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分是切實可行的；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 《私隱條例》第2(1)條。

2 根據《私隱條例》第2(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、處理或使用的人。

(a) 該資料的種類及如該等事情發生便能做成的損害；

(b) 儲存該資料的地點；

(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；

(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及

(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

保障資料第4(2)原則規定，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[3]，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。

香港發生資料外洩事故的常見原因

資料外洩事故可由不同的原因造成。部分較常見的原因包括：

- **網絡攻擊**

  基於個人資料的價值，機構或會成為網絡攻擊（例如勒索軟件、暴力攻擊、分散式阻斷服務攻擊或網絡釣魚）的目標。這些攻擊有機會導致個人資料遭未獲准許的查閱，甚至從其伺服器或數據庫中外洩。

- **系統配置錯誤**

  錯誤的系統配置及管理可以導致資料外洩，例子包括數據系統在毋須驗證或欠缺查閱權控制的情況下遭未獲准許的查閱。

- **遺失實體文件或可攜式裝置**

  資料外洩的其中一個常見原因是遺失載有個人資料的實體文件或可攜式裝置（例如信件、填妥的表格、USB儲存裝置及手提電腦）。遺失亦可能是由受資料使用者委託處理個人資料的資料處理者無意地造成。

- **不當/錯誤棄置個人資料**

  載有個人資料、以不同形式（例如硬碟、紙本檔案、USB記憶體或其他類型的資料儲存裝置）儲存的文件在沒有依從機構的銷毀文件政策的情況下被意外地或不當地棄置，令載於該等文件中的資料受影響。

- **經電郵或郵件的無意披露**

  載有個人資料的電子檔案或實體文件被無意地發送予非指定的收件人，令可能載有個人資料的附件遭未獲准許的披露。

- **職員疏忽/行為不當**

  這主要涉及獲授予有效查閱權的職員故意地、意外地及/或惡意地不當處理個人資料，導致資料外洩。

3 根據保障資料第2(4)及第4(3)原則，「資料處理者」指代另一人處理個人資料及並不為該人本身目的而處理該資料的人。

為突發事故作好準備—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，以及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。迅速的應對可大幅減少及遏止事故的影響。

計劃應涵蓋以下範疇（非包括所有範疇）：

- **描述構成資料外洩事故的要素**，並因應機構的性質列舉例子及啓動資料外洩事故應變計劃的準則
- **內部事故通報程序**：向高級管理層、保障資料主任及/或資料外洩事故專責應變小組（專責應變小組）通報事故，並制訂標準表格，以便報告所需資料
- 指明專責**應變小組**成員的角色及責任（例如保障資料主任在處理事故上可能承擔整體責任；資訊科技部負責找出可能外洩的資料的位置及採取補救措施；客戶服務部負責照顧受影響人士的需要及向客戶提供最新消息）
- **聯絡名單**：列出專責應變小組各成員的聯絡詳情（例如核心管理人員、首席保障資料主任、資訊科技專家、風險管理及人力資源人員）
- **風險評估工作流程**：評估事故對受影響資料當事人造成損害的可能性及嚴重性
- **遏止策略**：遏止事故擴大及作出補救
- **通訊計劃**：涵蓋決定是否向受影響資料當事人、規管機構及其他相關人士作出通報的準則及門檻、必須提供的資訊種類、與持份者聯絡的機構聯絡人，以及通報的方式
- **調查程序**：調查事故及向高級管理層匯報結果
- **保存紀錄的政策**：確保已妥善記錄事故，因為規管機構或執法部門可能需要相關紀錄
- **事後檢討機制**：找出需要改善的範疇，以防事件再次發生
- **培訓或演習計劃**：確保所有相關職員能恰當地依從計劃，處理資料外洩事故

