資料來源：香港個人資料私隱專員公署

資訊及通訊科技的保安措施指引（下）

“香港個人資料私隱專員公署透過《資訊及通訊科技的保安措施指引》，為資料使用者提供與資訊及通訊科技相關的資料保安措施之建議，以協助他們遵從《個人資料（私隱）條例》（第486章）（《私隱條例》）的相關規定。上期《香港印刷》已分享部分《指引》內容，今期將繼續介紹資料保安建議措施。”

資訊及通訊科技的資料保安建議措施

資料處理者的管理

將處理個人資料的工作外判予承辦商（即資料處理者）的做法日益普遍。資料處理者的例子包括雲端服務和資料分析服務的供應商。根據《私隱條例》第65（2）條，資料使用者有可能需對其代理人（包括資料處理者）的有關行為負責[1]。保障資料第4（2）原則亦規定，資料使用者須採取合約規範方法或其他方法，以防止轉移予資料處理者作處理的個人資料在未獲准許或意外的情況下被查閱、處理、刪除、喪失或使用。

資料使用者可在聘用資料處理者時考慮採取以下行動（非詳盡）：

- 實施政策及程序確保只聘用稱職且可靠的資料處理者[2]；
- 進行評估確保只有必要的個人資料轉移至資料處理者；
- 資料處理合同應明確規定資料處理者須採取的保安措施；
- 要求資料處理者在發生資料保安事故時立即作出通知；及
- 進行現場審核以確保資料處理者遵守資料處理合同，並對資料處理者違反合同的行為施加後果。

[1] 《私隱條例》第65（2）條規定，任何作為另一人（如資料使用者）的代理人（如資料處理者），並獲該另一人（即資料使用者）授權而作出的任何作為或所從事的任何行為，就《私隱條例》而言須視為亦是由該另一人作出或從事的。

[2] 視乎具體情況，措施可能包括（1）在聘用資料處理者前進行盡職審查，及（2）透過獨立並有信譽的認證，對資料處理者的能力進行審查，例如 ISO/IEC 27000 系列的資訊安全管理系統標準。

資料處理者的管理

案例

2014年5月，一家銀行在廣州的外判電話服務中心的一名前僱員在網誌上發佈了三名香港名人的個人資料。

事件發生後，銀行禁止員工在電話服務中心使用智能電話和相機，並要求所有員工在進入電話服務中心前將其個人物品放進可上鎖的櫃內。該銀行更將電話服務中心的巡邏次數增加了一倍，並要求所有員工完成有關資料保安的電子學習課程。

有關管理資料處理者的更多詳細資訊，請參閱私隱公署發出的《外判個人資料的處理予資料處理者》資料單張[3]。

資料保安事故發生後的補救措施

保障資料第4(1)(a)原則規定，資料使用者須採取所有切實可行的步驟以保障由其持有的個人資料，並強調資料使用者須注意一旦發生資料保安事故「便能造成的損害」。資料使用者在資料保安事故發生後採取及時和有效的補救措施，可能減低個人資料被未獲准許的或意外的查閱、處理或使用的風險，從而減輕對受影響人士（即資料當事人）可能造成的傷害。

