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

資料外洩事故詳情

此通報是新的通報／早前通報所提供的資料更新。*#

資料外洩事故日期：_____（日／月／年）

你所屬公司／機構於何時得悉資料外洩事故？*

_____（日／月／年）

受影響人士的數目*：請註明：_____

是否有香港居民受影響？*# 是／否／有待確認

受影響香港居民的數目*：請註明：_____

涉及的個人資料類別*：

- ❑ 姓名
- ❑ 香港身份證號碼
- ❑ 護照號碼
- ❑ 相片
- ❑ 出生日期
- ❑ 地址
- ❑ 電郵地址
- ❑ 電話號碼
- ❑ 健康資料
- ❑ 財務資料
- ❑ 僱傭資料
- ❑ 社交媒體帳戶資料
- ❑ 學歷資料
- ❑ 其他，請註明：_____

你是否有聘用服務供應商／外判商處理上述個人資料？# 是／否

資料外洩事故詳情*：
（肇事原因／懷疑肇事原因摘要，以及你所屬機構最先是如何得悉有關資料外洩）

事件的評估及所採取的補救措施

事故的原因／懷疑原因*：

❑ 意外棄置　❑ 網絡攻擊（例如：黑客入侵）　❑ 電郵外洩
❑ 郵件外洩　❑ 遺失文件　❑ 遺失便攜式儲存裝置
❑ 員工行為失當　❑ 程式錯誤　❑ 伺服器設定錯誤
❑ 盜竊　❑ 其他，請註明：_____

對資料當事人實質構成的風險*：

❑ 人身安全受到威脅　❑ 身份盜竊　❑ 財務損失
❑ 名譽受損　❑ 失去商業機會　❑ 失去就業機會
❑ 沒有對資料當事人構成實質損害的風險　❑ 其他，請註明：_____

採取的補救措施摘要*：

_____
_____
_____
_____
_____

是否有通知受影響的人士？*# 是／否／否，將會於（　　）日內作出通知

你所屬的公司／機構是否已發出或將會發出新聞稿？*# 已發出／將會發出／不會

有否向其他機構通報資料外洩事故？（例如香港警務處）*# 是／否

向其他機構作出通報摘要（如適用）*：

_____
_____
_____
_____

填妥表格後，你可透過以下途徑把表格及其他與資料外洩事故相關的文件（如有）一併遞交：

- **親臨公署或郵寄**
  地址：香港灣仔皇后大道東 248 號大新金融中心 13 樓 1303 室
- **傳真**
  傳真號碼：2877 7026
- **電子郵遞**
  電郵地址：dbn@pcpd.org.hk

簽署：_____
姓名：_____
職位：_____
日期：_____

處理資料外洩事故的實務建議

附錄

資料外洩事故	意外棄置／遺失文件或電子儲存裝置
即時採取的補救措施	• 盡快嘗試尋找遺失的文件／便攜式儲存裝置 • 若無法尋回遺失的文件／便攜式儲存裝置，立即通知資料當事人
防止事故再次發生的措施	• 使用特定及設有穩妥拉鏈／鎖扣的袋運送載有個人資料的文件 • 將文件／裝置存放在已上鎖的儲物櫃／抽屜內 • 備有一份記載文件轉移的紀錄 • 在可行的情況下，減少列印文件及改用電子檔案 • 定期安排集中銷毀文件 • 使用便攜式儲存裝置前應先取得管理層的核准 • 安裝流動裝置管理軟件，以便在便攜式儲存裝置遺失時，以遙距方式刪除當中的資料 • 刪除已完成原本收集目的之個人資料
資料外洩事故	**網絡攻擊（例如黑客入侵／暴力攻擊／勒索軟件攻擊等）**
即時採取的補救措施	• 切斷被入侵的裝置與互聯網及其他網絡的連接 • 使用防毒軟件為離線的電腦網絡進行掃描。不要理會任何提示你連接互聯網的訊息，若發現任何惡意軟件，依照防毒軟件的指示隔離或移除惡意檔案 • 更改被入侵的裝置／軟件／資料庫／系統的登入資料 • 若發生或有可能發生身份盜竊或其他刑事活動，將事件通報相關的執法部門
防止事故再次發生的措施	• 安裝兩層防火牆及啟用端點保護 • 使用最新的作業系統及防毒程式 • 為所有裝置（包括離線虛擬機器）安裝最新的保安修補程式及病毒識別碼 • 限制單一互聯網規約地址在一分鐘內向用戶登入頁面的請求次數 • 在登入頁面設立 CAPTCHA[1] 驗證碼抵禦暴力攻擊 • 定期進行備份 • 進行網絡分段，將企業網絡劃分為多個子網絡，並為每個子網絡設置特定所需及功能，員工只可按「需要知道」的原則查閱特定區域 1. CAPTCHA 是一個程式產生人類可通過，但現時電腦程式不能通過的測試來保護網站免受機器人攻擊。例如，人類可閱讀扭曲的文字但電腦程式不能閱讀。

