私隱專員公署發表有關八宗資料保安事故的報告

根據香港法例第 486 章《個人資料（私隱）條例》第 8 條發表

背景

個人資料私隱專員公署（私隱專員公署）早前處理八宗有關披露個人資料及個人資料保安的事故並已完成跟進工作。個案涉及不同行業的機構，涉事機構因不同方面的缺失令個人資料被不當披露，或令個人資料受未獲准許的或意外的查閱、處理或使用，違反《個人資料（私隱）條例》（《私隱條例》）的相關規定。

八宗資料保安事故的簡介（詳見附件一）

(1) 一間化驗中心的醫生在替投訴人進行超聲波掃瞄後，於離開檢查室時未有登出系統，令仍留在檢查室內的投訴人看到檢查儀器的顯示屏上展示的其他病人資料，包括英文姓名、完整香港身份證號碼及簡單病歷。

(2) 一名旅行團領隊向團員派發的團體電子機票上載有包括領隊及團員共 30 多名人士的英文姓名及出生日期，令所有團員均能透過該團體電子機票得知彼此的個人資料。

(3) 一名停車場保安員在處理有關泊車的投訴時，將投訴人的電話號碼提供予另一名涉事的停車場租戶，讓其自行與投訴人處理泊車事宜，構成將投訴人的電話號碼不當地披露予另一名租戶。

(4) 一間醫療服務機構透過網上登記表格收集市民的個人資料時，未有對表格的「查看結果摘要」功能作出適當設定，令 100 多名登記人士的個人資料包括中英文姓名、電話號碼、電郵地址和出生日期可透過「查看結果摘要」功能被其他填表人士查閱。

(5) 一個政府部門向投訴人發出一封郵遞文件，但部門職員未有跟從既定的摺信要求處理信件，以致透過信封窗口可看到當中的信件標題及由投訴人香港身份證號碼組成的個案編號。

(6) 一間保險公司以環保紙打印發送到其他公司的文件，而所用的環保紙為待棄置的個人簡歷及香港身份證副本，令當中所載的個人資料亦一併被錯誤地發送到其他公司。

(7) 一間零售商向會員寄發優惠訊息電郵，惟寄發電郵的職員因操作失誤，將全體會員的電郵地址填寫在「收件人」欄目，令收件人因而可在該電郵中看到逾千名會員的電郵地址。

(8) 一間航空公司的會員帳戶系統使用了錯誤指令碼，以致投訴人在登入會員帳戶時被錯誤連結至另一會員的帳戶，並可查閱該會員帳戶內的個人資料。

跟進結果

《私隱條例》附表 1 的保障資料第 3(1)原則訂明，如無有關的資料當事人的訂明同意（即當事人自願給予的明示同意），個人資料不得使用（包括披露及轉移）於新目的，即於當初收集資料時擬將該資料用於的目的或直接有關的目的以外的目的。

保障資料第 4(1)原則訂明，資料使用者須採取所有切實可行的步驟，以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。

在上述個案中，經考慮個別事件的情況及所獲得的資料，個人資料私隱專員（私隱專員）鍾麗玲發現涉案機構分別違反了《私隱條例》下保障資料第 3(1)原則有關使用（包括披露）個人資料的規定，或保障資料第 4(1)原則有關個人資料保安的規定。

私隱專員的決定

私隱專員已分別向各機構發出執行通知、警告信或勸喻信，指示相關機構糾正其違反事項，以及防止同類違反的行為再發生。

建議

資料保安的陷阱可能潛藏在每個工作步驟，為了協助機構應對個人資料保安的挑戰，私隱專員希望藉此報告，向各行各業的機構作出以下六項建議：

(i) **將保障個人資料私隱納入機構的核心價值**，並委任合適的主管人員負責資料保安，公開展示管理層對保障個人資料私隱的決心，讓員工感受到其重要性；

(ii) **通過培訓提升員工保障私隱的意識和能力**，按照工作職能為員工提供針對性的培訓，重點講解常見風險及進行情景演練；

(iii) **制定清晰易明的工作指引**，針對不同崗位的工作特性，設計檢查清單或流程圖向員工清晰傳達具體易明的操作指引，並定期通過電郵、內部平台或會議重申相關重點；

