「中小企防範網絡攻擊」研討會

鍾麗玲
個人資料私隱專員

2025年3月20日

資料外洩事故

甚麼是資料外洩事故?

一般指**資料使用者**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**

例子

- **遺失**載有個人資料的可攜式裝置
- **不當處理**個人資料
- 載有個人資料的資訊**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

《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

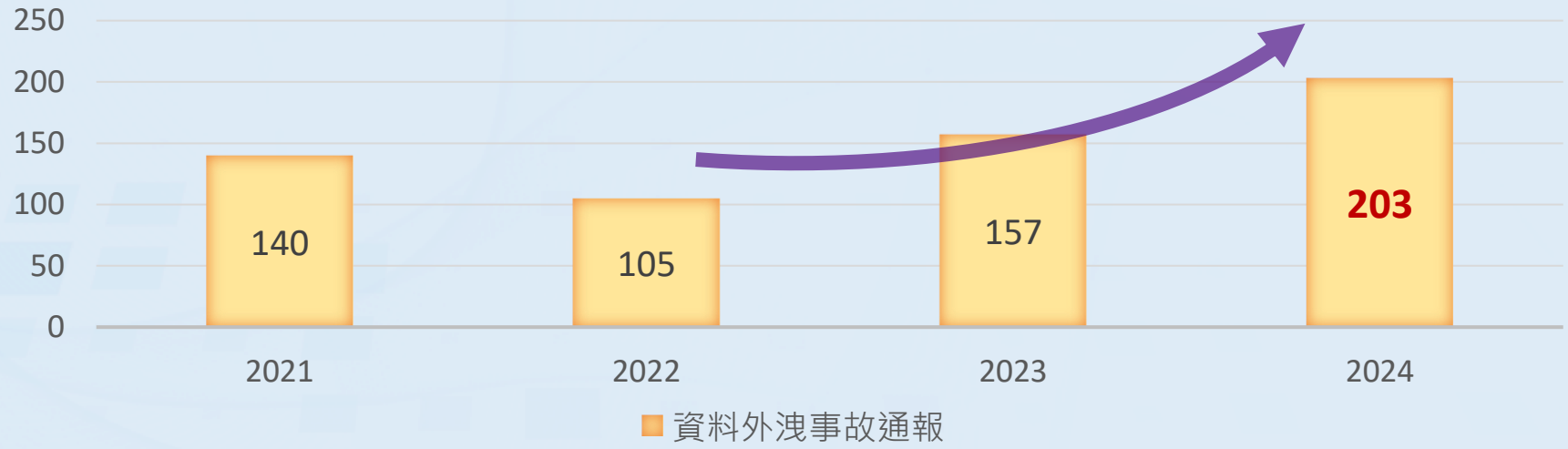
資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響

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被未獲准許或意外地查閱、處理、刪除、喪失或使用

公署接獲的資料外洩事故通報

- 私隱專員公署於2024年共接獲203宗資料外洩事故通報，較2023年的157宗**增加近三成**：



- 涉及黑客入侵的資料外洩事故由2022年的29宗（佔2022年資料外洩事故的28%），大幅增加逾一倍至2023年的64宗（佔2023年資料外洩事故的41%）
- 在2024年接獲的資料外洩事故通報中，61宗涉及黑客入侵，佔整體資料外洩事故通報的30%

個案分享

科技公司A的資訊系統遭勒索軟件攻擊

2023年8月，科技公司A向私隱專員公署作出資料外洩事故通報，表示其電腦系統及檔案伺服器遭受到勒索軟件攻擊及惡意加密。自稱Trigona的黑客組織要求公司A支付贖金，為已被加密的檔案解鎖

科技公司A的資訊系統遭勒索軟件攻擊

- 共有超過13,000名資料當事人受外洩事件影響，包括近8,000名與僱傭有關的人士，其中超過5,000名求職者及離職僱員的個人資料已被保留超過保留期限。其他受外洩事件影響的人士包括管理人員，實習生，以及與公司有業務往來的人士

