「學校數據安全與風險管理」網上研討會

鍾麗玲女士

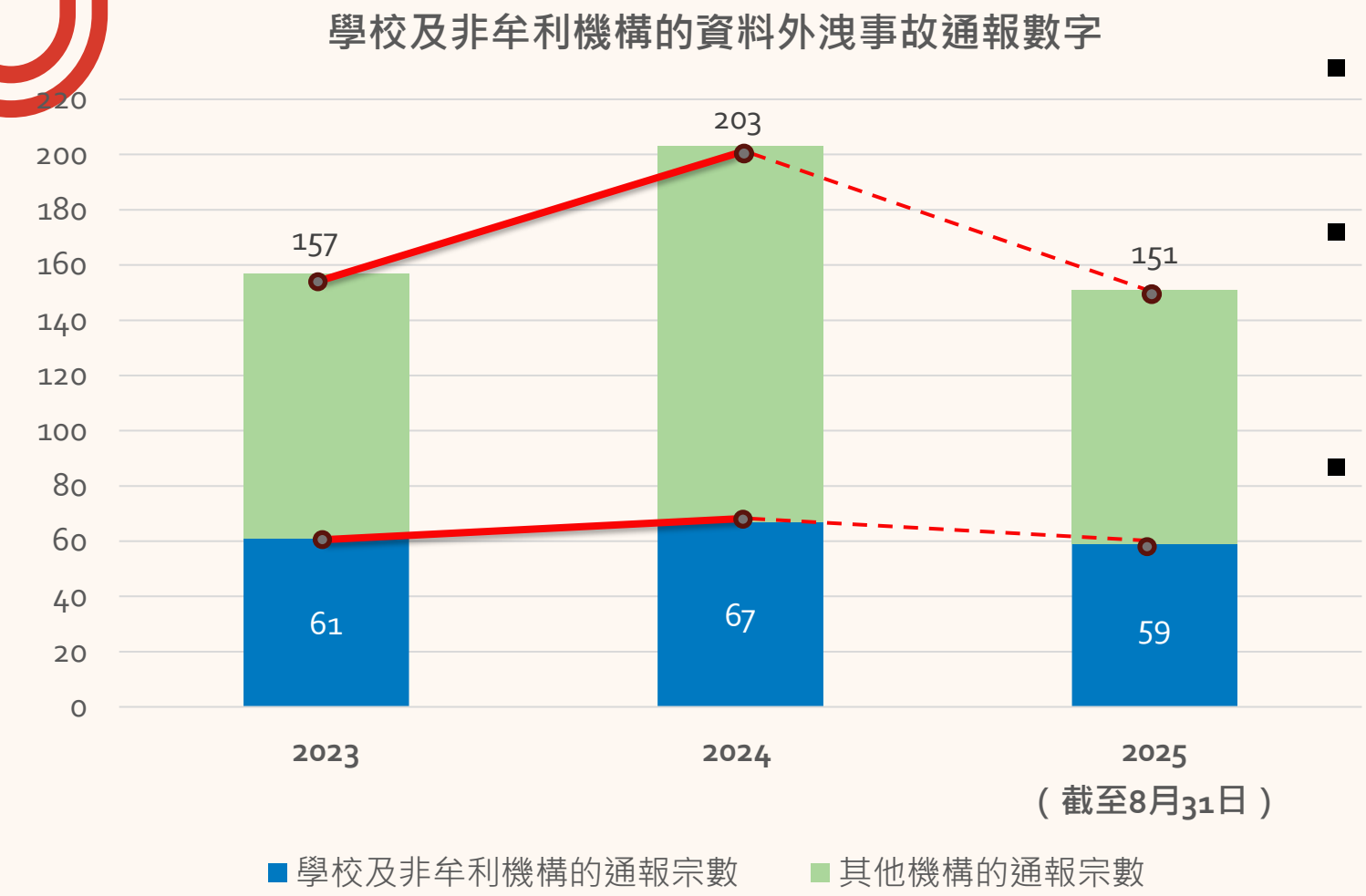
個人資料私隱專員

2025年10月9日

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

資料外洩事故通報趨勢



- 私隱專員公署於2024年共接獲203宗資料外洩事故通報
- 當中來自學校及非牟利機構的個案佔67宗（約33%），比2023年上升約10%
- 於2025年首8個月，私隱專員公署共接獲59宗來自學校及非牟利機構的資料外洩事故通報，佔整體個案總數約39%，比上年同期接獲此類個案的百分比上升約6%

