資料外洩事故的處理及通報指引

PCPD HK

PCPD.org.hk

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

資料外洩事故－處理及通報行動

甚麼是資料外洩事故？

資料外洩事故一般指資料使用者持有的個人資料懷疑外洩，令此資料有被未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。資料外洩事故可構成違反《個人資料(私隱)條例》下的保障資料第4原則—個人資料保安。

行動

立即收集資料

立即收集有關資料以評估對資料當事人的影響，包括：

- 事故於何時及何地發生？
- 事故如何被發現及由誰人發現？
- 事故的肇因是甚麼？
- 涉及甚麼種類的個人資料及範圍有多大？
- 受影響的資料當事人有多少？

行動

聯絡相關人士及採取遏止措施

相關人士可包括：

- 執法部門
- 相關規管機構（例如香港個人資料私隱專員（「私隱專員」））
- 互聯網公司
- 資訊科技專家

遏止措施可包括：

- 如資料外洩是系統故障造成，應停止有關系統的操作
- 更改用戶密碼及系統配置，以控制查閱及使用資料
- 考慮是否需要尋求技術協助，以修補系統上的漏洞及／或阻止黑客入侵
- 停止或更改涉嫌作出或導致資料外洩的人士的查閱權
- 如犯罪活動已發生或相當可能發生，應通知有關執法部門
- 保留資料外洩的證據以協助調查
- 指示資料處理者立即採取補救措施及將進度告知資料使用者(如適用)

甚麼是資料外洩通報機制？

這是資料使用者向資料外洩事故受影響的資料當事人及相關人士作出的正式通知。

雖然法例沒有規定資料使用者就他們持有的個人資料的外洩事故通知香港個人資料私隱專員公署（「公署」），但公署建議資料使用者作出通報，以妥善處理有關事故。

如資料使用者決定向私隱專員通報資料外洩事故，可填寫「資料外洩事故通報表格」，然後透過網上、傳真、親身或郵遞方式交回填妥的表格。

行動

評估損害

評估資料外洩事故可造成的損害，如：

- 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

行動

考慮作出通報

在資料外洩事故中，如可以合理地估計實在的傷害風險，資料使用者應考慮：

- 通知資料當事人及相關人士
- 不作出資料外洩通知的後果

＊詳情請參閱《資料外洩事故的處理及通報指引》內文。

下載本刊物

查詢熱線 ： **(852) 2827 2827**
傳真 ： **(852) 2877 7026**
地址 ： **香港灣仔皇后大道東248號陽光中心13樓1303室**
電郵 ： **enquiry@pcpd.org.hk**

免責聲明

本刊物所載的資訊只作一般參考用途，並非為法例的應用提供詳盡指引。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。

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）

資料外洩事故的處理及通報指引

引言

本指引旨在協助資料使用者處理資料外洩事故及減低對有關資料當事人所造成的損失及損害，尤其當事故涉及敏感個人資料。

甚麼是個人資料？

個人資料是指

(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。

由於個人資料與一名在世的個人有關，資料使用者處理個人資料時應對資料當事人秉持尊重、互惠和公平的原則。資料使用者亦應建立道德數據管治文化，以處理資訊及通訊科技所帶來的個人資料私隱風險。

甚麼是資料外洩事故？

資料外洩事故一般指資料使用者持有的個人資料懷疑外洩，令此資料有被未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。

下列是一些資料外洩事故的例子：

- 遺失儲存的個人資料，例如筆記電腦、USB記憶體、便攜式硬碟、備份磁帶、文件檔案
- 不當處理個人資料，例如不當地棄置、把資料錯誤地發給他人或僱員未獲准許而查閱資料
- 資料使用者載有個人資料的資料庫遭黑客入侵或遭外人未經授權查閱
- 第三者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《個人資料(私隱)條例》(下稱「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，尤其須考慮該資料的種類及如該等事情發生可能造成的損害。**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[1]，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。