- 受影響的個人資料包括姓名、身份證號碼及／或副本、護照號碼及／或聯絡資料，以及部分人士的財務資料（例如銀行帳戶號碼）、健康資料（例如醫療報告）、照片、出生日期、僱傭資料、社交媒體帳戶資料及／或學歷資料等

調查結果 五項缺失

1. 資訊系統欠缺有效的偵測措施
2. 未有為遠端存取資料啟用多重認證功能
3. 對資訊系統進行的保安審計不足
4. 資訊保安政策有欠具體
5. 不必要地保留個人資料

科技公司A的資訊系統遭勒索軟件攻擊

- 科技公司A違反了《私隱條例》保障資料第4(1)及第2(2)原則有關個人資料保安及保留的規定

- 私隱專員已向科技公司A送達執行通知，指示公司A糾正其違反事項，以及防止類似違規情況再次發生

慈善團體B的雲端儲存資料外洩

- 慈善團體B向私隱專員公署作出資料外洩通報，表示儲存於雲端內的檔案的存取權限被不明人士設定為公開。慈善團體B懷疑有黑客入侵其雲端儲存修改存取權限
- 事件影響1,146名培訓計劃報名人士、導師及員工的個人資料，當中包括姓名、 身份證號碼、電話號碼、電郵地址、工作 / 服務機構、職位、年資及銀行帳戶號碼

慈善團體B的雲端儲存資料外洩

缺失

- 事件源於員工錯誤地更改檔案的存取設定，或員工使用公共無線網絡登入雲端硬碟而引致黑客入侵
- 未有就使用雲端硬碟處理個人資料制訂指引或提供培訓

慈善團體B的雲端儲存資料外洩

補救措施及建議

- 停止使用涉事的雲端硬碟，並建立兩個雲端硬碟以分開存放載有敏感個人資料及一般資料的檔案
- 啟用雙重認證及使用高強度密碼保護新建立的雲端硬碟， 有關密碼須每三個月作出更改
- 制訂《在家工作網絡安全指引》以提醒員工在家工作時如何妥善保障個人資料
- 持續採取措施確保所有員工遵照有關保障個人資料的規定行事

使用雲端服務

下載指引

- 評估雲端服務供應商的能力，要求他們為雲端環境的保安管控提供證明
- 留意雲端服務的合約條款及外判安排
- 於雲端環境設立穩固的查閱管控和認證程序，例如嚴格的密碼政策、多重身份驗證、妥善的紀錄保存，以及定期覆檢存取權限
- 留意雲端服務更新，並更新相關軟件及／或調整適當的配置

非牟利組織C
遭勒索軟件攻擊

- 2024年7月，非牟利組織C向私隱專員公署作出資料外洩事故通報，表示組織遭受勒索軟件攻擊，其資訊系統因而受到影響

- 調查發現：
  - 黑客透過暴力攻擊及利用防火牆的嚴重漏洞，執行遠端指令，以取得保密插口層虛擬私有網絡（SSL VPN）主控台的存取權限，繼而控制一個資訊科技（IT）測試人員帳戶
  - 黑客識別出組織網絡中存有漏洞的伺服器，並取得管理員權限。黑客隨後進行橫向移動，入侵組織的伺服器、工作電腦及手提電腦

非牟利組織C
遭勒索軟件攻擊

- 超過330GB的數據從非牟利組織C的資訊系統中被竊取，可能受事件影響的資料當事人約550,000名，包括捐款者、活動參加者、義工、項目夥伴、項目參與者、項目顧問、現職及離職僱員、求職者及管治成員

- 涉及的個人資料包括姓名、配偶姓名、香港身份證號碼 / 副本、護照號碼 / 副本、出生日期、電話號碼、電郵地址、地址、信用卡號碼及銀行帳戶號碼

調查結果 七項缺失

1. 過時的防火牆存在嚴重漏洞
2. 未有啟用多重認證功能
3. 沒有對伺服器進行關鍵保安修補
4. 資訊系統欠缺有效的偵測措施
5. 對資訊系統進行的保安評估不足
6. 資訊保安政策有欠具體
7. 過長地保存個人資料