《私隱條例》的相關規定

資料外洩事故可構成違反《私隱條例》附表1的保障資料第4原則

保障資料第4(1)原則

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

保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用

個案分享

個案（1）

一間教育機構因密碼管理欠佳而導致學生和家長的個人資料被未獲授權查閱

背景

一間教育機構的資訊管理系統遭黑客利用**暴力攻擊**獲取了管理員帳戶密碼，並建立了具有管理員權限的新帳戶，以查閱當中的個人資料。事故影響**超過24,000名家長及學生用戶的個人資料**。該機構調查後發現，是次事故源於**密碼管理欠佳**。

補救措施

1. **採用雙重認證功能**為帳戶提供額外的保護；
2. **設定高強度密碼**；
3. **定期清理不必要的帳戶**；及
4. **加強培訓**提高員工的資料保障意識。

個案（2）

即時通訊軟件帳戶遭騎劫

背景

私隱專員公署曾接獲23宗有關社福機構及學校的資料外洩事故通報，表示用作與服務使用者、學生及／或學生家長通訊的**即時通訊軟件帳戶遭騎劫**，騙徒繼而盜用有關即時通訊軟件帳戶**假冒受害機構**，向通訊錄的聯絡人發送訊息企圖騙取金錢。

事件涉及近**2,600名服務使用者、學生、學生家長及／或職員的**姓名及手提電話號碼等**個人資料**。

補救措施

1. **加強即時通訊軟件帳戶的保安措施**，例如啟用帳戶的雙重認證功能、定期檢查已連結的裝置及登出不再使用或不明的裝置連結；及
2. **制訂指引**向員工述明安全使用即時通訊軟件的注意事項，包括小心留意網頁連結，不要誤按虛假的即時通訊軟件網頁版，及切勿向他人透露任何密碼或驗證碼等。

保障WhatsApp帳戶的措施

啟用WhatsApp雙重認證功能

定期在WhatsApp設定中檢查已連結裝置

切勿向他人透露任何密碼或驗證碼

小心誤按虛假的WhatsApp網頁版

切勿從非官方渠道下載及使用WhatsApp應用程式

一旦收到可疑訊息，先確認發送者的身分

切勿隨意打開連結或披露個人資料

復原遭盜用WhatsApp帳戶

1. 以你的手機號碼登入 WhatsApp

2. 輸入你於SMS短訊收到的 6 位數驗證碼來驗證手機號碼

3. 當你輸入驗證碼後，盜用你的帳戶的人便會被自動登出

NOTE

- 如需輸入**雙重認證驗證碼**，而你不知道此驗證碼，那**可能是盜用你的帳戶的人已啟用雙重認證功能**
- 若你沒有此驗證碼，**等待7日後**便能登入你的帳戶

來源：WhatsApp

個案（3）一名中學教師沒有適當地設定內部檔案的存取權限

背景

一名中學教師在離職前將文件連同**117名學生的個人資料製成雲端範本供內部使用**。然而，該名教師沒有適當地設定有關檔案的存取權限，以致學生可以未經准許查閱相關檔案，當中載有學生的姓名、性別、就讀小學名稱、成績、跨境生和有特殊學習需要的學生標示及分班結果。

補救措施

1. 停止了所有用戶建立或使用雲端的範本功能；及
2. 制定守則述明教職員透過雲端分享檔案時需注意的事項，例如確保在**分享檔案之前設定存取權限**等。

個案（4）載有學生及家長個人資料的文件夾遭意外棄置

背景

一間學校的工友**錯誤地把一個載有超過100名學生及家長個人資料的「自動轉賬」文件夾當作廢物處理**，並棄置於學校附近的垃圾站。該學校調查後發現，是次事故源於負責處理自動轉賬工作的文員將相關文件夾放置在其桌下的垃圾桶上，以致工友誤以為相關文件夾屬可棄置，並與其他廢物一併處理。