資料外洩事故	電郵或郵件外洩
即時採取的補救措施	• 在可行的情況下，嘗試回收／取回有關電郵／信件 • 若未能回收／取回有關電郵／信件，立即通知並要求非預期的收件者刪除有關電郵／銷毀有關信件
防止事故再次發生的措施	• 採用四眼原則（即由另一員工覆核文件）以確保所有收件者姓名、聯絡資料、內容及／或附件均正確無誤 • 在可行的情況下，使用開窗信封作郵寄用途 • 減少在電郵內載有個人資料的類別 • 停用電郵系統內自動完成清單的功能，防止將電郵發送至相似但錯誤的電郵地址 • 妥善地將檔案命名以如實反映檔案內容，以減少在發送電郵時錯誤夾附檔案的機會 • 使用共享硬碟傳送內部載有個人資料的檔案 • 使用高強度的密碼保護載有個人資料的電郵附件，並透過電郵以外其他方式向收件者提供附件的密碼
資料外洩事故	員工行為失當
即時採取的補救措施	• 停用有關員工的帳戶／存取權限 • 若發生或有可能發生刑事活動，將事件通報相關的執法部門
防止事故再次發生的措施	• 安裝資料外洩防護系統／工具以掃描對外發出的電郵，及隔離載有敏感資料（例如香港身份證號碼及信用卡資料）的電郵，在發送有關電郵前須取得管理層的同意 • 只按個案情況、需要使用或職能需要的情況下，准許獲授權的人士查閱個人資料 • 在任何時間將限閱及機密文件鎖上 • 主動檢視系統日誌紀錄以便及早偵測任何異常情況 • 為離職員工帳戶進行資訊科技審計

資料外洩事故	防冒詐騙
即時採取的補救措施	• 切斷被入侵的裝置與互聯網及其他網絡的連接 • 使用防毒軟件為離線的電腦網絡進行掃描。不要理會任何提示你連接互聯網的訊息，若發現任何惡意軟件，依照防毒軟件的指示隔離或移除惡意檔案 • 更改被入侵的裝置／軟件／資料庫／系統的登入資料
防止事故再次發生的措施	• 不要回應任何要求你提供登入資料或敏感資料（例如銀行帳戶資料）的電郵 • 避免開啟任何可疑的電郵附件 • 小心檢查可疑電郵的域名 • 點擊電郵內的網址前，將鼠標懸停在網址上以檢視其連結網站，確定該連結的真實性 • 安裝反防冒詐騙及反濫發電郵軟件 • 安排員工接受個人資料保安方面的培訓
資料外洩事故	**程式錯誤或系統設定錯誤**
即時採取的補救措施	• 切斷有關程式／系統／平台的存取連接 • 若有關程式／系統／平台由第三者開發／維護，立即聯絡負責的供應商
防止事故再次發生的措施	• 在將程式／系統移至生產環境前，執行測試（包括綜合測試、用戶驗收測試）以核實有關程式／系統 • 定期及在有任何重大變更後，對系統進行漏洞掃描及滲透測試 • 定期檢查是否為檔案及文件夾設置了適當的權限 • 與業界中有良好信譽及紀錄的外判商簽訂合約／協議，有關合約／協議須包含完備的私隱保障要求