處理資料外洩事故

妥善處理及管理資料外洩事故顯示了資料使用者解決問題的決心，並可能大幅降低事故對當事人的影響及對機構的聲譽可能造成的損害。現建議下述處理資料外洩事故的步驟：

步驟 1 ：立即收集重要資料

首先，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？

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

資料使用者在發現資料外洩事故並進行初步評估後，應立即採取步驟盡量遏止事件擴大，以及採取補救行動，以減低可能對受影響資料當事人造成的傷害或損害。

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（非包括所有措施）：

- 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
- 聯絡互聯網公司，要求它們從搜尋引擎移除相關的緩存連結
- 關閉或隔離受損/遭破壞的系統/伺服器，並徹底檢查其他載有個人資料的相連系統是否受影響
- 停止可能與事故有關的系統功能
- 修復導致事故的漏洞或錯誤
- 告知銀行或信用卡公司，或有助減低受影響資料當事人蒙受財務損失的風險
- 就事故的發生及所採取的所有跟進行動保存紀錄，便利調查及採取糾正行動
- 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
- 如資料外洩是因資料處理者的作為或不作為而造成，應要求資料處理者立即採取補救措施及將進度告知資料使用者
- 遙距刪除遺失或被盜電子裝置內的資料
- 更改用戶密碼及系統配置，以阻止系統遭（進一步）未獲准許的查閱
- 移除涉嫌造成或引致資料外洩的用戶的查閱權
- 保存受損系統的適當紀錄，以作調查之用
- 考慮是否需要技術上的協助

步驟 3：評估事件可造成的損害

收集重要資料後，資料使用者應確保他們了解事件對受影響人士造成損害的風險，以採取步驟限制影響範圍。**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

受影響資料當事人因資料外洩而可能蒙受的傷害程度取決於：

- 外洩個人資料的種類及敏感程度：一般來說，資料越敏感，對受影響資料當事人造成損害的風險越大
- 涉及個人資料的數量：一般來說，外洩的個人資料數量越多，後果會越嚴重
- 資料外洩的情況：要有效遏止網上資料外洩存在一定困難，因此網上外洩的資料有機會被進一步散播及使用。但如收取資料的人是可已知及可追溯的，則較容易遏止事件擴大
- 傷害的性質
- 身份盜竊或詐騙的可能性：有時，外洩資料本身或與其他資料結合在一起後，有利賊人盜用身份或進行詐騙。例如，香港身份證號碼、出生日期、地址、信用卡資料及銀行戶口資料結合起來會較易令身份被盜用
- 遺失的資料是否有備份
- 外洩資料有否進行足夠的加密、匿名化或其他保障措施而令其不能被查閱，例如需要用密碼進行查閱
- 資料外洩持續的時間
- 有關事故是獨立事件，抑或屬於系統性問題
- 如屬於實物遺失，遺失的物品是否在可遭查閱或複印前已被尋回
- 有關事故發生後，是否已採取有效的緩和/補救措施
- 資料當事人可避免或減低可能蒙受傷害的能力
- 受影響資料當事人對個人資料私隱的合理期望

評估結果可能會顯示實際存在的傷害風險，例如當載有能辨識個人身份的資料、聯絡資料及財務狀況的資料庫意外地經檔案分享軟件在網上洩漏，可能會導致很多外洩的情況。在一些情況下，資料外洩事故可能涉及較低的傷害風險，例如遺失的USB記憶體載有安全加密的非敏感資料，或載有個人資料的儀器在遺失或隨意擱置後再度被尋回，而有關個人資料看來未曾被查閱。

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、這些影響有多嚴重或重大，以及發生的可能性有多大。資料使用者亦應考慮不作出通知的後果。

一般來說，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。在某些情況下，受其他監管要求規限的資料使用者亦可能需要根據相關的法定條文、實務守則及/或指引規則[4]通報資料外洩事故。如情況適用，亦會牽涉其他司法管轄區法例及規例[5]的通報責任。資料使用者如有需要，可就依從相關規定尋求專業意見。

步驟5：記錄事故

資料使用者應檢討資料外洩事故，從中汲取教訓，並視情況而改善其處理個人資料的做法。因此，資料使用者必須完整地記錄事故。一份全面的資料外洩事故紀錄應包含該事故的所有事實，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的，亦應留意有關法例及規例下的強制記錄要求[6]（如有）。

4 例如，上市規則的披露責任適用於上市公司。香港金融管理局就通報資料外洩事故發出的指引適用於認可機構。

5 本地實體遭受的資料外洩事故可能受其他司法管轄區的強制通報要求所規限，例如歐洲聯盟的《通用數據保障條例》及內地的《個人信息保護法》，視乎每宗個案的情況而定。

6 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。資料外洩通報有利於：

- 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，例如保護其人身安全、名譽或財務狀況；
- 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，例如當資料外洩事故可能影響公眾健康或安全時；及
- 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。

向誰通報？

視乎個案的情況，資料使用者應決定是否需要在切實可行的情況下盡快向以下單位作出通報：

- 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：聯絡互聯網公司，如谷歌和雅虎，要求它們從搜尋引擎移除相關的緩存連結）

