「Web 3.0下的網絡安全及資料外洩事故處理」講座
2023年7月27日

資料外洩事故的處理及通報指引

郭正熙先生
署理首席個人資料主任（合規及查詢）

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

《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使用者作處理的個人資料被未獲准許或意外地被查閱、處理、刪除、喪失或使用

資料外洩事故的常見原因

系統配置錯誤

網絡攻擊

經電郵或郵件的無意披露

職員疏忽/行為不當

不當/錯誤棄置個人資料

遺失實體文件或可攜式裝置

「事故發生前」—
資料外洩事故應變計劃

資料外洩事故應變計劃

- 載列機構一旦發生資料外洩時會**如何應對的文件**
- 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：
  ① 概述發生事故後**須執行的程序**
  ② 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

計劃涵蓋範疇(非詳盡)

- 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
- 培訓或演習計劃

「事故發生後」－
處理資料外洩事故

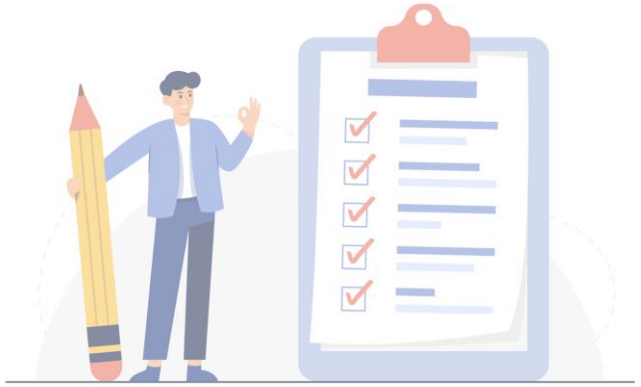
處理資料外洩事故的步驟

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

步驟 1：立即收集重要資料

資料使用者必須**迅速收集事故的所有相關資料**，以評估對資料當事人的影響及找出適當的緩和措施，包括：

- 事故於**何時**發生？
- 事故在**哪裏**發生？
- 事故**如何被發現**及由**誰人發現**？
- 導致事故的**原因**是甚麼？
- 涉及**甚麼種類**的個人資料？
- **有多少個**可能受影響的資料當事人？
- 可能對受影響人士造成甚麼**傷害**？



NOTE

最先發現事故的職員應考慮是否依從資料外洩事故應變計劃所訂的程序向專責應變小組／高級管理層／保障資料主任通報事故

步驟 2：遏止事件擴大

機構可視乎所涉及個人資料的類別及事故的嚴重性，考慮採取以下的遏止措施：

- **徹底搜尋**載有個人資料的遺失物品
- 要求錯誤接收有關電郵 / 信件 / 傳真的人士**銷毀或交回誤發的文件**
- **關閉或隔離**受損 / 遭破壞的系統 / 伺服器
- **修復**導致事故的**漏洞或錯誤**
- **更改用戶密碼及系統配置**
- **移除**涉嫌造成或引致資料外洩的**用戶的查閱權**
- 如已發生或可能發生身份盜竊或其他犯罪活動，應通知有關執法部門

步驟 3：評估事件可造成的損害

資料外洩事故可導致的損害包括：

- 人身安全受到威脅
- 身份盜竊
- 財務損失
- 受辱或喪失尊嚴、名譽或關係受損
- 失去生意或聘用機會

因資料外洩而可能蒙受的傷害程度取決於:

例如：

- 外洩個人資料的**種類**、**敏感程度**及**數量**
- 資料外洩的情況
- 傷害的性質
- **身份盜竊**或**詐騙**的可能性
- 遺失的資料**有否備份**
- 外洩資料有否進行足夠的**加密**、**匿名化**或其他保障措施
- 資料外洩**持續的時間**

步驟 4：考慮作出資料外洩通報

資料使用者在決定是否把事故通知受影響資料當事人、私隱專員公署及其他執法部門時，應考慮：

- 事故可能對受影響人士造成的影響
- 影響有多嚴重或重大
- 發生的可能性
- 不作出通知的後果

如資料外洩事故相當可能對受影響資料當事人有構成實質傷害的風險，資料使用者應在知道發生資料外洩後在切實可行的情況下盡快通知私隱專員公署及受影響資料當事人。

步驟 5：記錄事故

- 資料使用者必須**完整地記錄事故**，包括事故的**詳情**、**影響**，**資料使用者所採取的遏止措施和補救行動**
- 機構如須依從其他司法管轄區的法例及規例，亦應留意有關法例及規例下的**強制記錄要求**