(iv) **採取技術上的保安措施**，例如使用預設加密的電郵系統或自動填充電郵正確收件人，減低錯誤操作的風險；

(v) **定期監察、評估及改善資料保安政策的遵從情況**，包括安排主管人員定期或突擊巡查前線員工的工作情況，透過監察以確保個人資料保安政策獲得貫徹執行，並定期收集員工的意見以持續改善有關政策；及

(vi) **制定全面的資料外洩事故應變計劃**，以助機構快速應對及有效管理一旦發生的資料外洩事故。

鍾麗玲
個人資料私隱專員
2025 年 7 月 7 日

附件一

有關八間機構不當披露個人資料的個案摘錄

個案(1) – 化驗中心沒有採取充足保安措施導致病人資料外洩

投訴人到某化驗中心進行超聲波掃瞄。當完成檢查後，醫生先行離開檢查室，並獨留投訴人一人在檢查室內整理衣服。期間，投訴人看到超聲波儀器的顯示屏清晰展示數名病人（包括投訴人）的英文姓名、完整香港身份證號碼及簡單病歷（例如擬掃瞄的器官或所患疾病）。投訴人不滿自己的個人資料被展示，遂向私隱專員公署作出投訴。

經私隱專員公署介入事件後，該化驗中心已調整顯示屏的方向避免其直接面向病人，並不再展示病人姓名和香港身份證號碼，以及添置活動屏風以作遮擋。此外，該化驗中心亦修訂操作指引，要求醫護人員離開檢查室前必須登出系統，同時加強員工就有關個人資料私隱方面的培訓及定期進行私隱風險評估。

個案(2) – 旅行社分發載有所有團友個人資料的團體電子機票

投訴人因參加旅行團而向某旅行社提供其個人資料。涉事旅行團領隊於入境目的地國家前向團員分發同一張團體電子機票，供團員於辦理入境手續時自行向當地海關展示，惟該電子機票載有包括領隊及團員一共 30 多名人士的英文姓名及出生日期，令所有團員均能透過該團體電子機票得知彼此的個人資料。

旅行社承認事件源於相關領隊派發團體電子機票前，未有注意到航空公司在其中附加了乘客的出生日期。經私隱專員公署介入後，旅行社已通知相關旅行團每一組別之聯絡人自行銷毀該團體電子機票，並就團體電子機票的處理方式作出多項改善措施，包括統一電子機票之格式，當中只可包含航班資料、相關團員的姓名及其電子機票號碼，並在覆核後才將該些為每名團員特製的電子機票提供予領隊，不再將團體電子機票分發給團員，以及加強內部監察和員工培訓。

個案(3) – 保安公司在處理有關泊車的投訴時披露一名停車場租戶的電話號碼予另一名租戶

投訴人為一個屋苑的停車場租戶。投訴人早前收到另一名租戶（租戶 A）的來電，要求他到停車場重新泊好車輛，讓租戶 A 可順利將車輛駛入其所屬的車位。投訴人到場後獲悉當值的保安員將其手提電話號碼披露予租戶 A。

保安公司事後承認事件源於租戶 A 向涉事保安員要求協助聯絡投訴人，其後該保安員錯誤地應要求將投訴人的電話號碼披露予租戶 A，讓其自行與投訴人聯絡處理泊車事宜。

經私隱專員公署介入後，保安公司採取措施糾正違規事項，以及防止類似違規情況再次發生，包括制定和實施政策及程序確保員工不會在未獲資料當事人的同意下，將停車場用戶的個人資料使用於「新目的」，並定期將相關政策及程序向員工傳閱。