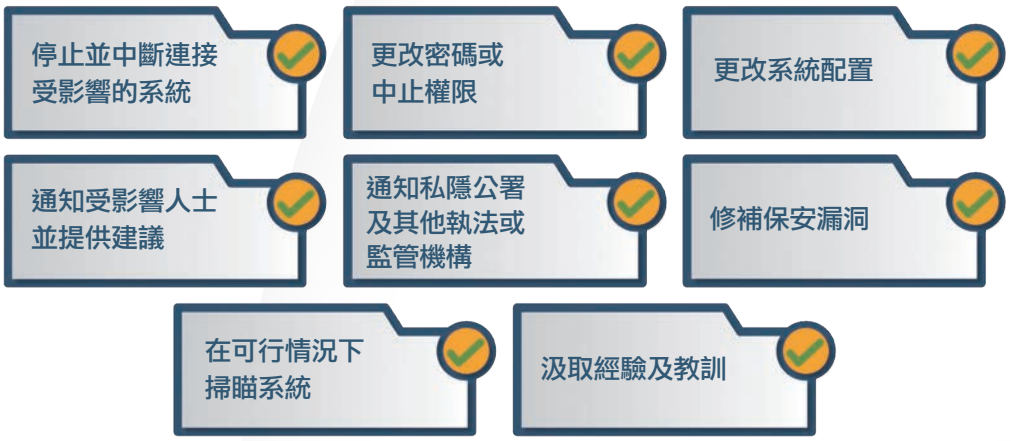
以下是資料使用者在發生資料保安事故時可採取的補救措施的一些常見例子：

- 在切實可行的情況下立即停止受影響的資訊及通訊系統，並將其與互聯網和資料使用者的其他系統的連接中斷；
- 立即更改涉嫌導致資料保安事故的用戶的密碼，或中止其存取權限；
- 立即更改系統的配置，以管制對受影響資訊及通訊系統的存取；
- 在沒有不當延誤的情況下通知受影響的人士，並向他們建議保障自己的可行辦法；
- 在沒有不當延誤的情況下通知私隱公署及其他執法機構或監管機構（如適用）；
- 適時修補保安漏洞；及
- 在可行並且在不影響未來調查取證分析的情況下掃瞄資訊及通訊系統，以查找任何其他未知的保安漏洞。

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。

[3] 請參閱：https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

發生資料保安事故時可採取的補救措施



有關如何處理資料外洩的詳細指引，請參閱私隱公署發出的《資料外洩事故的處理及通報指引》[4]。

監察、評估及改善

資料使用者可委派獨立的專責小組（例如內部或外部審計隊）負責定期監察資料保安政策的遵從情況，以及定期評估資料保安措施的成效。如發現違反政策的行為或保安措施成效不彰，應採取改善行動。

其他考慮

隨着數碼化工作場所的普及，在辦公室以外的地方工作越趨普遍（例如在家工作或其他遙距辦公方式）。在此情況下，資料有可能需要從資料使用者的資訊及通訊系統轉移出去，因而造成各種資料保安的問題。

雲端服務

第三方雲端服務供應商所提供的運算和資料儲存服務，既可降低資料使用者就資訊及通訊系統方面的成本，而又能提高其靈活性，故雲端服務越趨普及。

與傳統的資料處理者不同，雲端服務供應商可能無法為資料使用者提供度身訂造的服務。資料使用者作為使用標準雲端服務的眾多客戶之一，通常無法有效控制雲端服務供應商的營運和保安措施。儘管如此，資料使用者仍須為其採用雲端服務供應商代其持有的個人資料之保安負主要責任。

資料使用者應在使用雲端服務時採取以下措施，以確保雲端環境和個人資料的保安：

- 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正式的保證；
- 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；及
- 檢視雲端的現有保安功能，並啟用合適的保安功能，不要只依賴預設的保安設置。

[4] 請參閱：https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/DataBreachHandling2015_c.pdf

使用雲端服務時的考慮因素

自攜裝置

自攜裝置是一項機構性政策，允許員工使用屬於其個人的電子裝置（例如智能電話、手提電腦）查閱資料使用者的系統並處理其持有的資料。在此情況下，資料使用者實際上是把資料從保安良好的企業系統轉移至安全程度較低、亦較難以有效控制的員工設備上。在這情況下，資料使用者仍須為轉移到員工設備的個人資料完全負上遵守《私隱條例》的責任。

因此，資料使用者應設立行政和技術性措施以確保此類個人資料受到保障。資料使用者亦應通過明文政策和培訓，藉以加強這些措施的成效。為遵從《私隱條例》規定的資料保安責任，實施自攜裝置政策的資料使用者可採取包括以下保安措施：

