大公報
2025年4月7日 星期一

私隱署《指引》助企業實施內部規範

僱主須訂AI政策 減資料外洩風險

►在國際創科展上，參觀者在香港生成式人工智能研發中心展館體驗AI成像。

個人資料私隱專員公署於3月31日發表《僱員使用生成式AI的指引清單》，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》的相關規定。個人資料私隱專員鍾麗玲昨日表示，如今生成式AI愈來愈普及，期望清單協助企業制定內部政策，讓員工能更安全使用。

有立法會議員相信，有關政策有助企業在數碼轉型中保障市民私隱，防止無意間洩露客戶私隱或營運資料。

大公報記者
義昊、黃鈺淼

▲鍾麗玲表示，公署發指引協助企業制定內部政策，讓員工能更安全使用生成式AI。

鍾麗玲昨日出席電台節目時指出，現時生成式AI十分普及，但僱主未必知道員工的使用方式，期望清單協助企業制定內部政策，讓員工能更安全使用，釋放AI最大威力。她再提醒有關機構輸入顧客資料，會受私隱條例規管，如果涉及改變用途目的，需要取得客戶同意。

業界盼公署提供政策樣本

是次《指引》涵蓋五大範疇，分別是使用AI的範圍、保障個人資料私隱、要合法和合乎道德使用避免偏見、數據安全以及違反指引的後果。鍾麗玲形容僱主可以「執藥咁執」，按各範疇了解什麼資料可以輸入，制訂適合的內部政策。鍾麗玲表示，《指引》推出數日後，有業界反映希望公署製作內部政策的樣本，署方會考慮制訂樣本予機構參考，而公署設有AI安全熱線，讓企業查詢問題，亦有度身訂造的培訓課程，亦會在今年6月與生產力促進局舉辦AI安全研討會，幫助業界了解如何讓機構安全地使用AI工具。

至於AI可能造成的風險，鍾麗玲表示，最關注個人資料私隱風險，尤其是資料的使用，例如員工將收集到的客戶資料悄悄用於訓練AI；其次是員工輸入一些公司不允許的敏感機密資料。再者是關注資料外洩問題，因為訓練AI通常需要大量數據，如果發生外洩事故，後果可以相當嚴重。

鍾麗玲強調，公署絕對有權力介入AI人工智能的合規使用，若收到資料外洩事故，會發表報告及公開譴責機構，以及發出執行通知，若機構違反執行通知屬刑事罪行。另外，公署每年也會主動做循規審查，每年大概做400宗，收到約200多宗數據安全投訴，公署會進行調解及調查的工作。不過，公署希望未發生事件前就做好預防，因此希望市民大眾「不要成日當我哋係老虎，唔係吓吓要咬人，很多時候我哋都會做很多教育、推廣的工作。」

應設定各級員工使用權限

立法會資訊科技委員會主席葛珮帆認同私隱專員提出訂立AI政策的建議，相信這有助企業在數碼轉型中保障市民私隱。她說，員工使用AI工具，例如上載資料生成表格確實可能無意間洩露客戶私隱或營運資料，因此建議企業採取以下措施，包括禁止員工將敏感資料，尤其涉及客戶或員工的個人資料輸入公開AI平台，改用內部部署或經認證的企業級工具；設定各級員工AI使用權限，並記錄操作日誌供定期稽核；加強員工使用AI保護個人私隱的意識教育，例如辨識AI回覆可能夾帶的第三方資料，必須小心核查及使用。

立法會議員、商湯科技戰略顧問尚海龍認為，生成式人工智能已經在相當多的工作中有了實際應用，例如數據挖掘、海報製作、數字人營銷、創意視頻等等，對許多工作大有幫助，但相關弊端也存在，例如模型選用仍有門檻、各種市場上的開源模型均有不同程度的歧視如性別歧視、被開源模型訓練後的數據洩露風險。他贊同私隱專員公署幫助廣大中小企制定普適性的AI內部員工守則，以標準化附件或LEGO式選擇的方案，協助更新員工合約或關鍵崗位指引。

▲企業僱員使用AI安全政策，有助企業在數碼轉型中保障市民私隱，防止無意間洩露客戶私隱或營運資料。

香港常見AI工具及使用風險

聊天機器人
- 如果沒有使用加密等方式保護客戶資料，存在資料盜竊的風險，資料也可能遭竄改
- 黑客可假冒聊天機器人與客戶互動，誘導客戶提供私人資料

光學字符識別
- 在財務和醫療場景中，或存在金額小數點位置錯誤，藥物劑量的誤讀等情況
- 特定文字模式可能會觸發模型的非預期行為，造成資料意外污染

文字／圖像／影片／語音生成器
- AI模型不能眞正理解用戶指令的含義，或數據未及時更新，給出錯誤信息
- 生成圖像／影片的透視、光影效果與現實生活不符
- 風格與知名藝術作品相似，或引發版權爭議

語音轉問題工具
- 對專有名詞、內部職位簡稱或行業術語的轉錄不夠精確
- 處理強烈口音時誤差較大

《僱員使用生成式AI的指引清單》內容

- **獲准使用的AI工具和用途：明確指定可使用的生成式AI工具（包括公眾可用及內部開發的工具），以及允許的用途，如起草文件或總結資訊。**
- **個人資料保護：提供清晰指示，說明可輸入的資訊種類和數量，特別是涉及個人資料時須格外謹慎。**
- **合法使用和預防偏見：僱員不得利用AI進行非法或有害活動，需校對和查核AI生成結果的準確性。**
- **數據安全：規定可使用的裝置、授權使用AI的員工類別，並強調保安設定和事故報告的重要性。**