補救措施

1. 提醒涉事員工須謹慎處理及保管載有個人資料的文件，及向涉事工友提供有關處理廢物做法的**培訓**；及

2. 將保障個人資料私隱的工作指引及注意事項**納入教職員守則內**；並透過會議及工作坊，向員工講解已修訂的守則。

借鑑

學校應：

- **制訂保障資料政策和程序**，並**加强保安措施**以保障個人資料；
- **採取措施及監管機制**，**確保教職員遵從**相關政策和程序的要求行事；及
- **為教職員提供全面的培訓**，加強他們保障個人資料私隱的意識，減低人為錯誤的風險。

資料保安建議措施

《資訊及通訊科技的保安措施指引》

1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

下載指引

下載小冊子

資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

- 在網絡安裝**防火牆**，以防止未經許可的網絡連接，亦可偵測網絡攻擊；
- 在電腦及伺服器安裝**防毒軟件**（反惡意軟件），以偵測及防止病毒及威脅；
- 定期進行**保安漏洞評估**及**滲透測試**；
- 使用**網站安全掃描服務**，定期掃描以偵測最新的已知或潛在的網絡安全風險；
- 及時更新正在使用的系統及軟件，可以**修補保安漏洞**，減少被攻擊的機會。

資料保安建議措施

技術上及操作上的保安措施

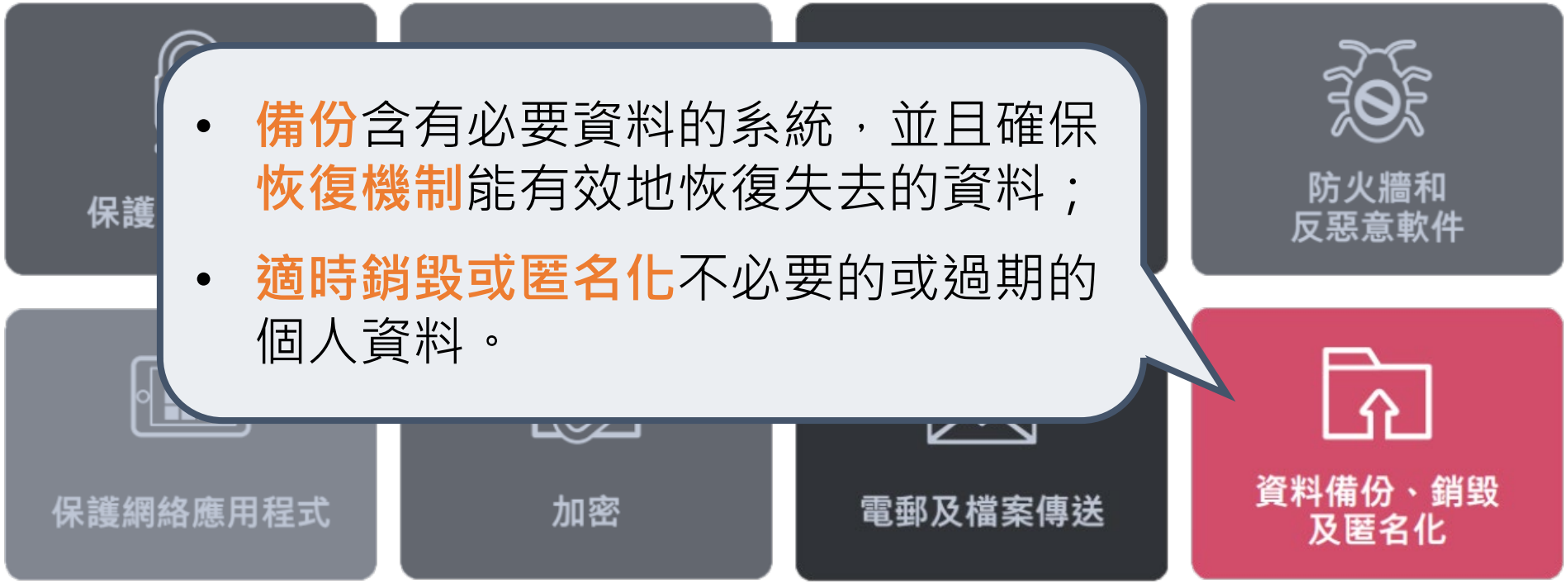
資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

