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

指引資料

使用便攜式儲存裝置指引

導言

便攜式儲存裝置如USB記憶體、筆記型電腦或備份磁帶，為儲存及轉移個人資料提供了方便的途徑。不過，倘若沒有足夠的資料保障政策及措施規限此等裝置的使用，會增加私隱外洩的風險。

本指引旨在協助機構資料使用者在了解使用便攜式儲存裝置時，如何處理及保障個人資料。

甚麼是便攜式儲存裝置？

一般而言，任何可攜帶，並備有儲存或記憶功能的裝置，即屬便攜式儲存裝置。便攜式儲存裝置不限於USB記憶體，亦包括其他裝置類別，如平板／筆記型電腦、流動／智能電話、電子手帳、便攜式硬碟機，備份磁帶及光碟（例如DVD）。

資料保安的法律規定

《個人資料（私隱）條例》（下稱「**條例**」）附表1的保障資料第4(1)原則規定，資料使用者須採取所有合理地切實可行的步驟，以確保其持有的個人資料受保障而不受未獲准許或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮：

(a) 該資料的種類及如該等事情發生可造成的損害；

(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。

因此，資料使用者應採取步驟，管理有關使用便攜式儲存裝置的保安風險，以遵從保障資料第4(1)原則的規定。

保障資料第4(2)原則進一步規定，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]，以代行處理個人資料，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。

了解風險

容許使用便攜式儲存裝置，意味着大量的個人資料可以在不經意間快速及輕易地被複製到裝置內。若此等裝置遺失或盜竊，會產生資訊保安的風險，個人資料有可能會遭受未獲准許或意外的查閱或使用。在極端的例子中，即使便攜式儲存裝置已被重新格式化，過往被刪除或曾經儲存的個人資料亦可輕易地還原。

由上而下的策略

機構要管理有關使用便攜式儲存裝置的風險，應由上而下採取貫徹機構的政策。為方便制定政策，應首先進行風險評估。風險評估最少應涉及下述範疇：

(a) 儲存個人資料的便攜式儲存裝置是甚麼類型？

[1] 資料處理者指符合以下兩項說明的人－(a) 代另一人處理個人資料；及(b) 並不為該人本身目的而處理該資料。

(b) 便攜式儲存裝置內所儲存的是甚麼類別的個人資料？該資料對所涉人士的敏感程度如何？

(c) 在甚麼情況下使用便攜式儲存裝置儲存個人資料？使用便攜式儲存裝置的頻密程度如何？

(d) 如發生涉及便攜式儲存裝置的資料外洩事件，對資料當事人可能產生甚麼影響？

(e) 在使用便攜式儲存裝置方面，是否有任何行政或技術上的監控？

風險評估的結果有助制定相關的資料保障政策、實務指引及易於依從的程序。要確保整個系統的有效性，必須定期檢討及審核有關政策、指引及程序。

指引、程序及培訓

除非機構的政策是徹底禁止使用便攜式儲存裝置，否則機構應為使用者制定實務指引，以協助他們執行機構的政策。如使用者在依從機構的政策時須執行技術操作，機構應訂立程序，確保使用者正確執行有關操作。例如，若使用者需要利用某特定軟件將檔案加密至預定的加密標準，才可獲准將檔案儲存至便攜式儲存裝置，機構應向使用者提供逐步程序。此等程序會因應便攜式儲存裝置的類型而有別。

在制定政策、指引及程序後，機構必須為使用者提供培訓，以依從有關指引及程序，如使用者不依從，則須負上責任。

成文的政策

有關使用便攜式儲存裝置的政策應包括或針對下述事宜。下述事宜僅供參考，並非鉅細無遺：

避免風險

- 如不使用便攜式儲存裝置儲存個人資料，便可以避免資料外洩的風險。鑑於便攜式儲存裝置的固有風險，機構必須首先衡量風險，以決定是否有必要使用便攜式儲存裝置。

- 如需要使用便攜式儲存裝置儲存個人資料，但沒有需要鑑定或辨認其中某人的身份，便應研究使用內部標識方式的可行性，從而避免使用身份證號碼所帶來的資料外洩風險。

- 在決定儲存資料的範圍及詳細程度時，應有合理理由。例如，如只需使用部分資料庫，為何要把整個資料庫儲存在便攜式儲存裝置？在其他情況中，如只需要某人的一些基本資料，為何要把該人在資料庫中的全部資料儲存在便攜式儲存裝置？