應用廣泛 引發版權及私隱爭議

隱患頻生

生成式AI的應用場景愈來愈廣泛，其背後引發的版權、私隱外洩等問題日益凸顯。為防止私隱經AI外洩，不少行業已着手訂立相關規定。有教育界人士呼籲將如何正確使用AI、保護個人私隱等內容滲透進中小學教育中。

冀學校教授AI正確應用

OpenAI在3月26日推出AI生成圖像功能，可以把任何照片轉換成不同動畫風格的圖片，吸引了全世界網民在社交網站貼出相關作品。然而，這股潮流也掀起關於版權、創作等問題的不少爭議，而OpenAI過去已有不少未經授權使用素材的爭議和官司。2023年底，《紐約時報》向OpenAI發起版權訴訟，索賠金額高達數十億美元，《紐約時報》指控OpenAI偷竊了其內容訓練數據，甚至原封不動把本應付費才能閱讀的內容提供給用戶。

◄《紐約時報》2023年底向OpenAI提出版權訴訟，指控OpenAI原封不動把付費才能閱讀的內容提供給用戶，索賠數十億美元。

立法會議員、香港中文大學工程學院副院長（外務）黃錦輝表示，學校十分注重研究與私隱的關係，要求教師在申請項目時申報是否涉及使用非公開數據並提供詳細說明；知識產權相關教育更是中大學生的必修課。但他強調，隨着AI的普及，青少年出於好奇與AI互動或無意洩漏私隱，因此希望將如何正確使用AI、保護個人私隱等內容滲透進中小學教育中。

廣告集團The Bees行政總裁曾錦強向《大公報》表示，目前業界使用AI製作廣告的情況並不普及，公司主要利用AI生成效果圖，向客戶展示廣告效果，但最終成品依然是在現場拍攝，並進行後期製作。為保護私隱，公司禁止使用客戶提供的資料訓練AI，所以目前應該不存在客戶或公司數據經AI洩漏的情況，但依然會參考私隱專員的指引，訂立相關規定。

大公報記者 義昊

◄►OpenAI早前推出AI生成圖像功能，可以把照片轉換成不同動畫風格的圖片，網上湧現大量「吉卜力風格」的圖片，引起版權爭議。左圖為AI《毒舌大狀》電影劇照中的黃子華；右圖為AI《飯戲攻心》電影劇照中的林明禎。

何永賢談昔日制水苦況 籲飲水思源

【大公報訊】記者黃知行報道：房屋局局長何永賢昨日在社交網站以「城市生命線　感恩點滴」為題撰文，表示近日與房屋局同事到添馬公園的「舞動水滴展」打卡，一起慶祝東江水供港60周年。她指出，在社會各界感恩這道「城市生命線」的時候，年輕一輩也逐漸了解當年香港制水之苦。

何永賢提到，香港儲水最緊絀時，四天才有一次四小時的供水，作為最基本又最缺乏的資源，不論是市民生活或是商業活動都嚴重受限。今日香港「水源充足」，城市潔淨又煥發活力，一點一滴都來之不易，感恩國家「要高山低頭，令河水倒流」的決心，築建輸水路線，一直默默支持香港，佔全香港的食水用量七成至八成，可見這道生命線的重要。

何永賢早前與副局長戴尚誠，聯同多位同事到「舞動水滴展」，在水滴裝置前打卡。她憶述母親以前常常提到其胞兄出生時會因為制水而無水幫哥哥洗尿布的苦日子。有水供應時，什麼器皿都會用來裝水，先為還是嬰兒的哥哥洗澡，同一盆水，再到媽媽洗澡，然後再用來洗尿布，相信今時今日的年輕人都覺得難以想像。她表示，對比今天打開水龍頭便有源源不絕的供水，大家更要飲水思源，不負國家的支持，為香港的發展努力。

她又表示，歡迎市民一起前往參觀，親身參與東江水供港60周年的重要時刻，並提提大家，參觀市民需在活動網頁預先登記，每人每日只可登記一個場次。

▲何永賢早前與房屋局同事到添馬公園的「舞動水滴展」打卡。

學童長時間上網增壓力 學者倡設時限

【大公報訊】記者賴振雄報道：衞生署早前發表報告，超過六成中、小學生，每日最少兩小時使用電子屏幕產品作娛樂用途。有學者表示，多項研究顯示，本港學童上網娛樂時間日益增加，有可能遭受網上欺凌或接收不合適資訊，影響身心發展，青少年把事情上載至社交平台分享受別人的品評，也可能引起精神壓力問題，建議仿效其他地區，研究為學童上網時間設限。

香港大學賽馬會防止自殺研究中心總監葉兆輝指出，本地或海外研究顯示，若青少年使用互聯網時間越長，精神健康越差，焦慮、抑鬱等精神問題相對較多，認為或可以透過適當規限，教導青少年不要長時間上網。

他認為，內地已為使用電子產品時間設上限，建議特區政府仿效，若企業出品的遊戲軟件產品有意使人沉迷，明知會產生不良影響，應負上社會責任，額外付稅作為補償，社會各界同時要為青少年提供更多選擇，引發他們其他興趣。

港大醫學院兒童及青少年科學系臨床教授葉柏強表示，長時間使用電子產品，導致學童眼球拉長，有可能提早在約40歲出現視網膜脫落、黃斑病變及青光眼等眼疾，提醒學童使用電子產品時，眼睛距離屏幕最少30至40厘米，並適當時候休息，預防勝於治療，呼籲家長陪同子女上網，增加進行戶外活動，減少子女上網時間。

▲多項研究顯示，本港學童上網娛樂時間日益增加，有可能引起精神壓力問題。