「預防及處理資料外洩事故 提升教育界的數據安全措施」研討會

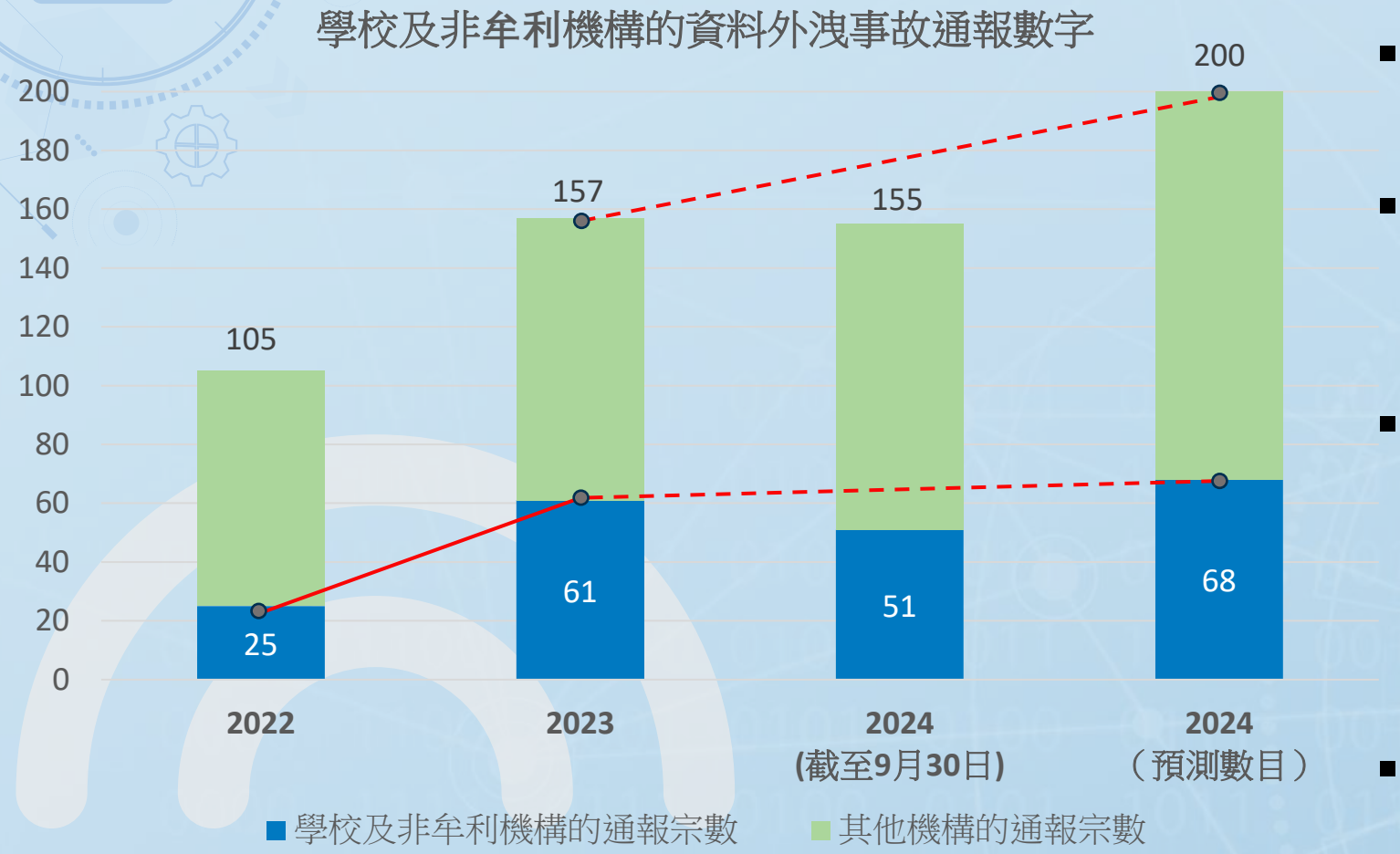
郭正熙先生

首席個人資料主任

（合規及查詢）

2024年12月16日

資料外洩事故通報趨勢



- 私隱專員公署於2023年共接獲157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61宗（約39%），比2022年上升接近一倍半
- 於2024年首三季，私隱專員公署共接獲51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33%，與上年同期接獲此類個案的百分比相若
- 今年全年數字預計會上升

《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

資料外洩事故

主要技術風險

- 網絡釣魚
- 未修補保安漏洞
- 低強度密碼
- 過時的操作系統和應用程式
- 植入惡意軟件

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**，未有採取行業最佳做法保護管理員帳戶所致。

補救措施

1. **採用雙重認證功能**為系統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（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

借鑑

- 當教育機構利用資訊科技帶來方便的同時，不應忽視隨之而來的**私隱風險**，特別是關乎兒童及青少年的個人資料；及
- 機構管理個人資料系統須加強警惕，**制定適當的系統安全政策、措施和程序**（例如善用**多重認證**功能及採用合適的**密碼管理政策**），以減低個人資料遭未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。

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。有關事件涉及近**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。

個案（2）

即時通訊軟件帳戶遭騎劫

借鑑

機構應**採取足夠的安全措施**保障有關帳戶的安全，包括：

- 啟用雙重認證功能；
- 定期更新軟件；
- 留意官方發出的安全資訊，並制定合適的政策供員工依循；
- 就安全使用有關軟件向員工提供合適的培訓；及
- 定期監察員工使用有關帳戶的情況，確保他們符合相關政策的規定。