- 採用**「最小權限」**的原則，以**角色爲本**分配適當的存取權限；
- 實施**密碼管理**，包括強制密碼長度和複雜性等；
- **定期覆檢存取權限**及適時刪除不必要的帳戶；
- 使用**多重身份驗證**的存取管控。

資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：



- **備份**含有必要資料的系統，並且確保**恢復機制**能有效地恢復失去的資料；
- **適時銷毀或匿名化**不必要的或過期的個人資料。

資料保安建議措施

資料保安事故發生後的補救措施

- 停止並中斷連接受影響的系統
- 更改密碼或中止權限
- 更改系統配置
- 通知受影響人士並提供建議
- 通知私隱公署及其他執法或監管機構
- 修補保安漏洞
- 在可行情況下掃瞄系統
- 汲取經驗及教訓

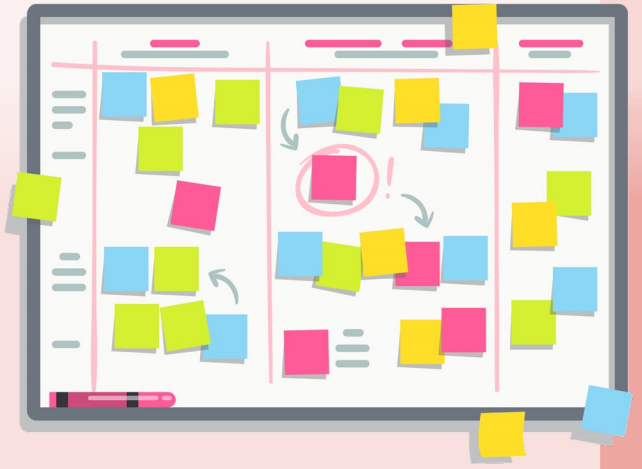
NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料治理和資料保安措施

處理資料外洩事故

資料外洩事故應變計劃

資料外洩事故應變計劃是載列機構一旦發生資料外洩時會**如何應對的文件**。一套全面的資料外洩事故應變計劃有助機構**快速應對及有效管理事故**。



資料外洩事故應變計劃應：

- 概述發生事故後**須執行的程序**
- 資料使用者由事故開始到完結就**識別、遏止、評估**以至**管理事故**所帶來的影響的策略

如何處理資料外洩事故

1. 立即收集重要資料
2. 遏止事件擴大
3. 評估事件可造成的損害
4. 考慮作出資料外洩通報
5. 記錄事故

PCPD.org.hk

指引資料

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

資料外洩事故的處理及通報指引

引言

良好的資料外洩事故處理作為營商之道

採取良好的資料外洩事故處理政策及措施不但能協助資料使用者減低外洩事故所帶來的損害，還能透過有關資料使用者處理外洩事故以及訂立清晰的後續行動方案，展現其願意承擔責任的精神。另一方面，作出資料外洩通報除了能協助受影響的資料當事人採取適當的應對保護措施，亦有助有關資料使用者減低訴訟風險和維持其商譽及生意關係，而在個別情況下，甚至能保持公眾對有關機構的信心。

本指引旨在協助資料使用者準備及處理資料外洩事故，以防止類似事件再次發生，從而減低對有關資料當事人所帶來的損失和損害，特別是當外洩事故涉及敏感個人資料。

甚麼是個人資料？

資料外洩事故通常涉及個人（例如機構的顧客、服
職者）的個人資料。根據《個
(香港法例第486章)(《私隱條
合以下說明的任何資料[1]—

名在世的個人有關的；

間接地確定有關的個人的身分
及

式令予以查閱及處理均是切實

甚麼是資料外洩事故？

資料外洩事故一般指資料使用者[2]持有的個人資料懷疑或已經遭到外洩，令有關資料當事人的個人資料有被未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。