[1] 「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。

如何處理資料外洩事故？

資料使用者應採取補救措施以減低資料外洩事故對資料當事人可能造成的傷害或損害，並同時考慮事故對資料當事人可能造成的影響。現建議下述行動計劃：

行動：立即收集有關資料外洩事故的重要資料

資料使用者須立即收集有關資料以評估對資料當事人的影響，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？
- 事故的肇因是甚麼？
- 涉及甚麼種類的個人資料及範圍有多大？
- 受影響的資料當事人有多少？

資料使用者應考慮指派適當人士/小組(下稱「統籌者」)負責處理資料外洩事故，例如帶領進行初步調查及就調查結果撰寫詳細報告。統籌者需要與不同部門/組別聯絡及作出報告，以及把事情轉達高層，讓資料使用者可以盡快採取補救行動及作出決定。

行動：聯絡相關人士及採取措施遏止事件擴大

資料使用者在發現資料外洩後，應採取步驟，以杜絕事件的肇因，這可能需要聯絡執法部門(例如警方)、相關的規管機構(例如個人資料私隱專員(下稱「私隱專員」)、互聯網公司(例如Google及雅虎)及/或資訊科技專家，作出報告、尋求建議及協助。這裏所列舉的並非全部，還須視乎每宗個案的情況，考慮聯絡其他相關人士。

以下是一些應予考慮的遏止措施：

- 如資料外洩是系統故障造成，應停止有關系統的操作
- 更改用戶密碼及系統配置，以控制查閱及使用資料
- 考慮是否需要尋求內部或外部的技術協助，以修補系統上的漏洞及/或阻止黑客入侵
- 停止或更改涉嫌作出或導致資料外洩的人士的查閱權
- 如已發生或相當可能發生身份盜竊或其他犯罪活動，應通知有關執法部門
- 保留資料外洩的證據，這可能會有利調查及採取糾正行動
- 如資料外洩是因資料處理者的作為或不作為而造成，資料處理者須立即採取補救措施及將進度告知資料使用者

行動：評估事件可造成的損害

資料外洩事故可導致以下的損害：

- 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

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：一般來說，資料越敏感，對資料當事人所造成的損害會越大
- 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：網上外洩的資料要有效阻止被進一步散播及使用是困難的。另一方面，如收取資料的人是可被確定及可追溯的，則較容易遏止資料外洩

- 身份被盜或假冒的可能：有時，外洩資料本身或與其他資料結合在一起後，有利賊人盜用或假冒身份。例如，香港身份證號碼、出生日期、地址、信用卡資料、銀行戶口資料等在結合起來會較易令身份被盜竊
- 外洩資料有否進行足夠的加密、匿名程度保障而令其不能查閱，例如查閱時是否需要用密碼
- 資料外洩是否持續，及外洩資料會否進一步曝光
- 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，相關個人資料有機會被查閱或複印前，是否已尋回資料
- 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
- 資料當事人對個人資料私隱的合理期望

評估結果會顯示實際存在的傷害風險，例如有助評估當載有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時可能導致的損害。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，或受影響的資料當事人不多；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。

行動：考慮作出資料外洩通報

在資料外洩事故中，如可以辨識資料當事人並能合理地估計實在的傷害風險，資料使用者應考慮通知資料當事人及相關人士。資料使用者在作出決定前，應恰當地考慮不作出通知的後果。

以上建議的行動，資料使用者應因應實際事故的情況，判斷所需行動的多寡和具體內容。

甚麼是資料外洩通報機制？

這是資料使用者向資料外洩事故受影響的資料當事人及相關人士作出的正式通知。資料外洩通報機制有利於：

- 告知受影響人士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
- 讓相關機構因應事故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