NOTE

例如歐洲聯盟的《通用數據保障條例》規定資料控制者記錄所有資料外洩事故並保存有關紀錄

資料外洩通報

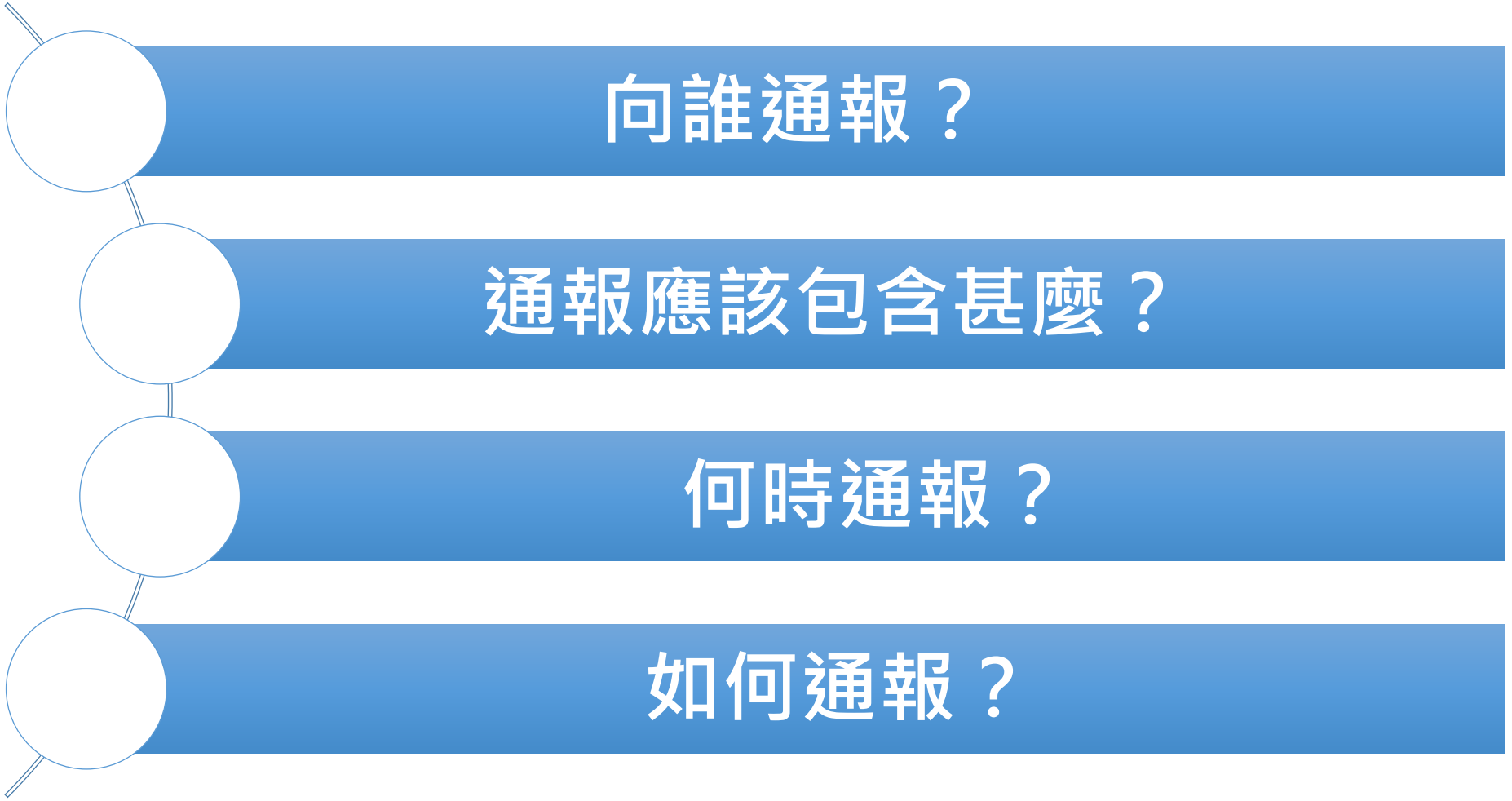
資料外洩通報

資料外洩通報是資料使用者向資料外洩事故的相關人士包括**受影響資料當事人**及**私隱專員公署**作出的正式通知

好處

- ✓ 告知受影響資料當事人宜**主動採取步驟**或**措施**，以減低潛在的傷害或損害
- ✓ 讓相關機構採取適當的**調查**或**跟進行動**
- ✓ 顯示資料使用者決意依從具透明度及負責任的原則，作出妥善的個人資料私隱管理
- ✓ **提高公眾的警覺性**
- ✓ 從私隱專員公署取得適當的意見，以迅速應對事故及改善其處理個人資料的系統及政策，**防止同類事故再次發生**

資料外洩通報



資料外洩通報

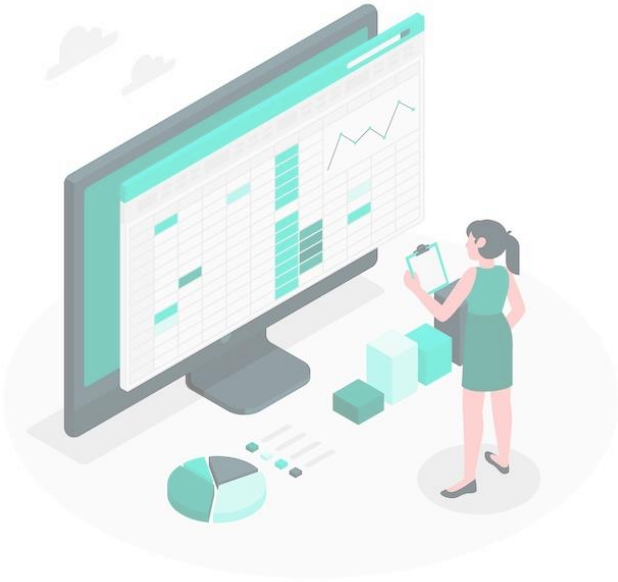
向誰通報?