個案(4) – 醫療服務機構的網上登記表格不當披露登記人士的個人資料

某醫療服務機構的網上登記表格被發現不當披露 100 多名登記人士遞交的個人資料，包括中英文姓名、電話號碼、電郵地址和出生日期。事件源於人為疏忽，因相關機構的職員沒有更改網上表格設定的「查看結果摘要」功能，讓填表格的人士可以從「查看結果摘要」功能看到其他填表人士的資料。

相關機構於知悉有關情況後已即時停用網上登記表格之連結及移除該表格。該機構確認日後會正確設置「查看結果摘要」功能，方將網上表格上載網站使用。

個案(5) – 政府部門發出的信件內容可透過信封窗口被查閱

有政府部門向投訴人郵遞有關通知更改地址的文件，投訴人收悉有關信件後發現透過信封窗口可看到當中的信件標題及其個案編號，而該編號即其香港身份證號碼。投訴人就此向私隱專員公署投訴相關政府部門沒有妥善保障其個人資料安全。

該政府部門承認事件源於有關職員未有跟從相關政府部門既定的摺信要求處理向投訴人發出的信件，且未有意識到信封窗口顯示了個案編號。經私隱專員公署介入事件後，相關部門已採取一系列跟進措施，包括提醒有關職員必須遵從既定程序處理信件、就相關摺信要求及程序制定清晰的圖示指引、將個案編號於信件範本中的位

置向下調整、安排主管定期抽查信件，以及安排員工參與培訓，加強他們在保障個人資料私隱方面的意識。

個案(6) – 保險公司使用載有個人資料的文件作為環保紙

一間保險公司將原本需要棄置的個人簡歷及香港身份證副本等載有個人資料的紙張當作環保紙使用，並將以該些環保紙打印的文件發送到其他公司，令當中所載的個人資料遭外洩。

經私隱專員公署介入事件後，相關公司已與處理個人資料的員工進行面談及解釋事件的嚴重性，並強調不可再發生同類事件。此外，該公司亦向所有員工發出通告，指示員工有關重用紙張及棄置載有個人資料文件需要注意的事項，包括必須棄置所有完成投保手續的文件於指定回收位置並待環保回收公司代為處理、棄置或銷毀，並安排定期傳閱有關通告，以確保其員工不會重蹈覆轍。

個案(7) – 零售商向會員寄發優惠訊息電郵時意外披露其他會員的電郵地址

事件源於一間零售商向會員寄發優惠訊息電郵時，將全體會員的電郵地址錯誤填寫在「收件人」欄目，引致收件人看到其他逾千名會員的電郵地址。事件肇因是一名職員發出電郵時錯誤將所有會員的電郵地址填寫在「收件人」一欄。

事件發生後，相關公司向所有涉事會員發出道歉信，要求客戶注意錯發的電郵並刪除涉事電郵。經私隱專員公署介入後，該公司已就電郵發送作出糾正措施，每當員工發送電郵至兩個或以上公司以外人士的電郵地址時，系統會自動以密件副本功能（即 b.c.c.形式）發送電郵，讓除收件人自己以外的其他電郵地址均被隱藏。該公司亦發出通告提醒所有員工正確使用發送電郵的密件副本（即 b.c.c.）功能。

個案 (8) – 航空公司的會員帳戶系統因指令碼錯誤導致個人資料外洩

投訴人為某航空公司的客戶。投訴人在輸入電郵地址登入其帳戶後發現所展示的個人資料屬於另一名客戶。

航空公司承認事件源於其服務供應商將其會員帳戶系統更新時編撰的指令碼出現錯誤，以致該指令碼錯誤讀取電郵地址中的一些特殊字符(例如“_”, “*”, “%” 等) 為通用字符，導致該帳戶錯誤連結至另一名擁有相似電郵地址的客戶帳戶。

私隱專員公署就個案指令航空公司制定指引及程序，以確保其供應商在測試系統提升時檢查特殊字符，並制定及實施措施要求供應商日後在進行涉及個人資料的系統提升時，就編撰指令碼或類似的規程進行額外的審查。