雖然條例沒有有關規定，但如大多數海外保障個人資料的機構一樣，私隱專員鼓勵資料使用者採取資料外洩通報機制(尤其是機構資料使用者)，以處理資料外洩事故。

向誰通報？

資料使用者應視乎個案的情況，考慮盡快通知下述人士：

- 受影響的資料當事人
- 執法部門
- 私隱專員
- 相關規管機構
- 其他可採取補救行動以保障受影響資料當事人的個人資料私隱及利益的人士(例如互聯網公司，如Google及雅虎可提供協助，從其搜尋引擎移除相關的快取連結)。

通報應包含甚麼？

視乎個案的情況，通報可包括下述資料：

- 事件的概況
- 外洩日期及時間，及持續時間(如適用)
- 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)
- 表列所涉及的個人資料類別
- 對外洩事件導致的傷害(例如身份遭盜用或假冒)的風險評估
- 為防止個人資料進一步遺失或在未經許可下被查閱或洩漏而採取或將會採取的措施
- 由資料使用者指派機構內的部門或個人(受影響人士可向其取得進一步資料及協助)的聯絡資料
- 資料當事人可如何保障自己免受事故的不利影響及自己的身份不被盜用或被假冒的資料及指引
- 執法部門、私隱專員及其他有關人士是否獲通知

資料使用者應小心謹慎決定通報的內容(包括個人資料)，以免影響同時進行的調查工作。

何時通報？

在評估資料外洩事故的情況及影響後，應在發生事故後盡快作出通報；除非執法部門以調查事故為由，要求延遲通報。

如何通報？

向受影響當事人的通報可透過電話、書面、電郵或親身作出。如未能即時辨識資料當事人或涉及公眾利益，作出公開通報(例如透過網站或媒體)是較有效的方法。資料使用者亦應考慮所採用的通報方法會否增加傷害風險。

資料外洩事故的教訓：防止再次發生

資料外洩事故的調查可以找出資料使用者在處理個人資料方面的不足之處。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，並制定清晰的策略，防止事故重演。檢討時應考慮：

- 改善個人資料處理程序當中的保安問題
- 限制授予個別人士查閱及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
- 因應資料外洩事故而修改或制定相關的私隱政策及措施
- 如何有效偵測資料外洩事故。保存適當的查閱記錄有助察覺早期警號
- 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良好操守、審慎態度及辦事能力
- 聘用資料處理者的政策和檢討與資料處理者簽訂的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立即通報任何資料外洩事件[2]

[2] 請參閱公署發出的《外判個人資料的處理予資料處理者》資料單張 www.pcpd.org.hk/tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

資料外洩事故的良好善後，有助企業重建聲譽

資料使用者採取良好的處理資料外洩事故政策及措施，不單有助遏止事故所造成的損害，亦顯示資料使用者在應付問題及發出清晰的行動計劃方面具負責任的態度。作出資料外洩通報，除了讓受影響的資料當事人採取適當保護措施之外，還可減低訴訟的潛在風險及重建資料使用者的商譽及業務關係，而在某些情況下，長遠可以恢復公眾的信心。

資料外洩事故通報表格

通報資料外洩事故不會阻礙私隱專員收取投訴及對事故進行查詢或調查(不論是因應投訴而作出或是由私隱專員主動作出)。如資料使用者決定向私隱專員通報資料外洩事故，可填寫「資料外洩事故通報表格」(可從本署網頁[3]下載)，然後透過網上、傳真、親身或郵遞方式交回填妥的表格。如資料使用者需要協助以填寫本表格，請聯絡本署。

[3] 請參閱www.pcpd.org.hk/tc_chi/enforcement/data_breach_notification/dbn.html

下載本刊物

查詢熱線 ： **(852) 2827 2827**
傳真 ： **(852) 2877 7026**
地址 ： **香港灣仔皇后大道東248號陽光中心13樓1303室**
電郵 ： **enquiry@pcpd.org.hk**

免責聲明

本刊物所載的資訊只作一般參考用途，並非為法例的應用提供詳盡指引。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。

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）