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

資料使用者收集、持有、處理或使用個人資料而不再需要使用該資料於原來目的時，應小心考慮如何刪除不再需要的個人資料。

此外，資料使用者棄置載有個人資料的儲存工具時，亦須採取切實可行的步驟確保當中的個人資料已被刪除，及不能再被讀取。

本指引旨在建議就何時應刪除個人資料；以及如何用電子刪除及／或銷毀實體方式永久地刪除個人資料。

本指引亦介紹將匿名化作為永久刪除個人資料的替代方式。匿名化是指刪除個人資料中可識別身份的元素，令人無法切實可行地直接或間接地憑該資料識別個人的身份。在這情況下，該資料將不受到《**個人資料（私隱）條例**》（下稱「**條例**」）的管限。

與刪除個人資料相關的法律規定

條例**第26條**規定，當個人資料的使用目的再不符原初持有的需要（包括與其目的有直接關係），資料使用者須採取所有切實可行的步驟刪除該等個人資料（若任何其他法例禁止刪除該等資料，或該等資料基於公眾利益不應被刪除的情況則例外）。

條例附表1的**保障資料第2（2）原則**規定，資料使用者須採取所有切實可行的步驟確保個人資料的保存時間，不超過將該資料被使用於或擬用於某目的（包括任何直接有關的目的）所需的時間。

保障資料第2（3）原則規定，如資料使用者聘用不論是在香港或香港以外的資料處理者，以代處理個人資料，該資料使用者須採取合約或其他規範，以防止資料交予承辦商的保存時間超過處理該資料所需的時間。

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切實可行的步驟去保障個人資料，防止該資料在未經許可或意外地被查閱、處理、刪除、喪失或使用。特別要考慮的事項包括：

(a) 該資料的種類及如以上情形若發生可造成的損害；
(b) 儲存該資料的實際地點；
(c) 儲存資料的設備應引入保安措施（如透過自動化或其他方法）；
(d) 應有措施確保可查閱該資料的人有良好操守、審慎態度及辦事能力；及
(e) 應有措施確保資料的傳送安全。

保障資料第4（2）原則規定，如資料使用者聘用資料處理者，無論是在香港或境外，以代為處理其個人資料，資料使用者須採取合約或其他規範，防止資料處理者在處理個人資料時，資料未經准許或意外地被查閱、處理、刪除、喪失或使用。

第26條、保障資料第2（2）及2（3）原則清楚訂明，當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資料，防止資料的保存時間超過所需的時間。

雖然**保障資料第4原則**主要關乎個人資料的保安，但亦涉及如何穩妥地銷毀以紙張形式持有或以儲

存裝置形式記錄的個人資料（或其複本）。常見例子是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儲存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。

由上而下推行政策至為重要

機構就不同的原因而有需要銷毀個人資料，或棄置載有個人資料的實體檔案或儲存裝置。針對這些情況，機構須以由上而下的管理方式來處理資料銷毀。機構有必要制定全面的政策、指引及／或程序。若未能由上而下地管理，個人資料的記錄或儲存裝置有可能被保存超過實際需要的時間，或被隨意棄置。

保留及刪除資料的政策

為依從**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，提出特定管理的方式來鑑定各種需要被刪除的電子或實體紀錄。

刪除資料的政策亦應顧及**保障資料第4(1)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）妥善及安全地棄置。刪除資料的政策亦應顧及如何安全穩妥地刪除不再需要的電子紀錄或銷毀不再需要的紙張紀錄，以及如何處理過時或損壞的儲存裝置。

資料使用者應備有刪除個人資料的紀錄，以證明已遵從刪除資料的政策。刪除個人資料的紀錄應列明已被刪除或銷毀的資料種類、處理時間、負責人及方式。資料使用者應小心確保刪除個人資料的紀錄本身不包含個人識別碼（例如銷毀求職表格的紀錄可載有其他行政資料及某段時期就某空缺所收到的表格數目，但刪除紀錄內不應載有求職者姓名等個人識別碼）。

安全穩妥地刪除資料

資料使用者應視乎情況制定指引或程序，訂明哪類型的紀錄應採用哪種刪除方法。刪除目的是徹底移除或銷毀個人資料，令資料無法還原或修復。因此，須就不同的儲存技術媒體採用最適當的方法去刪除其所儲存資料。

以紙張紀錄為例，用交叉切割的碎紙方式，而非條狀碎紙方式，可令紙碎不能輕易地被重組。資料使用者亦須決定該把切碎的廢紙作特別處理或是與辦公室一般垃圾一併棄置。另一問題需要小心考慮的是，銷毀紙張紀錄的程序應在機構所在地還是別處進行（如屬後者，則涉及運送個人資料至資料使用者所在地以外的地方）。

同樣，就刪除電子紀錄，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中永久刪除資料。單靠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，因為現時常見的坊間軟件可以把資料復原。因此，公署建議資料使用者使用業界或認受性高的標準軟件（例如美國國防部的刪除標準，DoD 5220.22-M標準的軟件），以永久刪除儲存裝置（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。至於伺服器上的紀錄，應選擇適當的方法刪除，因伺服器可能具備能恢復已被刪除紀錄或檔案的功能（例如某些伺服器的「取消刪除」指令可恢復伺服器上曾被刪除的檔案）。

實體銷毀是刪除電子紀錄的有效方法（常用方法是在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）。這種方式特別適合不能再以電子方式查閱的紀錄，例子包括資料使用者沒有適合的裝置閱讀或刪除的陳舊備份磁帶，已損壞的硬盤或USB記憶體。由於實體銷毀方式通常會令有關媒體不能被循環使用，故此資料使用者或會視這方法為刪除紀錄的最後一着。

刪除個人的整體記錄

在依從**第26條**及**保障資料第2(2)原則**刪除個人資料時，該資料的所有複本亦應一併刪除。這包括該資料所有影印本、備份或數碼複本。保留政策或刪除政策應指明如何識別、收集及記錄所有複本，以保證刪除徹底。在某些情況下，銷毀儲存於備份裝置內的個別無需保留資料是不切實可行的，例如不同保留期限的紀錄儲存於同一個備份磁帶或微型膠卷內。在這情況下，資料使用者應該本著尊重資料保障原則的精神，訂立管理政策和行事方式，以確保不再讀取及／或使用無需保留的資料。

整全性的考慮

刪除資料不一定是限於資料的保留期屆滿，及要棄置多餘的紀錄和儲存裝置。一些不為意的情況可以包括把損壞的硬盤以舊換新的形式交予維修商。雖然資料使用者未必再能在機構內的電腦或伺服器再使用這些硬盤，但維修商可以把這些裝置復修、翻新或轉售，而資料則可能繼續留在硬盤內。資料使用者必須採取步驟去減低風險。

此外，各式各樣的儲存裝置存在於不同的器材中，這包括內置儲存功能的打印機及影印機、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等便攜式儲存裝置。機構應該訂立正式的便攜式儲存裝置及手提裝置的使用政策以監管此類由機構提供裝置的使用，保安及資料刪除程序。

若機構容許工作人員在工作時使用其個人的電子裝置(如電腦，平板電腦，手機等)，機構應訂一個自攜設備使用政策以監管其一切的運作，除一般使用及保安程序外，亦需包括裝置遭棄置、遺失、或使用者離職等情況時，裝置上的資料應如何刪除。

另外，機構需要定期檢討保留及刪除政策，以配合工作程序及科技發展，確保已經刪除的個人資料不能再復還原，以及確保載有個人資料的儲存裝置不會在資料使用者不察覺的情況下被棄置。

循環再用

資料使用者有時會忽略循環再用資源會帶來資料外洩的風險。當載有個人資料的打印文件循環再用之時，個人資料可能會落入未獲授權的人士手中。沒有妥善刪除電腦設備的資料，而把電腦調配給新用戶使用，亦可導致個人資料外洩。資料使用者在這方面必須制定清晰的政策及措施，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

資料使用者可能會把實際的刪除資料的工作外判予服務供應商(例如因為涉及特別的器材而有需要外判)，這方面的安排必須小心處理。

根據本地及海外經驗，很多資料使用者將刪除資料的工作外判予服務供應商時，錯誤地以為其保障個人資料私隱的承擔或法律責任都一併轉移予服務供應商，因而疏於監察服務供應商的工作。在某些個案中，資料使用者甚至沒有與服務供應商簽訂任何合約。條例**第65(2)條**清楚規定，代理人(例如服務供應商)獲授權(不論是明示或默示)所作出的任何作為，須視為是該授權人所作出的。

此外，**保障資料第2(3)**及**4(2)原則**均規定，聘用服務供應商處理個人資料的資料使用者須採取合約或其他規範方法，以確保該服務供應商依從條例的相關規定。資料使用者最低限度應在刪除服務合約中訂明(i)有關運輸、運送及處理個人資料的保安規定；(ii)刪除資料的標準及服務水平；(iii)確保所有個人資料按合約規定刪除的機制；及(iv)不依從合約條款的後果。有關合約條款的更多資訊，請參閱私隱專員發出的《外判個人資料的處理予資料處理者》資料單張[1]。

[1] 請參考www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf

僱員的意識

於現今科技世代，資料使用者常會准許其僱員查閱及下載大量其機構持有的個人資料。因此，僱員應意識到及遵守機構的資料保留及刪除政策是非常重要的。機構必須定期提供培訓，提高僱員的意識，確保他們做好本份。

銷毀資料與將資料匿名化

資料使用者要處理其不再使用於原來目的之個人資料時，完全刪除並不是唯一的方法。基於種種原因，例如為研究及／或統計目的，資料使用者可能希望保留部分的個人資料。把持有的個人資料匿名化，以致資料使用者（或任何其他人）不能直接或間接憑資料識別相關的人士，那麼該資料便不會被視為條例所界定的「個人資料」。

把個人資料匿名化，是指從個人資料移除當中任何可令人讀取後，而足以識別出某人身份的資料。匿名化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。然而最重要的是，資料使用者應以清晰政策承諾，禁止該等匿名資料有機會被重組而確立資料當事人的身份，或禁止資料在重組後會再被使用。

移除資料中的姓名、地址或其他明顯的身份識別代號（包括生物識別數據）並非徹底的匿名化。若相關資料包含對某人較複雜或獨特的描述，即使其他人沒有掌握明顯的身份識別代號，也可憑資料識別當事人。舉例說若資料涉及一個群組，如某班別學生的資料，只要當中保留某些間接的識別代號，例如居住地區、就讀年份、學業成就等，便足以可確認有關人士的身份。

此外，隨著資訊科技的發展，資料使用者或第三者可利用公開取得的資料以確定或合理地確定資料當事人的身份。為免發生這情況，資料使用者必須小心考慮應否向其他人或公眾發放已被匿名化的資料。

資料使用者必須明白，將個人資料匿名化而沒有刪除資料有着潛在風險：別人日後或可從該資料再識別出資料當事人的身份。在這個「大數據」年代，是否可以在龐大數據庫內，把某人的個人資料真正有效地匿名化逐漸受大眾關注。資料使用者保留匿名資料的好處，必須超於該資料日後可被利用來識別個別人士身份的潛在風險。因此，資料使用者必須定期檢討匿名資料是否有機會被用作識別身份，及此等識別行為所帶來的衝擊，並根據條例採取適當的行動，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：enquriy@pcpd.org.hk