

私隱專員公署推出AI《模範框架》 促進人工智能安全

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

隨着人工智能（AI）在各行各業的應用越趨廣泛，不少企業已開始採用AI技術以提升生產力或業務板塊。然而，許多企業對於應如何妥善使用或管理AI存有疑問。個人資料私隱專員公署（私隱專員公署）聯同香港生產力促進局於去年進行的調查發現，只有四成受訪企業已就使用生成式AI制定內部指引。

面對人工智能帶來的潛在風險，人工智能安全不容忽視。國家去年10月發布的《全球人工智能治理倡議》也強調各國都應秉持發展與安全並重的原則。事實上，人工智能安全乃國家安全的重點領域之一，日前第二十屆三中全會通過的《中共中央關於進一步全面深化改革 推進中國式現代化的決定》亦提到要建立人工智能安全監管制度，推進國家安全體系和能力現代化。

個人資料私隱專員（私隱專員）鍾麗玲表示：「為應對AI對個人資料私隱帶來的風險，並體現國家的《全球人工智能治理倡議》，私隱專員公署於6月發布了《人工智能（AI）：個人資料保障模範框架》（《模範框架》），幫助機構在採購、實施及使用AI時遵從《個人資料（私隱）條例》的相關規定，妥善保障市民的個人資料私隱。我相信《模範框架》將有助孕育AI在香港的健康發展，促進香港成為創新科技樞紐，並推動香港以至大灣區的數字經濟發展。」

《模範框架》建基於一般業務流程，提供國際認可及切實可行的建議和最佳行事常規，《模範框架》涵蓋以下四個範疇：（一）制定AI策略及管治架構；（二）進行風險評估及人為監督；（三）實行AI模型的定製與AI系統的實施及管理；以及（四）促

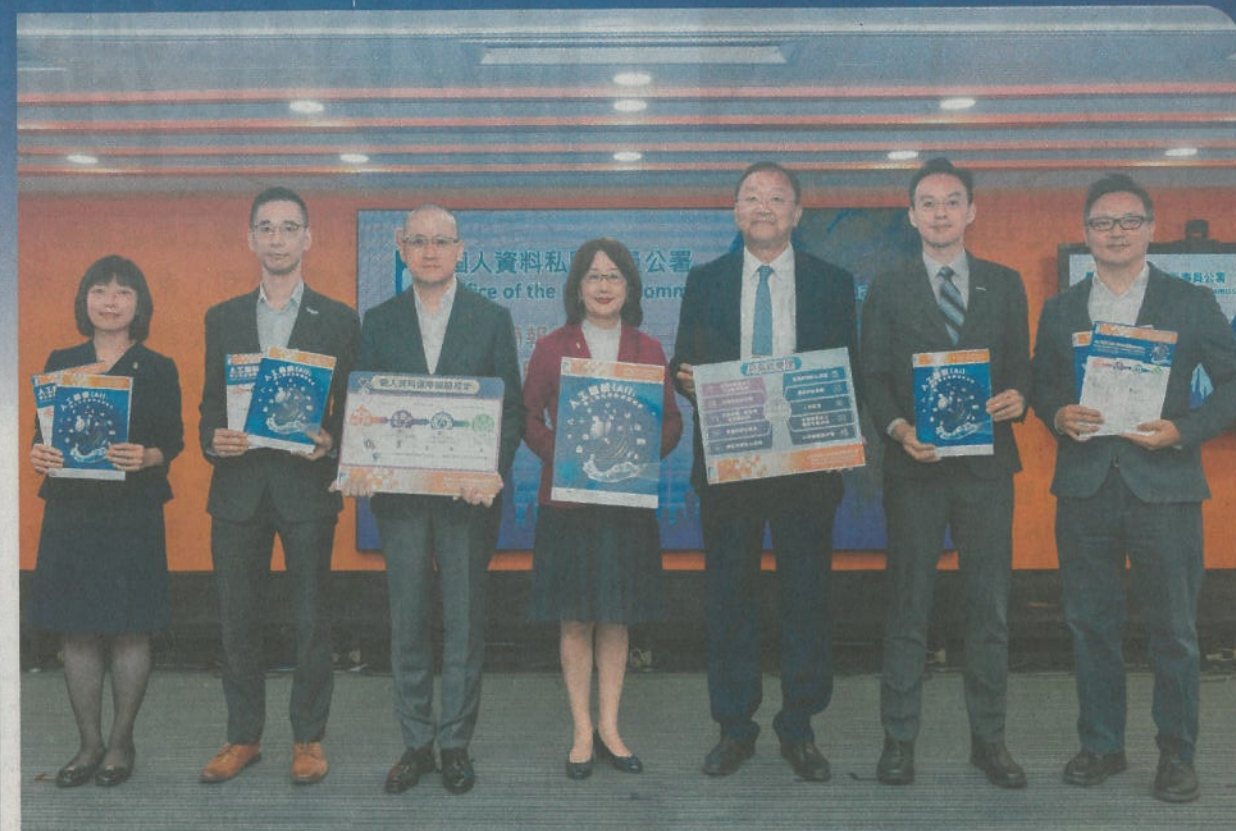
個人資料私隱專員公署
Office of the Privacy Commissioner傳媒簡報會
Media Briefing

■私隱專員鍾麗玲發布《人工智能（AI）：個人資料保障模範框架》。

進與持份者的溝通及交流。有見不同機構應用AI的目的、方式各異，《模範框架》建議機構以「風險為本」的方式管理AI，根據相關AI系統的風險程度而採取相應的風險緩減措施，包括決定人為監督的程度。

舉辦研討會助業界應用 《模範框架》

為協助業界進一步理解及應用《模範框架》，私隱專員公署已於7月30日舉辦「人工智能與私隱保障：發展與安全並重」研討會。企業對是次研討會反應相當熱烈，共有



■私隱專員公署發布的《模範框架》獲政府資訊科技總監辦公室（資科辦）（現稱數字政策辦公室）及香港應用科技研究院（應科院）的支持。圖為私隱專員鍾麗玲（中）與資科辦及應科院代表及公署科技發展常務委員會成員合照。

接近1000人參加。

小領袖 大智慧 共創AI未來

為培育中學生踏進AI新世紀，公署今年亦舉辦了「AI新世代保障私隱領袖培訓計劃」，以「小領袖 大智慧 共創AI未來」為主題，舉辦不同活動，包括個人資料私隱管理專題講座、與保障資料主任進行交流，以及於7月23日舉辦的AI實踐工作坊，特別安排100位中學生參觀Microsoft微軟香港總部，讓學生透過專題講座及AI互動遊戲，認識AI的私隱風險及負責任地使用AI。



■中學生透過互動遊戲了解AI的私隱風險。



■私隱專員鍾麗玲（左六）及微軟香港的代表與參加AI實踐工作坊的同學合照。

《模範框架》



了解更多

《模範框架》懶人包



了解更多

（資料由客戶提供）