- 機構必須採取步驟，減低所涉及的保安風險。機構應對下述事宜作出政策決定：

  - 是否要限制可使用的便攜式儲存裝置的類型，特別是考慮到不同的便攜式儲存裝置能提供不同的保安程度；
  - 只應准許使用由機構提供的便攜式儲存裝置（即禁止僱員使用私人的便攜式儲存裝置以避免資料被儲存於可能未達保安標準的裝置內，未能追蹤資料被儲存於何處，及共用私人儲存裝置時可能令個人資料被未獲准許的人士所查閱）；
  - 指定何等情況下使用；
  - 准許在便攜式儲存裝置上儲存或處理的個人資料的類別及數量；
  - 使用便攜式儲存裝置是否需要通過批核程序；
  - 僱員以外的使用者，例如承辦商、代理或義工，是否獲准使用便攜式儲存裝置；
  - 是否容許不同人士或處理程序均可共用同一便攜式儲存裝置；
  - 便攜式儲存裝置是否可被帶離機構的處所；
  - 在每次使用後，強制刪除便攜式儲存裝置內所儲存的資料等。

- 如要棄置便攜式儲存裝置，機構應永久刪除內裏儲存的個人資料。如要送往維修或更換，機構必須確定已損壞的便攜式儲存裝置內的個人資料不能被其他人取得，又或已與維修商訂明有關的保護個人資料條款。

防止未獲准許的查閱

- 儲存於便攜式儲存裝置的個人資料應予以加密，因為加密是最有效的方法，可以防止便攜式儲存裝置一旦遺失或被盜竊時，被非獲授權人士查閱資料。

- 在進行加密時，應小心考慮兩方面：

  加密算法－加密算法用於決定將資料轉化為難解形式時的複雜或困難程度。因此加密時應選擇強的算法[較複雜的加密法]。使用者須留意，為便於與舊版本兼容，有些軟件是預設了弱算法[較舊式簡單的加密法]的。

  加密機制－最佳的加密機制是可以強制執行加密，不能被使用者繞過或停用。如不能以技術強制執行加密，應制定足夠的政策及程序，以確保儲存在便攜式儲存裝置的所有資料是以強算法加密的。

- 不強的密碼或差劣的密碼控制措施（例如把寫在紙上的密碼與便攜式儲存裝置放在一起）會使加密保障未能發揮效果，機構應有政策，甚至可以以技術監控措施來確保用於便攜式儲存裝置的密碼，不論在長度或字母和數字組合方面都具一定的複雜程度。機構亦應就其他與密碼有關的事宜，例如是否需要為每一個便攜式儲存裝置設定不同的密碼、或密碼是否只提供予有需要知道的人士等，制定適合的政策或指引。

- 有些便攜式儲存裝置，例如電話及平板電腦，設有備用自動密碼鎖功能，作為存取控制（但此控制與加密不同）。使用者應啟用這項功能，以防止未獲授權的存取。

- 在每次使用便攜式儲存裝置後，以特別程式安全地刪除內存的資料，可以確保其後使用或接觸到有關裝置的人不能把資料還原。

- 便攜式儲存裝置時常會被遺留在公眾地方或在運送途中遺失。機構應提醒使用者小心看管其便攜式儲存裝置，並制定方法協助他們，例如為筆記型電腦提供鋼索鎖。此外，機構不應在便攜式儲存裝置貼上機構的標誌，因為此舉或會透露所儲存資料的價值。

- 除了基本連接外，有些便攜式儲存裝置亦具備其他方式的連接，如Wi-Fi、藍芽或流動電話網絡。機構應制定政策，控制或限制使用這些連接，以避免這些連接意外地披露資料或受到惡意攻擊。例如，若容許儲有個人資料的智能電話使用手機應用程式，這些應用程式會否在使用者不知道的情況下取得並公開電話內儲存的個人資料？

- 鑑於便攜式儲存裝置的弱點，若機構沒有制定相關的個人資料加密及防止資料遺失的政策，機構一般不會被視為未有根據保障資料第4(1)原則採取所有合理地切實可行的步驟，防止未獲准許或意外查閱便攜式儲存裝置內的個人資料。

