

「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



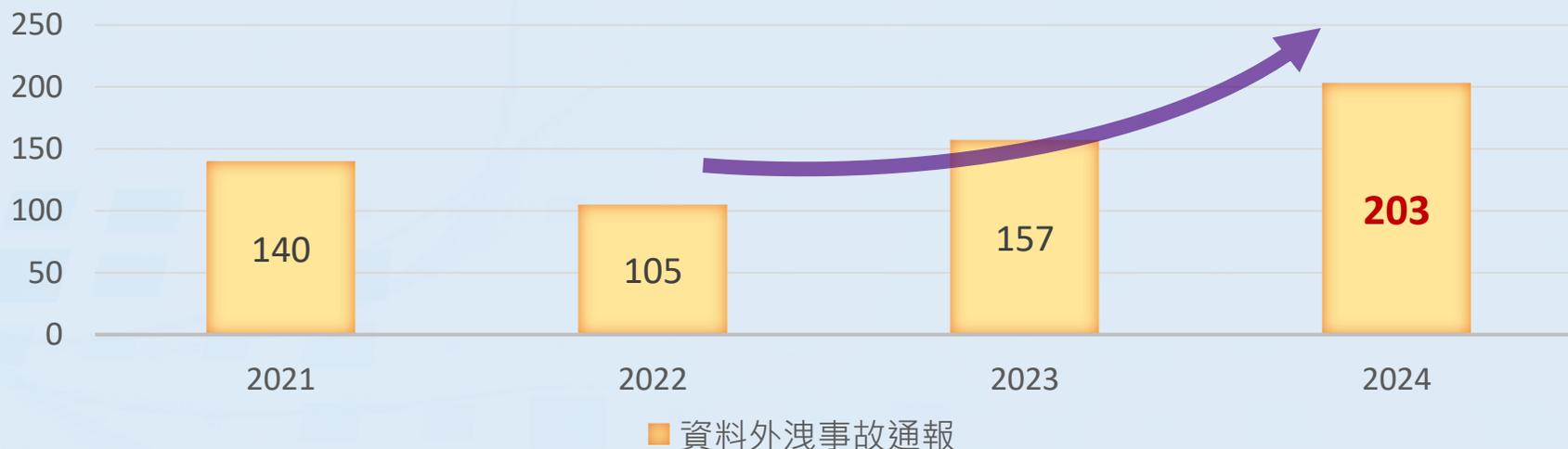
保障資料第4(2)原則

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

個案分享 (1)

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

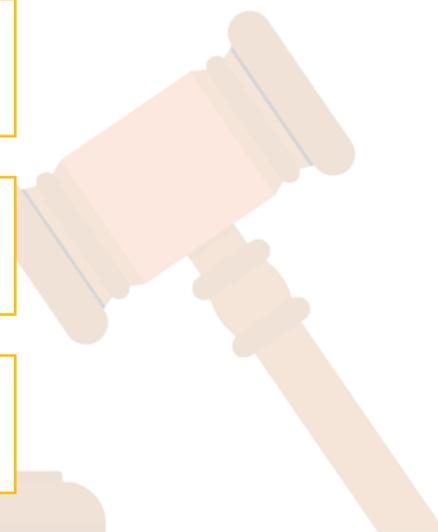
對資訊系統進行的保安審計不足

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

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



PCPD
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

指引資料

雲端運算指引

引言

本指引重點指出機構採用雲端運算時應考慮的因素。本指引闡釋《個人資料(私隱)條例》(條例)適用於雲端運算的相關要求，並提醒機構採用雲端運算時徹底評估雲端運算的益處、風險及了解其對保障個人資料私隱的影響。

何謂雲端運算？

「雲端運算」並沒有一個普遍認定的定義。一般而言，雲端運算模式能讓用戶隨時隨地、便捷地按需要透過網絡接連一系列可配置的電腦運算資源(例如網絡、伺服器、儲存器、應用系統及服務)，這些資源只需透過少量的管理工作或與服務供應商少量的互動，便能迅速地準備妥當及發布。雲端是根據使用量及租金來計算，而無需投放任何資本。

雲端運算的採用與條例的相關要求

資料使用者(即採用雲端運算的機構)在持有、處理資料的規定，包括附表1的保障資料原則。在聘用雲端資料第2(3)、3、4原則及條例第65(2)條的要求。

「處理」在條例第2條被定義為就個人資料而言，包括將資料修訂、廣播、刪去或更改資料。
「使用」在條例第2條被定義為就個人資料而言，包括披露或轉移資料。

雲端運算



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



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、服務使用者、僱員及求職者）的個人資料。根據《個人資料（私隱）條例》（香港法例第486章）（《私隱條例》），個人資料指符合以下說明的任何資料¹—

(a) 直接或間接與一名在世的個人有關的；
(b) 從該資料直接或間接地確定有關的個人的身份是切實可行的；及
(c) 該資料的存在形式令予以查閱及處理均是切實可行的。

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運到外洩，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、可攜式硬碟或後備磁帶
- 不當處理個人資料，例如不當棄置、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. 用者」，就個人資料而言，指獨自或聯同其他人或與其他共同控制該資料的收集。



下載指引

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
掃描系統



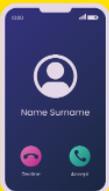
汲取經驗及教訓



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

「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

「數據安全」套餐 “Data Security” Package

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

數據安全套餐

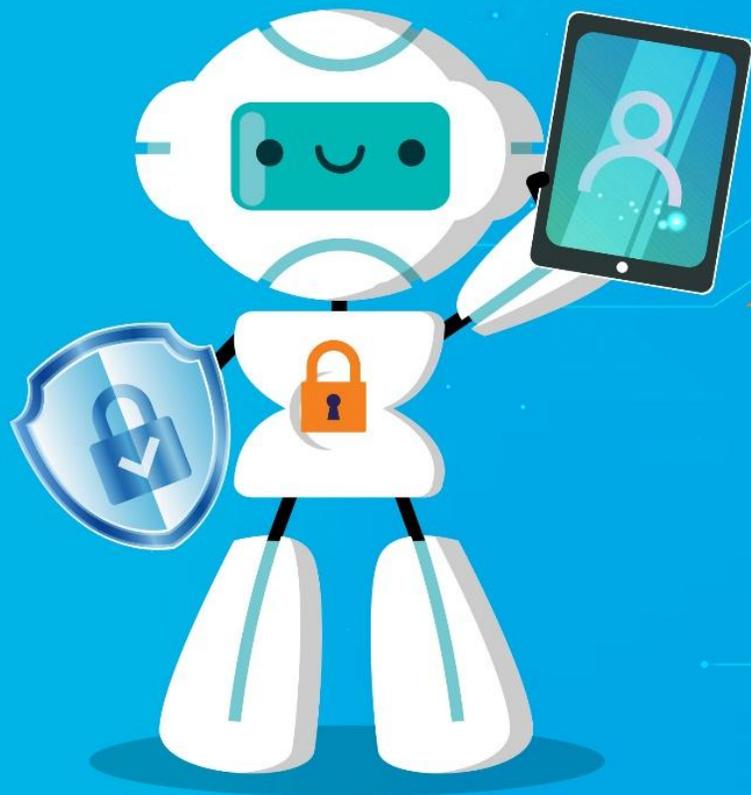
截止日期：4月30日

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



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