通報應該包含甚麼？

視乎個案的情況，資料外洩通報可包括以下資料：

- 事件的概況
- 外洩日期及時間，及估計或確實的持續時間
- 發現事故的日期及時間
- 外洩的源頭（資料使用者本身或代資料使用者處理個人資料的第三者）
- 有關事故類別的基本資料
- 所涉及的個人資料類別的清單
- 所涉及的資料當事人的類別及大約數目
- 所涉及的個人資料紀錄的類別及大約數目
- 對事故導致的損害（例如身份盜竊或詐騙）作出的風險評估
- 為減輕損失或防止個人資料進一步被未經許可查閱及/或洩漏而採取或將會採取的措施的概述
- 專責應變小組或負責處理事故的指定職員的聯絡資料
- 向受影響資料當事人建議他們可採取甚麼行動保護自己不受外洩的不利影響及防範身份盜竊或詐騙（例如強制重設密碼、對釣魚電郵或帳戶上的詐騙活動提高警覺、聯絡有關的金融機構更改信用卡資料，以及聯絡信貸資料機構要求暫停向第三方提供他們的信貸報告）

資料使用者應考慮個案的具體情況，如對通報的內容有任何疑問，應尋求法律意見。

何時通報？

資料使用者必須盡快作出通報才能獲得通報的最大好處，特別是減低對受影響資料當事人造成損害的風險以及維持資料使用者的商譽。**一般來說，在知悉事故後，不論內部調查的進度如何，都應在切實可行的情況下盡快作出通報。**如資料使用者尚未能提供事故的詳情，最好先在通報中盡量提供所有已掌握的資訊。一旦調查得到事故的詳情，應即時把有關資訊提交私隱專員公署及其他執法部門。

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。

如何通報？

- 通知資料當事人

資料使用者可直接透過電話、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，例如資料當事人未能被即時辨識或公眾利益可能受影響，則以公眾通知的方式，如發出公告、報章廣告，或於網站或社交媒體平台發出帖文可能較為有效。如資料外洩事故導致特別嚴重的損害，或影響數目龐大的人士，使用多種方法公布事故則較為合理。

- 通知私隱專員公署

資料使用者向私隱專員公署通報事故時，應使用公署的「資料外洩事故通報表格」[7]。填妥的「資料外洩事故通報表格」可經私隱專員公署網頁，傳真，親身或郵寄方式遞交。私隱專員公署並不接受口頭通報。如資料使用者在填寫表格時需要協助，請聯絡公署。

汲取教訓：防止資料外洩事故再次發生

防範未然能更有效地防止資料外洩。進行資料外洩調查有助加深對個人資料保安措施的認識及找出資料使用者在個人資料保安措施方面的不足之處。**因此，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。**檢討時應考慮：

- 改善個人資料處理程序中的保安問題。保安的程度應與個人資料的敏感程度及其箇中風險相符。
- 限制授予個別人士使用個人資料的查閱權。應遵守「有需要知道」及「有需要查閱」的原則。
- 現有資訊科技保安措施是否足以保障個人資料免受黑客入侵、未經准許的或意外的查閱、處理、刪除、喪失或使用[8]。
- 因應資料外洩事故而修改或制訂的相關私隱政策及措施。
- 如何有效偵測及應對資料外洩事故。
- 加強對僱員、代理及資料處理者的監察及監督機制。
- 提供在職培訓，以推廣私隱意識及提高處理個人資料的僱員的審慎態度、辦事能力及良好操守。
- 在企業實施數據道德及問責原則[9]。
- 聘用資料處理者的政策和檢討合約中有關保障個人資料私隱的條款，包括規定資料處理者採取適當的資料保安措施及立即通報任何資料外洩事件[10]。

7 載於此網站：https://www.pcpd.org.hk/tc_chi/enforcement/data_breach_notification/dbn.html

8 請參閱私隱專員公署發出的《資訊及通訊科技的保安措施指引》
https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/guidance_datasecurity_c.pdf

9 請參閱私隱專員公署發出的《私隱管理系統最佳行事方式指引》
https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/PMP_guide_c.pdf

10 請參閱私隱專員公署發出的《外判個人資料的處理予資料處理者》資料單張
https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

私隱公署網頁
pcpd.org.hk

下載本刊物

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

查詢熱線 ： **(852) 2827 2827**
傳真 ： **(852) 2877 7026**
地址 ： **香港灣仔皇后大道東248號大新金融中心13樓1303室**
電郵 ： **communications@pcpd.org.hk**

二零一零年六月初版
二零一五年十月（第一修訂版）
二零一九年一月（第二修訂版）
二零二三年六月（第三修訂版）