- 盡可能避免資料使用者收集的個人資料存儲在自攜裝置設備內；
- 控制對儲存在自攜裝置設備內的個人資料的存取（例如，除了員工智能電話的屏幕鎖之外，再需要另外登入才能查閱）；
- 使用並非自攜裝置設備內建的加密方法來加密存儲在其中的個人資料；及
- 在自攜裝置設備上安裝適合的軟件，以便在丟失自攜裝置設備時可遙距刪除存儲在其中的資料。

制訂自攜裝置政策時可考慮的保安建議

避免儲存個人資料

控制個人資料的存取

容許遙距刪除資料

為個人資料進行加密

有關自攜裝置的更多資訊，請參閱私隱公署發出的資料單張《自攜裝置(BYOD)》[5]。

[5] 請參閱：https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/BYOD_c.pdf

便攜式儲存裝置

常見的便攜式儲存裝置包括便攜式硬盤，USB 記憶體和 SD 卡。便攜式儲存裝置提供一個便捷的方法儲存和轉移資料。不過，當資料使用者使用便攜式儲存裝置時，由於可以簡單且快速地複製和轉移大量個人資料至普遍來說有較佳保安的公司系統以外的地方，因而增加了資料保安事故的風險。

資料使用者應在切實可行範圍內避免使用便攜式儲存裝置來存儲個人資料。如有必要使用便攜式儲存裝置，為遵從《私隱條例》規定的資料保安規定，資料使用者可實施以下保安措施：

- 制訂政策，列明（1）允許使用便攜式儲存裝置的情況；（2）可轉移到便攜式儲存裝置上的個人資料的類別及數量；（3）使用便攜式儲存裝置的批准程序；及（4）轉移到便攜式儲存裝置的資料的加密要求等；
- 使用端點保安軟件防止資料從資料使用者的資訊及通訊系統轉移到不安全（例如沒有加密功能）或未獲批准使用的便攜式儲存裝置上；
- 保存便攜式儲存裝置的清單，並追蹤其使用和下落；及
- 在每次使用便攜式儲存裝置之後妥善地刪除當中的資料[6]。

使用便攜式儲存裝置時可考慮的保安建議

在政策中列明可使用便攜式儲存裝置的情況

使用端點保安軟件

保存便攜式儲存裝置的清單並進行追蹤

在使用後刪除便攜式儲存裝置中的資料

有關使用便攜式儲存裝置的詳細指引，請參閱私隱公署發出的《使用便攜式儲存裝置指引》[7]。

資料保安建議措施一覽

資料管治和機構性措施

制訂明確針對資料管治和資料保安的內部政策和程序

委任合適的領導人負責個人資料保安，並為資訊及通訊科技方面提供適當的人手配置

向工作人員提供有關《私隱條例》、資料保安政策及程序的足夠培訓

[6] 從便攜式儲存裝置中刪除的資料很容易可以通過特殊軟件恢復並再次讀取。 建議採取妥善的資料銷毀程序，從儲存設備中永久地和不可逆轉地移除資料。

[7] 請參閱：https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/portable_storage_c.pdf

風險評估

- 在啟用新系統和新應用程式前進行資料保安風險評估
- 就控制的個人資料備存清單，並評估有關資料的性質及風險

技術上及操作上的保安措施

- 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

資料處理者的管理

- 資料處理者的稱職及可靠程度
- 擬轉移的個人資料
- 資料保安事故的處理
- 合規及審核工作

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
- 在可行情況下掃瞄系統
- 汲取經驗及教訓

監察、評估及改善

- 監察資料保安政策的遵從情況，並定期評估資料保安措施的成效
- 採取改善行動

其他考慮

- 雲端服務
- 自攜裝置
- 便攜式儲存裝置

如想了解更多相關資訊，請聯絡香港個人資料私隱專員公署。

電話：+852 2827 2827

傳真：+852 2877 7026

電郵：communications@pcpd.org.hk

網站：www.pcpd.org.hk