- **受影響的資料當事人**
- **私隱專員公署**
- 私隱專員公署以外的執法機構
- 其他相關規管機構
- 其他能採取補救行動以保護個人資料私隱和受影響的資料當事人的權益的相關人士（例如：互聯網公司）

資料外洩通報

通報應該包含甚麼？

- 事件的概況
- 外洩的**源頭**、**日期及時間**，及估計或確實的持續時間
- 發現事故的日期及時間
- 所涉及的**個人資料類別**
- 所涉及的**資料當事人**的類別及大約**數目**
- 對事故導致的損害作出的**風險評估**
- 已**採取或將會採取的緩解措施**



資料外洩通報

何時通報?

- **在知悉事故後，不論內部調查的進度如何，在切實可行的情況下盡快作出通報**
- 如未能提供事故的詳情，最好盡量提供所有已掌握的資訊

NOTE

- **由於其他司法管轄區可能有指定的通報時限，如資料使用者須向海外的規管機構作出通報，有需要時應尋求專業意見，確保根據相關規定在法定時限內作出通報**

資料外洩通報

如何通報?

通知資料當事人

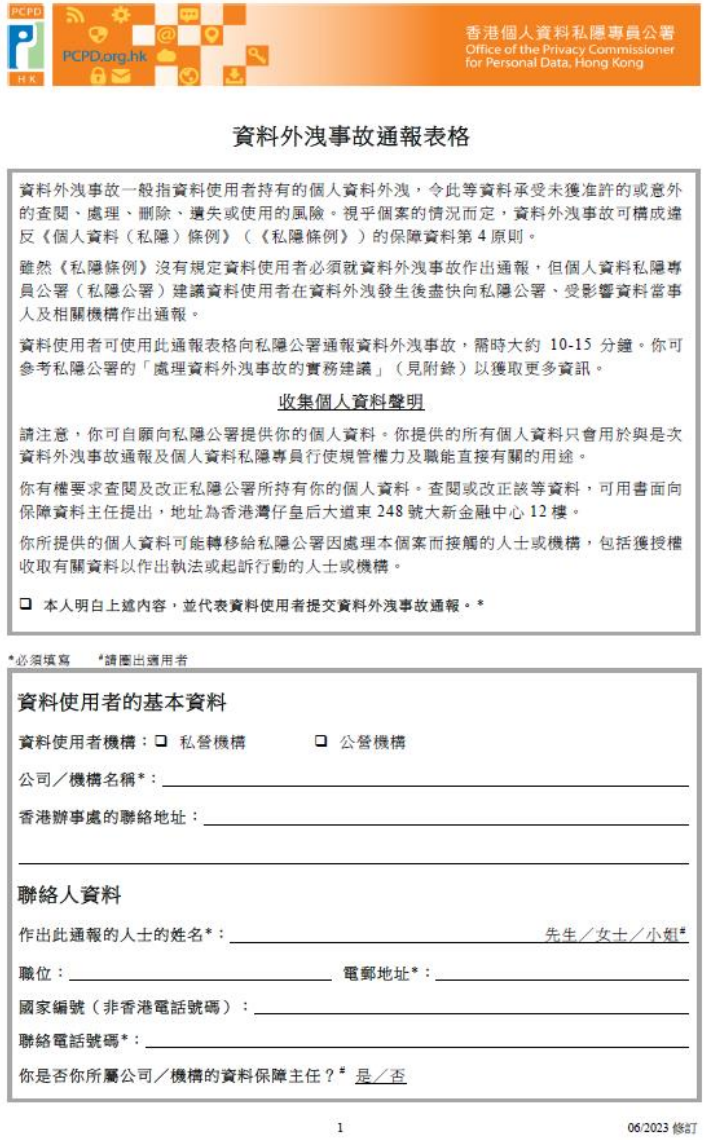
- 透過電話、書面、電郵或親身向資料當事人作出通報
- 如在有關情況下直接的資料外洩通報並不切實可行，可發出公告、報章廣告，或於網站或社交媒體平台發出帖文

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



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*：_____ 先生／女士／小姐#

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

汲取教訓：防止資料外洩事故再次發生

資料使用者應從事故汲取教訓、檢討處理個人資料的方式，以找出問題根源，並制訂清晰的政策，以防止類似事故再次發生

謝謝!

下載《資料外洩事故的處理及通報指引》