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，以致學生有機會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（3）一名中學教師沒有適當地設定內部檔案的存取權限

借鑑

學校應：

- **制訂清晰而有效的資訊科技政策及程序**，羅列教職員在使用資訊系統及軟件時應如何保障個人資料的安全；及
- **採取措施確保**負責處理學生個人資料的**教職員遵從有關規定行事**，減低出現人為錯誤的風險。

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培訓，向員工發放已修訂的守則並講解當中要點。

個案（4）

載有學生及家長個人資料的文件夾遭意外棄置

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**，**確保員工遵從**相關政策和程序的要求行事；及
- **為員工提供全面的培訓**，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**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

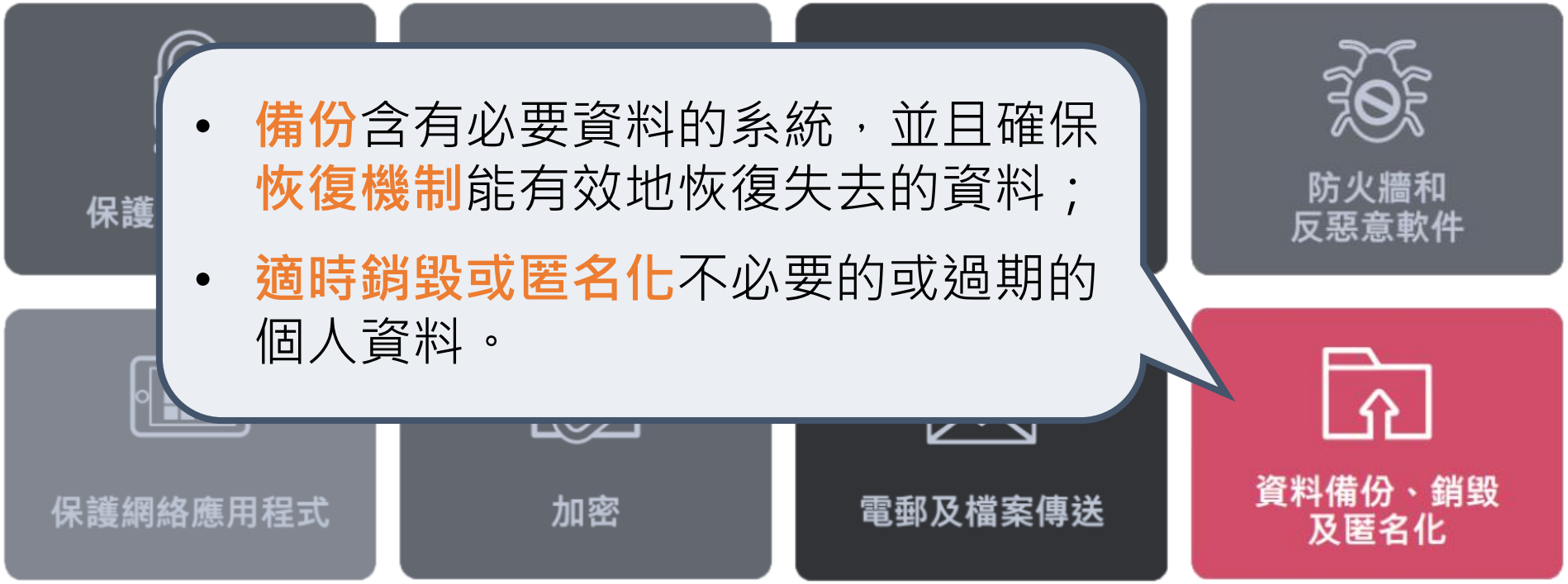
資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

- 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

資料保安建議措施

監察、評估及改善

資料使用者可委派獨立的專責小組負責：

- 定期**監察**資料保安政策的**遵從情況**
- 定期**評估**資料保安措施的**成效**

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

資料外洩事故應變計劃

- 描述構成資料外洩事故的要素
- 內部事故通報程序
- 指明專責應變小組成員的角色及責任
- 聯絡名單
- 風險評估工作流程
- 遏止策略
- 通訊計劃
- 調查程序
- 保存紀錄的政策
- 事後檢討機制
- 培訓或演習

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

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

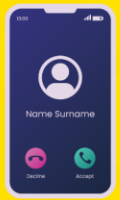
1　06/2023 修訂

其他資訊科技相關指引及報告

- 人工智能 (AI): 個人資料保障模範框架
- 《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
- 《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
- 保障個人資料私隱 – 使用社交媒體及即時通訊軟件的指引
- 資訊及通訊科技系統的貫徹數據保障設計指引

www.pcpd.org.hk

「數據安全」套餐 “Data Security” Package



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

免費名額參加研習班及講座
Free quotas to join professional workshop and seminars

PCPD HK

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

「數據安全」套餐 “Data Security” Package

數據安全快測

完成數據安全快測後，請將閣下的
參考編號及機構名稱，電郵至
training@pcpd.org.hk

參考編號: TK241112177527910

學校、非牟利機構及中小型企業：

如欲透過「數據安全」套餐換領五個免費參加由私隱專員公署舉辦的專業研習班及專題講座名額^，請將閣下的**參考編號**（如上）及**機構名稱**，電郵至training@pcpd.org.hk .

^註：五個免費參加由公署舉辦的專業研習班及專題講座的名額有效期至2025年12月31日。

謝謝！

Thank you!