非牟利組織C
遭勒索軟件攻擊

- 非牟利組織C違反了《私隱條例》保障資料第4(1)及第2(2)原則有關個人資料保安及保留的規定

- 私隱專員已向非牟利組織C送達執行通知

資訊及通訊科技的資料保安建議措施

資料保安建議措施 *七大建議措施一覽*

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

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：

- 保護電腦網絡
- 資料庫管理
- 存取管控
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 電郵及檔案傳送
- 資料備份、銷毀及匿名化

處理資料外洩事故的實務建議

處理資料外洩事故的步驟

步驟1
立即收集重要資料

步驟2
遏止事件擴大

步驟3
評估事件可造成的損害

步驟4
考慮作出資料外洩通報

步驟5
記錄事故

- 資料外洩事故應變計劃

資料外洩通報

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
- 如在有關情況下直接的資料外洩通報並不切實可行，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

- 使用私隱專員公署的「**資料外洩事故通報表格**」
- 經私隱專員公署**網頁**、傳真、親身或郵寄方式遞交

NOTE **私隱專員公署並不接受口頭通報**

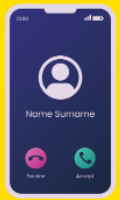
下載指引

資料保安事故發生後的補救措施

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

「數據安全」套餐 “Data Security” Package

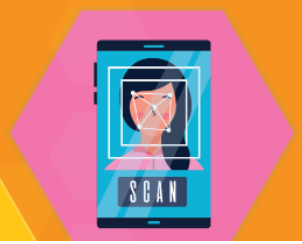


數據安全熱線
Data Security Hotline
2110 1155

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
H K
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

https://www.pcpd.org.hk/Toolkit/tc/

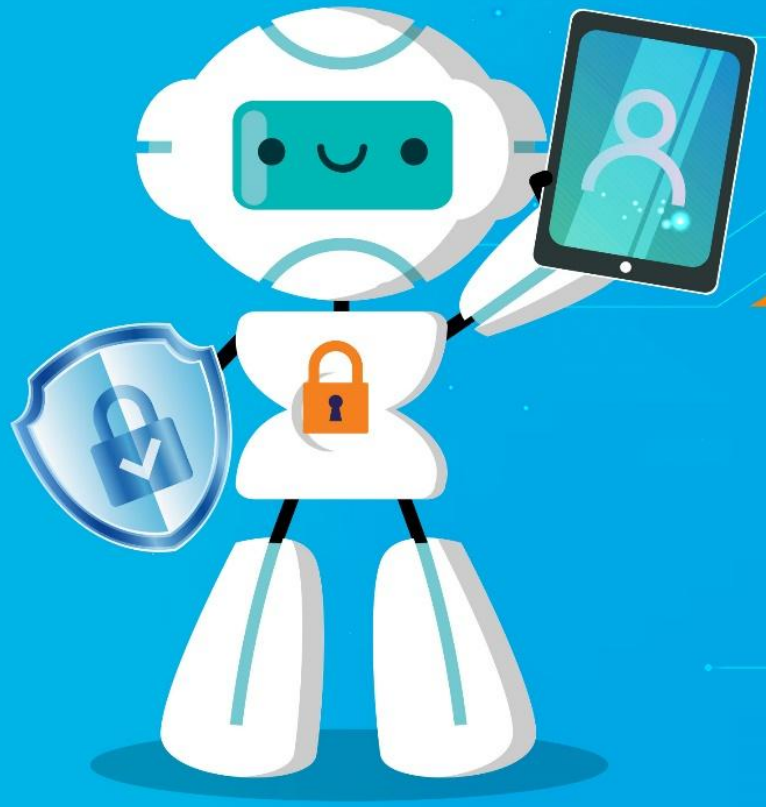
數據安全套餐

截止日期：4月30日

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

學校、非牟利機構及中小型企業:

- 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
- 名額有效期至2025年12月31日



謝謝 Thank you

公署網址

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