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

個人資料的刪除與匿名化指引

引言

資料使用者在收集、持有、處理或使用個人資料的時候，同時須小心考慮當個人資料不再需要被用於使用目的時，應如何刪除該等個人資料。

此外，資料使用者在棄置載有個人資料的儲存裝置時，須小心確保當中的個人資料已被刪除及不能再被檢索。

本指引旨在就何時應刪除個人資料及應如何以電子刪除及/ 或實體銷毀方式永久刪除個人資料提供建議。

本指引亦介紹將資料匿名化以作為永久刪除個人資料的替代方式。匿名化是把個人資料除去識別資料，令直接或間接從該等資料識別個人的身份不再切實可行，在這情況下，該等資料不會受到《個人資料（私隱）條例》（下稱「條例」）的管限。

關於刪除個人資料的法律規定

條例第26條規定，凡資料使用者持有的個人資料是用於某目的（包括與該目的有直接關係的目的），但已不再為該目的而屬有需要的，則該資料使用者須刪除該等資料。

條例附表1的保障資料第2(2)原則規定，個人資料的保存時間，不得超過將其保存以貫徹該等資料被使用於或會被使用於的目的（包括任何直接有關的目的）所需的時間。

條例附表1的保障資料第4原則規定，資料使用者須採取所有切實可行的步驟，以確保其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響，尤其須考慮—

(a) 該等資料的種類及如該等事情發生便能造成的損害；

(b) 儲存該等資料的地點；

(c) 儲存該等資料的設備包含（不論是藉自動化方法或其他方法）的保安措施；

(d) 為確保能查閱該等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等資料而採取的措施。

條例第26條及保障資料第2(2)原則清楚訂明，個人資料不再需要用於使用目的時，資料使用者有責任刪除該等資料，令該等資料不會再被使用。

雖然保障資料第4原則主要關於個人資料的保安，但亦關乎安全刪除以紙張形式持有或儲存於會離開資料使用者控制範圍的儲存裝置內的個人資料（或其複本）。常見例子包括銷毀載有個人資料的文件記錄或影印本，或將過時的資訊科技器材棄置或循環再用。

資料使用者應注意，違反條例第26條構成罪行，違例者可被判罰款。

由上而下方式的重要性

載有個人資料的記錄或儲存裝置可透過不同途徑被帶離一間機構。機構須以由上而下的方式管理資料的刪除。這需要制定機構性的政策、指引及/或程序。如管理不是由上而下，那即使載有個人資料的記錄或裝置被帶離了機構，也可能不被察覺。

保留及刪除政策

為依從條例第26條及保障資料第2(2)原則，資料使用者應制定保留個人資料的政策，詳細訂明其持有的個人資料的保留期限。與此同時，資料使用者應制定刪除個人資料的政策，以根據保留政策列明刪除或銷毀個人資料的時段。

刪除政策所涵蓋的記錄類型應較保留政策為廣，因為刪除政策應顧及保障資料第4原則的規定，以確保資料使用者不再需要的個人資料複本（例如面試小組成員用畢的求職表格影印本）應妥善及安全地棄置。刪除政策亦應顧及如何安全穩妥地刪除或銷毀不再需要的電子及紙張記錄，以及如何處理過時或損壞的儲存裝置。

刪除政策還須顧及保存刪除記錄的需要，以證明已遵從政策刪除記錄。刪除記錄應記下哪些記錄已被刪除或銷毀、刪除或銷毀的時間、負責人及方式。資料使用者應小心確保刪除記錄本身不會透露過多原本應刪除的個人資料（例如求職表格的銷毀記錄不應載有求職者的姓名）。

安全穩妥地刪除資料

資料使用者應制定指引及/ 或程序（視屬何情況而定），指明何種類型的記錄應採用何種刪除方法。刪除目的是徹底刪除或銷毀個人資料，令它們不可能再恢復原貌。因此，所採用的方法必須配合儲存技術的類型。

關於紙張記錄，應採用交叉切割的碎紙方式而不是條狀碎紙方式，令紙張不能逐一重組。資料使用者亦須決定要將切碎的廢紙特別處理抑或是與辦公室一般垃圾一併棄置。另一個需要小心考慮的問題是，銷毀紙張式記錄應在機構處所內還是別處進行（如屬後者，會涉及把個人資料運送至資料使用者的處所以外地方）。

就電子記錄而言，資料使用者須採用適當方法，從每種特定類型的電子儲存裝置永久刪除資料。簡單的刪除檔案或將硬盤及USB記憶體重定格式，並不是可靠的刪除資料方法，因為現時常見的第三者軟件已可以把資料完全恢復。因此，公署建議資料使用者購買或下載專用軟件，例如符合美國國防部的刪除標準（DoD 5220.22-M標準）的軟件，以永久刪除在不同儲存裝置（例如硬盤或USB記憶體）內的資料。這類軟件可能需要較長的時間（以小時計）才能刪除裝置內的資料，但效果安全可靠。就伺服器內的記錄而言，資料使用者應選擇適當的方法刪除資料，須留意伺服器可能具備能救回已被刪除記錄或檔案