一些資料外洩事故的例子包括：

- 遺失載有個人資料的可攜式裝置，例如手提電腦、USB儲存裝置、可攜式影碟或後備磁帶
- 不當處理個人資料，例如不當地棄置、把電郵發送予非指定的收件人或被未經授權的職員查閱資料系統
- 資料使用者載有個人資料的資料系統被非法侵入或被未經授權的第三方查閱
- 第三方以欺騙手法從資料使用者取得個人資料
- 在電腦安裝檔案分享軟件而導致資料外洩

資料外洩事故可構成違反《私隱條例》附表1的**保障資料第4(1)及(2)原則**。**保障資料第4(1)原則**規定資料使用者須採取所有切實可行的步驟，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，尤其須考慮—

(1)條，「資料使用者」，就個人資料而言，指獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或

1

2023年6月

如何通報？

通知資料當事人

- 透過電話、書面、電郵或親身向資料當事人作出通報
- 如直接的資料外洩通報不切實可行，可發出公告、報章廣告，或於網站或社交媒體平台發出帖文

通知私隱專員公署

- 經私隱專員公署網頁、傳真、親身或以郵寄方式遞交「資料外洩事故通報表格」
- 不接受口頭通報

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

PCPD.org.hk

資料外洩事故通報表格

資料外洩事故一般指資料使用者持有的個人資料外洩，令此等資料承受未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。視乎個案的情況而定，資料外洩事故可構成違反《個人資料（私隱）條例》（《私隱條例》）的保障資料第 4 原則。

雖然《私隱條例》沒有規定資料使用者必須就資料外洩事故作出通報，但個人資料私隱專員公署（私隱公署）建議資料使用者在資料外洩發生後盡快向私隱公署、受影響資料當事人及相關機構作出通報。

資料使用者可使用此通報表格向私隱公署通報資料外洩事故，需時大約 10-15 分鐘。你可參考私隱公署的「處理資料外洩事故的實務建議」（見附錄）以獲取更多資訊。

收集個人資料聲明

請注意，你可自願向私隱公署提供你的個人資料。你提供的所有個人資料只會用於與是次資料外洩事故通報及個人資料私隱專員行使規管權力及職能直接有關的用途。

你有權要求查閱及改正私隱公署所持有你的個人資料。查閱或改正該等資料，可用書面向保障資料主任提出，地址為香港灣仔皇后大道東 248 號大新金融中心 12 樓。

你所提供的個人資料可能轉移給私隱公署因處理本個案而接觸的人士或機構，包括獲授權收取有關資料以作出執法或起訴行動的人士或機構。

❑ 本人明白上述內容，並代表資料使用者提交資料外洩事故通報。*

*必須填寫　#請圈出適用者

資料使用者的基本資料

資料使用者機構：❑ 私營機構　❑ 公營機構

公司／機構名稱*：

香港辦事處的聯絡地址：

聯絡人資料

作出此通報的人士的姓名*：

職位：　電郵地址*：

國家編號（非香港電話號碼）：

聯絡電話號碼*：

你是否你所屬公司／機構的資料保障主任？# 是／否

1

其他資訊科技相關指引及報告

- 保障個人資料私隱 – 使用社交媒體及即時通訊軟件的指引
- 個人資料匿名化入門指南
- 私隱專員公署完成審查60間機構使用人工智能對個人資料私隱的影響
- 僱員使用生成式AI的指引清單
- 人工智能 (AI): 個人資料保障模範框架
- 雲端運算指引
- 《數碼時代的私隱保障：實測十個網上旅遊平台收集個人資料的情況》報告
- 《電子點餐的私隱關注》報告
- 使用AI聊天機械人「自保」十招
- 《數碼時代的私隱保障：比較十大網購平台的私隱設定》報告
- 社交媒體私隱設定大檢閱
- 開發及使用人工智能道德標準指引
- 資訊及通訊科技系統的貫徹數據保障設計指引

www.pcpd.org.hk

PCPD HK

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

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner
https://www.pcpd.org.hk/Toolkit/tc/

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

Thank you!

謝謝！