麼工作或活動**，例如： • 起草 • 總結資訊 • 生成文本、音頻及／或視像內容
政策適用性	訂明政策是否適用於**整個機構**；**指定部門**；**指定職級**；及／或**指定僱員**

02 保障個人資料私隱

獲准輸入的資訊種類及數量

提供清晰指示，說明：

✓ **可輸入至生成式AI工具的資訊種類及數量**

✘ **禁止輸入的資訊種類**

輸出資訊的獲准許用途

提供清晰指示，說明生成式AI工具所生成的資訊（包括個人資料）的**獲准許用途**，以及僱員應否、何時及如何在進一步使用這些個人資料前將其匿名化

輸出資訊的獲准許儲存方式

要求僱員根據機構的**資訊管理政策**儲存資訊和**資料保留政策**刪除生成式AI工具所生成的資訊

遵從其他相關內部政策

確保**使用生成式AI的政策與機構的其他相關內部政策一致**

03 合法及合乎道德的使用及預防偏見

違法行為	強調僱員有責任擔當審查員

清晰訂明僱員不能為進行非法或有害的活動使用生成式AI工具

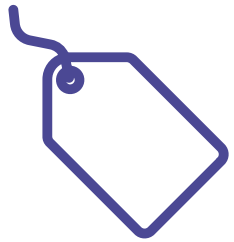
準確度及核實

強調僱員需要**核實AI所提供的資訊**

預防偏見及歧視

提醒僱員AI生成的結果可能帶有**偏見及歧視**

訂明**更正及報告機制**



加上水印 / 標籤

提供清晰指引，說明應**何時及如何**在AI生成結果上**加上水印或標籤**

04

數據安全

獲准許裝置

訂明准許僱員可用**哪些裝置**來**取用生成式AI工具**

保安設定

要求僱員保持**嚴格的保安設定**

獲准許使用者

訂明**可以使用**生成式AI工具的**僱員**

AI事故及資料外洩事故應變

要求僱員根據機構的**AI事故應變計劃報告AI事故**

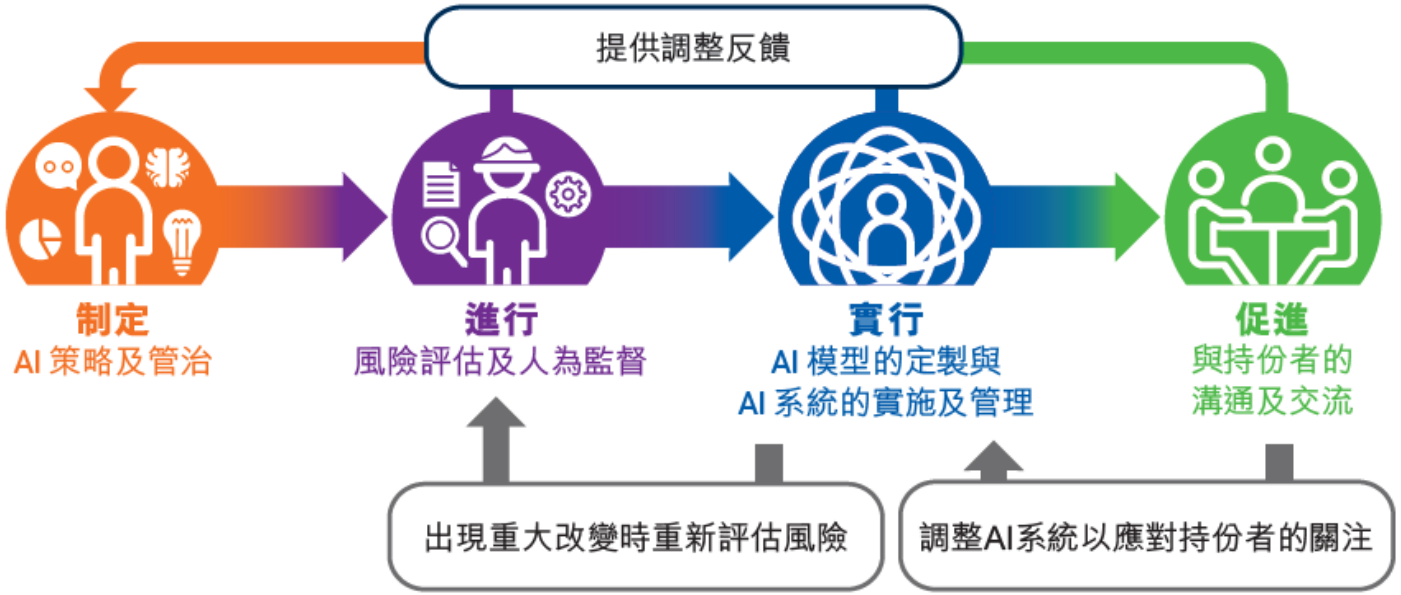
用戶憑證

要求僱員使用**獨特且高強度的密碼**及**多重認證**

《人工智能 (AI): 個人資料保障模範框架》

ⓘ 協助機構遵從《私隱條例》的規定

向採購、實施及使用任何種類的AI系統（包括生成式AI）的機構，就保障個人資料私隱方面提供有關AI管治的建議及最佳行事常規



聯絡我們

人工智能安全
專題網頁

AI安全熱線
2110 1155

保障、尊重個人資料私隱
Protect, Respect Personal Data Privacy

追蹤我們
最新資訊