偵測風險

- 如便攜式儲存裝置是由機構提供，機構應制定指引，列明使用者何時應交回有關裝置，以進行庫存檢查。機構應進行抽查，以確定使用者仍持有及沒有遺失或誤置所提供的便攜式儲存裝置。

- 制定通報遺失便攜式儲存裝置的正式政策，有助機構主動管理潛在的資料外洩事件。機構應為處理個人資料的使用者訂立強制性的內部通報規定，並應令使用者知悉有關規定。

- 機構應要求使用者盡快通報遺失事件。有些便攜式儲存裝置是可以支援以流動電話網絡遙距刪除資料的，但當機構獲通知遺失事件有延誤時，流動電話卡可能已被移除而令機構無法遙距刪除資料。

緊貼科技發展

- 與便攜式儲存裝置相關的政策應具體詳細，讓使用者知道該政策如何適用於特定類型的便攜式儲存裝置。鑑於科技發展迅速，機構應定期更新有關政策。如政策只適用於某類便攜式儲存裝置，機構應採取適當步驟，以避免因政策未涵蓋新式便攜式儲存裝置而在使用時所帶來的風險。

提醒員工留意政策及不依從政策的後果

- 為了落實政策，機構應採用有效方法定期把政策規定及不依從政策的後果通知使用者。

定期檢討及審核

- 要緊貼科技發展，機構應有正式的機制，定期對便攜式儲存裝置的風險評估、政策的相關性及範圍作出檢討。

- 為衡量便攜式儲存裝置政策的效用，機構應定期審核政策的施行及遵從程度。

技術監控措施

機構可以利用技術監控措施，協助施行便攜式儲存裝置的政策，例如：

端點保安－可以在所有電腦安裝端點保安軟件（用以監控端點裝置，如個人電腦、手提電話的保安），並由中央控制，以防止他人使用儲存裝置，如USB記憶體或光碟機。最基本的端點保安軟件可以阻止一切此等儲存裝置被使用。較精密的軟件容許對已批核的裝置進行讀取／寫入，而將其他裝置轉成唯讀裝置。最精密的軟件可以強制使用者在使用此等裝置前為檔案加密。過往經驗證明，單靠政策措施不能有效阻止使用者使用未獲准許的便攜式儲存裝置，因此機構應認真考慮採用端點保安軟件。

資料遺失防護系統－資料遺失防護系統可以偵測及阻止敏感資料被儲存到外置的儲存裝置，甚至是經電郵系統被傳送到外界。

庫存控制－庫存控制及盤點是很重要的，因為可以清楚知道所有便攜式儲存裝置的數目、類型及下落。此舉有助強化所有使用者對使用便攜式儲存裝置的責任感，並在發生遺失事件時，有助處理事件。

刪除／銷毀／再配置－在每次使用儲存於便攜式儲存裝置的資料後，應永久地刪除有關資料。除非便攜式儲存裝置已內置可以永久地刪除資料的系統，否則機構應採用最適當的軟件刪除資料。例如，專為刪除硬碟資料而設的軟件對刪除USB記憶體的資料不太有效。

資料外洩事故的處理及通報

雖然資料外洩事故並不在便攜式儲存裝置政策的範圍，但鑑於便攜式儲存裝置儲存資料的弱點，機構應就外洩事故的處理及通報制定正式政策。機構可參考專員發出的《資料外洩事故的處理及通報指引》[2]，該指引可從公署網站下載。

聘用服務供應商

如機構聘用的服務供應商會處理載有個人資料的便攜式儲存裝置，不論是作為營運的一部分，或是維修或棄置便攜式儲存裝置，相關機構作為主事人，須對服務供應商在處理受託的個人資料所作出的作為或所從事的行為負上責任[3]。

此外，保障資料第2(3)及4(2)原則規定，如資料使用者聘用服務供應商處理（包括刪除）個人資料，須採取合約規範方法或其他方法，以確保該服務供應商不會將轉移的個人資料保存超過所需的時間，及防止轉移的個人資料受到未獲准許或意外的查閱、處理、刪除、喪失或使用。

如需更多有關聘用服務供應商的資料，可參閱專員發出的《外判個人資料的處理予資料處理者》[4]資料單張。

香港個人資料私隱專員公署
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12樓
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk

[2] 請參閱http://www.pcpd.org.hk/chinese/publications/files/DataBreachHandling_c.pdf

[3] 見條例第65(2)條

[4] 請參閱http://www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf