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（上）

隨着資料數碼化趨勢加速、資訊及通訊科技的互聯互通，以及資料本身的價值不斷上升，個人資料保安的風險亦隨之而增加。近年在香港和其他司法管轄區所發生的資料保安事故呈上升趨勢亦證明這一點。個人資料私隱和資料保安有着密切的聯繫 —— 若資料保安的措施不足，個人資料便很可能會落入不法之徒手中，個人資料私隱將受到威脅。不論資料使用者是中小企業還是跨國企業，資料保安事故都可在聲譽及財務兩方面為其帶來嚴重後果。

此外，穩健的資料保安系統是構成良好資料管治的一個重要元素，而資料管治亦逐漸被視為企業社會責任不可或缺的一環。有見及此，香港個人資料私隱專員公署（下稱：私隱公署）經常在其提倡的私隱管理系統中強調問責的重要性，該系統主要由機構和管理層的決心、資料保安、資料外洩的處理等所組成[1]。

以下指引旨在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）（下稱：《私隱條例》）的相關規定。指引同時就加強資料保安系統方面向資料使用者提供良好行事方式的建議。《香港印刷》將分兩期分享關於《私隱條例》規定和相關的保安建議措施。

[1] 有關私隱公署私隱管理系統的詳情，請參閱私隱公署的專題網站：https://www.pcpd.org.hk/pmp/guide.html

UPM Finesse classic matt 80gsm

掃描二維碼
查閱《私隱條例》

《私隱條例》的規定

有關資料保安的規定

《私隱條例》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，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、喪失或使用所影響。尤其須考慮：

- 該資料的種類及如該等事情發生便能造成的損害；
- 儲存該資料的地點；
- 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；
- 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
- 為確保在保安良好的情況下傳送該資料而採取的措施。

「切實可行」是指「合理地切實可行」[2]。在發生資料外洩的情況下，資料使用者有責任證明他們已採取所有合理地切實可行的步驟以保障個人資料的安全。至於何謂「合理地切實可行」的步驟，將視乎每個個案的案情而定。

在評估資料使用者是否已採取「所有切實可行的步驟」以保障其持有或控制的個人資料的安全時，私隱公署會採用「衡量整體情況」的方法，並考慮以下因素（非詳盡，而各因素的重要性因個案而異）：

- 所涉及的個人資料的數量、種類和敏感度，以及在發生資料保安事故時可能造成的損害[3]；
- 資料儲存的地點[4]；
- 所用資訊及通訊科技的性質和複雜性[5]；
- 資料保安措施對於相關資料使用者擁有的資源而言是否足夠穩妥[6]；
- 資訊及通訊科技與相關行業對當前的資料保安問題的熟悉度，以及有否可用的解決方案[7]；及
- 資訊及通訊科技和資料保安的發展狀況[8]。

有關私隱公署針對資訊及通訊科技所建議的資料保安措施，本文接著將作詳細介紹。

---

[2] 《私隱條例》第2（1）條。

[3] 相關的規定為《私隱條例》附表1的保障資料第4(1)(a)原則，當中要求機構考慮資料的種類，以及一旦發生資料保安事故可能造成的損害。資料保安事故發生可能造成的損害很大程度上取決於所涉及個人資料的數量及敏感度。機構需要採取的步驟，必須與資料的敏感程度以及未獲准許的或意外的查閱該資料可能造成的損害成正比。例如，涉及大量敏感個人資料的外洩很可能對受影響的個人造成嚴重損害，因此，機構需採取更有力及更嚴格的保安措施來防止該些資料外洩。

[4] 詳見《私隱條例》附表1的保障資料第4(1)(b)原則。例如，如果存儲個人資料的處所可讓人輕易進入，則必須增強保安措施以限制資料的存取。

[5] 關於資訊及通訊系統的性質，《私隱條例》附表1的保障資料第4(1)(c)、(d)及(e)原則適用。至於資訊及通訊系統的複雜性，複雜的系統通常比簡單的系統更大機會有保安漏洞，因此需要更有力的保安措施。系統是在線或是離線亦有關連。在線的系統往往更容易受資料保安事故影響，並需要採取更有力的保安措施。

[6] 例如，私隱公署或會接受小型企業所採取的資料保安措施不如大型企業般精密，因為這樣對小型企業而言或許並非合理地切實可行。然而，此並不表示小型企業在資料保安方面可以不嚴謹。

[7] 例如，未能識別和修補一個眾所周知的漏洞，便可能違反了《私隱條例》規定的資料保安責任。

[8] 例如，隨着資訊及通訊科技不斷的發展和網絡攻擊的演變，機構應及時更新和升級其資訊及通訊科技，以確保其安全。

《私隱條例》其他相關規定

在保障資料第4原則對個人資料保安設下明確法律規定的同時，《私隱條例》的其他條文同樣關聯到資料保安。就「收集最少量資料」這一基本原則，保障資料第1（1）原則訂明，資料使用者只應為收集資料目的收集足夠但不超乎適度的資料。一般而言，資料使用者最初收集或保留的資料越少，日後的安全風險便越低。

在資料保存方面，保障資料第2（2）原則要求資料使用者採取「所有切實可行的步驟」，以確保個人資料的保存時間不超過將其保存以貫徹該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。《私隱條例》第26條亦要求資料使用者採取「所有切實可行步驟」刪除不再為使用目的而需要的個人資料（訂明的例外情況除外[9]）。透過制訂資料保留政策來確保適時刪除不再需要的個人資料，將有助減低資料外洩風險。資料使用者持有的資料越少，受攻擊或出現漏洞的風險便越低。

保障資料第2（3）及第4（2）原則要求資料使用者採取合約規範方法或其他方法，以確保他們聘用的資料處理者遵從資料保安和保存資料兩方面的類似規定。有關施加予資料處理者的建議合約責任，以及透過「其他方法」遵從規定的建議，資料使用者可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[10]。

個人資料保安在整個資料周期中至為重要。以上所列並非《私隱條例》有關資料保安的全部規定。

資訊及通訊科技的資料保安建議措施

資訊及通訊科技的七大資料保安建議措施

1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

資料管治和機構性措施

政策及程序

資料使用者應制訂明確針對資料管治和資料保安的內部政策和程序，並涵蓋以下範疇：

- 員工分別在維護資訊及通訊系統和保障資料安全的角色和責任；
- 資料保安風險評估；
- 資訊及通訊系統中資料的查閱和輸出；
- 外判資料處理及資料保安工作；
- 應付資料保安事故，包括事故應變計劃[11]和通報機制；及
- 銷毀不再為收集資料時所訂明的目的或相關目的而需要保留的資料。

[9] 《私隱條例》第26條下的例外情況包括：
(a) 該等刪除根據任何法律是被禁止的；或
(b) 不刪除該資料是符合公眾利益（包括歷史方面的利益）的。

[10] 載於此網站：https://www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf。

[11] 資料保安事故應變計劃是一套包括程序、章程及指引在內的計劃，助機構應對資料保安事故並從中恢復，務求將損害減至最低。

資料管治和資料保安的內部政策和程序

在評估及制訂資料管治和資料保安政策時，資料使用者可參考信譽良好的機構所制訂的標準和最佳行事方式，例如 ISO/IEC 27000 系列的資訊安全管理系統標準，以及由本地及其他司法管轄區有關機構發出的指引或建議[12]。當中 ISO/IEC 27701:2019 作 為 ISO/IEC 27001 及 ISO/IEC 27002 的延伸，提供了詳細的指引以協助各機構建立、執行、維護及持續改善其私隱資訊管理系統。不過，私隱公署強調保安措施是否足夠須視乎個案情況而定。

資料使用者應根據當時普遍適用的情況，例如行業內的新標準和資料保安的新威脅，定期和及時地覆檢與修訂其有關資料管治和資料保安的政策與程序。

人手

資料使用者應委任合適的領導人物（例如首席資料官、首席私隱官或同等人員）負責個人資料保安，並應為資訊及通訊科技（包括資訊及通訊科技安全）方面提供適當的人手配置。資料使用者應制訂指引列出：

- 資料使用者處理的個人資料從收集到銷毀的整個資料周期；
- 有關人員的角色和責任；
- 決策的權力分配；及
- 有關查閱和轉移個人資料的問責和監督權。

負責資料保安人員的數量、資歷及技術能力應與資訊及通訊科技和資料處理活動的性質、規模、複雜性，以及資料保安風險等合乎比例。

合乎比例的人員配置

資料使用者亦要注意其員工的審慎態度及誠信，以防因人為錯誤或內部攻擊而引致資料外洩。在適當的情況下，資料使用者可在僱傭合約中加入保密責任。

案例一

在私隱公署發佈的一宗循規審查個案[13]中，一家玩具製造商受到網絡攻擊後，成立了一個由集團主席為首的資料保安管治委員會，以決定有關資料保安政策的事宜、監督有關政策的實施、並定期進行覆檢。

[12] 例如，內地的《個人信息安全規範》(GB/T 35273-2020) 於 2020 年 10 月實施，並按資料生命周期不同階段列出資料安全措施的技術標準。

[13] 有關個案的詳情，請參閱私隱公署 2016-2017 年報第 38-39 頁：
https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport17_full.pdf

培訓

工作人員應在入職時及往後定期接受足夠的培訓，以確保他們熟悉《私隱條例》的規定，以及資料使用者的資料保安政策及程序。培訓類型可包括：

- 有效的密碼管理；
- 加密軟件的使用原則和正確用法；
- 便攜式儲存裝置和遙距存取工具使用原則和正確用法；
- 將資料永久銷毀的原則和相關工具的正確用法；
- 識別並小心可能含有有害內容的可疑超連結、二維碼及附件；
- 社交工程、詐騙電子郵件、勒索軟件或虛假網站所帶來的風險；
- 只使用經資料使用者內部核准而非其他的軟件；及
- 社交媒體和互聯網的適當使用。

為加強並鞏固員工的警覺性，企業亦可以將「演習」納入資料保安培訓。例如，企業在提供有關釣魚詐騙的培訓後，可透過安排「釣魚襲擊活動」來模擬工作場所內發生網絡騙案，繼而提高員工的警覺程度。此舉將有助建立一道「人力防火牆」，以抵禦網絡犯罪分子的新式行騙手法。

風險評估

資料使用者應在啟用新系統和新應用程式前，以及在啟用後定期根據既定的政策和程序進行資料保安風險評估。

缺乏相關專業知識的中小企應考慮聘用第三方專家，以進行安全風險評估。

風險評估的結果應定期向高級管理層匯報。

UPM Finesse classic matt 80gsm

資料使用者應就其控制的個人資料備存清單，並評估有關資料的性質，以及有關資料被洩露可能導致的損害。資料使用者尤其應在收集敏感資料[14]前作慎重考慮，確保只收集必要的資料並對資料提供更穩妥的保障（例如以加密的形式儲存在獨立、安全的資料庫中）。

在風險評估中發現的保安風險應及時處理。

技術上及操作上的保安措施

根據資訊及通訊科技和資料處理活動的性質、規模和複雜性，以及風險評估的結果，資料使用者應採取足夠及有效的保安措施，以保護其控制或所持有的個人資料和資訊及通訊系統。

以下提供一個詳盡的清單，列出資料使用者在確保資料保安時可考慮採取的技術及操作措施，以供參考。資料使用者並不一定要採取以下所有保安措施才能達到保障資料第4（1）原則所要求的「所有切實可行的步驟」的門檻，而全面採取以下所有保安措施亦不一定代表能達至上述的門檻。保安措施是否足夠取決於每宗案件的具體情況。

保護電腦網絡

- 採納實體存取控制措施以限制處所、房間、資訊及通訊科技設施（例如伺服器房和系統設備）的進出及使用。
- 使用保安裝置或軟件（例如防火牆及/或反惡意軟件應用程式）以保護電腦網絡。定期更新軟件（包括電話應用程式及反惡意軟件應用程式）來偵測新病毒及威脅。
- 使用端點保安軟件以防止用戶在網絡執行未獲授權的、並會對網絡帶來風險的應用程式/操作。
- 定期對網絡、伺服器和應用程式進行漏洞掃瞄以識別漏洞，並適當地採取跟進行動。
- 實施修補程式的管理，以適時修補保安漏洞。
- 進行定期審查/覆檢，以確保系統設定已更新並符合當前的要求。
- 記錄系統活動，以用於偵測和調查資料保安事故。

案例二

在私隱公署發佈的一宗循規審查個案[15]中，某酒店集團的信用卡系統遭連日惡意軟件的攻擊，導致使用了信用卡購買產品和服務的顧客的姓名和信用卡號碼懷疑遭外洩。法證調查顯示，黑客使用了有管理權限的系統帳戶在全球系統中放置了惡意軟件，以獲取信用卡資料。

事件發生後，該酒店集團採取了各種措施以加強其網絡保安，其中包括防止在其網絡執行任何未經授權的代碼及/或軟件，對系統管理員和遙距存取帳戶進行定期審核，以及增加對外網絡連接的限制以防止惡意流量。

資料庫管理

- 利用防火牆將資料庫伺服器與網絡伺服器分開，以在網絡伺服器受到威脅時保護內部伺服器。

[14] 一般而言，敏感資料是指基因資料、生物辨識資料，以及披露了種族或民族血統、政治取向、健康狀況、性生活狀況或性取向的資料；亦包括一旦處理不當便可能會對個人構成歧視或嚴重損害的資料（如信貸資料）。《私隱條例》並不區分敏感與非敏感的個人資料。但是，保障資料第4(1)(a) 原則要求機構在制定資料保安措施時，考慮有關「資料的種類」，以及如果發生資料保安事故時「便能造成的損害」。因此實際上，保障資料第4原則包含敏感資料的概念。

[15] 有關個案的詳情，請參閱私隱公署2015-2016年報第38-39頁：
https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport16_02.pdf

- 備存並定期更新個人資料清單，以便實施適當的資料保安措施。
- 資料集的分區——根據資料既定的屬性（例如敏感屬性）將資料集分割成更小的子集（故即使主要的資料庫的資料已遭洩露，被分割的資料也不會受到影響）。
- 數碼水印——在資料上添加水印，例如能夠識別資料集的始發者和證明檔案真實性的加密電子簽署（這使調查人員能夠在資料外洩時追蹤資料集的來源）。
- 禁止使用真實的資料進行測試。

存取管控

- 採用「最小權限」的原則，授予用戶盡可能少的存取權限以完成工作，並將適當的角色分配給用戶（即以角色為本的存取管控，包括限制存取資料的數量和時間）。
- 透過使用密碼、防火牆等對資訊及通訊系統進行有效的邏輯存取控制。
- 實施密碼管理以管理用戶密碼，包括強制密碼長度和複雜性、密碼歷史紀錄，並確保用戶遵循關於密碼保安的最佳行事方式。
- 制訂帳戶鎖定閾值策略來限制資訊及通訊系統允許登入失敗的次數，並在達到次數上限時封鎖帳戶一段特定的時間[16]。
- 對高風險的活動（例如遙距登入資訊及通訊系統和存取敏感資料庫）使用多重身份驗證或更高程度的存取管控。
- 定期覆檢存取權限並適時刪除不必要的帳戶和存取權限（例如在職員離職或重新調配職位時）。
- 如果不再需要遙距存取資料，則應切斷資訊及通訊系統與互聯網或內聯網的連接。

防火牆和反惡意軟件

- 使用域名系統（DNS）防火牆，防止資訊及通訊系統或其用戶連接到惡意網站。
- 定期（並足夠頻密地）對資訊及通訊系統進行保安漏洞評估及滲透測試，尤其是與互聯網連接的系統。
- 使用反惡意程式軟件為系統提供實時保護，防止各種惡意程式在系統上擴散。

保護網絡應用程式

- 避免於線上存儲不必要的個人資料。
- 當含有個人資料的系統已過時，將其網絡連接切斷。

加密[17]

- 正確地加密傳輸中和存儲中的資料，有效地管理和保護加密密鑰。
- 為流動裝置（例如智能電話）及便攜式儲存裝置（例如 USB 記憶體及外置硬碟）的資料進行加密。
- 代號化——將識別符及屬性轉換成只有已獲授權的用戶才能理解的數值（這適用於以後需要使用實際值的資料字段，例如個人的姓名）。
- 雜湊資料——使用算法得出理應不可逆轉的數值來取代敏感的數值，這適用於毋須恢復實際值的資料字段，例如密碼。（雜湊與一般加密不同，經雜湊的資料無法通過解密還原成原始資料。）

[16] 帳戶鎖定閾值策略設定會決定導致使用者帳戶鎖定的失敗登錄嘗試次數。 使用者必須重設鎖定帳戶，或直到帳戶鎖定持續時間政策指定的時間到期為止，才能使用鎖定的帳戶。

[17] 有關進行加密的方法，請同時參閱香港電腦保安事故協調中心於 2022 年 5 月發出的《數據保護指引》：https://www.hkcert.org/tc/security-guideline/data-protection-guideline

UPM Finesse classic matt 80gsm

電郵及檔案傳送

- 以密件副本功能（bcc / blind carbon copy）而非副本功能（cc / carbon copy）發出電郵，使收件者的資料（電郵地址或姓名）不會被其他收件者看見。
- 預防誤發電郵——安裝工具（例如資料外洩預防工具）確保任何可能屬高風險（例如有敏感資料）的郵件在發送之前已被仔細檢查，以防止資料透過電子郵件遭意外披露。
- 過濾濫發的、帶有惡意附件或鏈結的電郵。
- 使用端點保安軟件防止資料從資料使用者的電腦轉移到未獲批准使用或不設加密功能保障的便攜式儲存裝置上。
- 為載有敏感個人資料的檔案添加數碼水印（將重要資料嵌入檔案以追蹤擁有人，例如使用者資料、查閱時間 / 日期、所使用的裝置等），以防止資料喪失、被不當使用及未經授權地分享。

案例三

在私隱公署發佈的一宗循規審查個案[18]中，一名酒店員工無意中在一封提醒客戶領取訂購貨品的電子郵件內，附加了一份包含數百名客戶資料的文件。該文件既未加密也未受密碼保護。

事後回顧，該酒店應加密所有客戶資料文件並添加密碼，並且不應允許所有員工存取其客戶資料。

資料備份、銷毀及匿名化

- 備份含有必要資料的系統，並且確保恢復機制能有效地恢復失去的或因惡意 / 勒索軟件而無法存取的資料。
- 為安全地刪除資料，可以採用 NIST 800-88 R1（Guidelines for Media Sanitization）的清除操作。當中涉及物理或邏輯等技術，資料一旦清除，即使採用先進的實驗室技術也無法恢復[19]。
- 適時地銷毀或匿名化不必要的或過期的個人資料。

匿名化

匿名化是指利用技術使一項資料無法「合理地」與一位已識別或可識別的自然人聯繫起來。把個人資料「合理地」匿名化可被視為一種資料保安措施。要決定一項資料是否被「合理地」匿名化，資料使用者應考慮客觀因素（例如去匿名化所需的時間和技術）和個別的背景因素（例如有關現象的罕見性、牽涉人數的多寡和資料的多寡）。若所謂的「匿名化」資料未能通過合理性測試，有關資料將會被繼續視作個人資料。評估匿名化的穩健程度要考慮三項準則：

- 單獨挑出（即有關資料是否能令某個人從群體中被挑出）；
- 可聯繫性（即與同一個人有關的兩項資料是否能被聯繫在一起）；
- 推斷（即從有關資料是否可以很大確定性地推斷出某個人的未知資訊）。由於匿名化的程序複雜，因此資料使用者應提高進行匿名化方法的透明度。

[18] 有關個案的詳情，請參閱私隱公署 2013-2014 年報第 43 頁：
https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport14_02.pdf

[19] 請同時參閱香港電腦保安事故協調中心發出的《數據保護指引》：
https://www.hkcert.org/tc/security-guideline/data-protection-guideline

其他參考資料

- 關於開發資訊及通訊系統時應考慮的資料保安措施，可參考由私隱公署及新加坡個人資料保護委員會共同制訂的《資訊及通訊科技系統的貫徹資料保障設計指引》[20]。
- 有關資料保安的技術支援的資訊，可參考以下由香港政府的政府資訊科技總監辦公室維護的網站：
  - 網絡安全資訊站[21]；及
  - 資訊安全網[22]。
- Open Web Application Security Project（OWASP[23]）的十大項目中亦有關於常見的應用安全風險的有用見解。
- 有見物聯網技術的應用日益普及，香港電腦保安事故協調中心發出了《物聯網保安最佳實踐指引》[24]，以協助開發人員於物聯網裝置的設計和開發的早期階段採取適當的保安措施。用家在採購合適的物聯網解決方案時，亦可參考該指引就保安規格方面的要求。
- 香港電腦保安事故協調中心亦發出了《數據保護指引》[25]，就整個資料周期的資料保安提供全面指引。

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

[20] 請參閱：
https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf
（只有英文版本）

[21] 網絡安全資訊站：https://www.cybersecurity.hk/tc/index.php

[22] 資訊安全網：https://www.infosec.gov.hk/tc/

[23] OWASP 十大項目：https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project（只有英文版本）

[24] 請參閱：https://www.hkcert.org/tc/blog/implementing-iot-security-best-practice

[25] 請參閱：https://www.hkcert.org/tc/security-guideline/data-protection-guideline

UPM Finesse classic matt 80gsm