的功能（例如某些伺服器的「取消刪除」指令可以用來恢復伺服器內之前被刪除的檔案）。

實體銷毀是刪除電子記錄的有效方法（典型方式是在整個媒體上鑽孔或將磁性媒體放到消磁器，把其磁性完全隨機化）。這個方式特別適合用於資料使用者不能再以電子方式查閱的記錄。這類例子包括資料使用者沒有適合的裝置閱讀或刪除的備份磁帶，及已損壞的硬盤或USB記憶體。由於實體銷毀方式會令有關媒體不能再循環使用，資料使用者可視這方法為終極方法。

刪除整體記錄

在依從條例第26條及保障資料第2(2)原則刪除個人資料時，必須一併刪除有關個人資料的所有複本。這包括有關個人資料的所有影印本、備份或數碼複本。保留政策或刪除政策應指明如何識別、收集及記錄所有這些複本以保證刪除方法的全面性。

整體方式

保留期完結及棄置剩餘記錄和儲存裝置不一定是刪除資料的唯一原因。其他不太明顯的情況包括把已損壞的硬盤交予提供以舊換新服務的維修商。雖然這些硬盤未必能在資料使用者處所內的電腦或伺服器內接駁使用，但維修商可以把這些裝置復修、翻新或轉售，而資料則仍留在硬盤內。資料使用者必須採取步驟，防止這類資料外洩情況出現。

此外，儲存裝置可以以不同形狀及大小出現於不同類型的器材中，包括內置儲存功能的打印機及影印機，以及便攜式儲存裝置，如智能電話（包括記憶卡）、USB記憶體、相機記憶卡、平板電腦及音樂播放器。如機構內容許使用這些裝置，它們有機會被用來儲存或轉移個人資料。

因此，保留及刪除政策應定期予以檢討，以配合工作程序及科技發展，令被刪除的個人資料不能再恢復原貌，亦不會發生檔案在資料使用者不察覺的情況下被帶離機構。

循環再用

資料使用者有時會忽略與循環再用有關的資料外洩風險。把載有個人資料的打印文件循環再用，可導致此等個人資料落入未獲授權的人士手中。同樣地，沒有妥善刪除之前用作處理個人資料的電腦設備內的資料，而把電腦再調配他人使用，可導致個人資料外洩。資料使用者在這方面必須制定清晰政策及措施，讓僱員明白風險及知道如何防止資料外洩。

聘用服務供應商

雖然資料使用者可以把刪除資料工作外判予服務供應商（因可能涉及特別器材而有需要外判），但根據本地及海外經驗，這項安排必須小心處理。

經驗顯示，很多資料使用者將刪除資料的工作外判予服務供應商時，以為亦把保護器材內的個人資料的承擔或法律責任外判。這導致他們沒有監察或檢查服務供應商的工作，甚至在有些情況中，他們沒有與服務供應商簽訂任何合約。條例第65(2)條清楚規定，任何作為另一人的代理人

（即服務供應商）並獲該另一人授權（不論是明示或默示）所作出的任何作為，須視為亦是由該另一人作出的。資料使用者因此必須採取切實可行的步驟，確保他們所聘用的服務供應商有足夠的保障措施，保護受委託的個人資料的安全。為履行這責任，資料使用者須與刪除資料的代理簽訂正式合約，最低限度在合約中訂明(i)有關運輸及處理個人資料的保安規定；(ii)刪除標準及服務水平；及(iii)確保所有個人資料是按合約規定而刪除的機制。

僱員的意識

在這個分散處理資料的年代，資料使用者經常需要容許其僱員查閱及下載大量由資料使用者所持有的個人資料。因此，僱員知道並遵守機構的資料保留及刪除政策是非常重要的。機構必須定期進行足夠的培訓，提高僱員的意識，確保他們做好本份。

刪除與匿名

要處理資料使用者不再需要用於使用目的的個人資料，完全刪除並不是唯一的方法。基於各種原因，特別是為了研究及/或統計目的，資料使用者可能希望保留部分資料。只要持有的個人資料被永久匿名，而其程度令資料使用者（或任何其他人）不能直接或間接識別相關的個人，那麼該等資料便不會被視為個人資料，不會受到條例的規管。

把個人資料永久匿名是指從個人資料移除可以被閱讀記錄的人士識別出某人的任何資料。永久匿名亦指資料使用者不能利用其現有或日後的資料重組出該人的身份。這意味每當資料使用者向同一人收集新類型資料後，便需檢討資料的匿名程度。

只移除資料中的姓名、地址或其他明顯的身份代號並不足以令資料完全匿名。如資料包含個人的複雜或獨特描述，即使其他人沒有得到含有明顯識別代號的資料，也可以識別有關個人。例如，假若資料是關於一小撮人，如某班別的學生，只要保留某些間接的識別代號，例如他們的居住地區，也可以合理地確認有關人士。

此外，在配對技術的發展下，資料使用者或第三者或許可以透過公開取得的其他資料，確定或合理地確定個人的身份。因此，資料使用者必須小心考慮是否向其他人或公眾發放已被匿名化的資料。

資料使用者必須知道，使用匿名方式而不是刪除方式會帶來風險，別人日後或可從該等資料再識別出有關人士的身份。保留匿名資料的好處必須大於該等資料日後或會被用來識別身份的潛在風險。因此，資料使用者必須定期檢討匿名資料是否可以用來再識別身份，以便根據條例採取適當行動，保障個人資料。

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

12/11