「自攜裝置」(BYOD)

摘要

「自攜裝置」是一項機構政策，容許僱員使用屬於其個人的流動裝置以查閱機構的資訊，當中包括機構所收集的個人資料。在本單張內，由機構收集所得的個人資料將統稱為「機構收集的個人資料」。

機構應留意下述與個人資料私隱有關的事宜：

1 在容許使用「自攜裝置」時，機構實際上是把機構收集的個人資料從具保安的企業系統轉移至保安程度較低的僱員自攜裝置，且機構對該「自攜裝置」亦較難有效管控。機構必須要明白，儘管這些個人資料是儲存在僱員本身所擁有的自攜裝置內，但就該些個人資料而言，機構仍須繼續負責遵守《個人資料(私隱)條例》(「**條例**」)的規定。因此，機構應透過制定行政、實質及技術措施，來確保該些個人資料受到保障，並透過書面政策、通知及培訓強化這些措施。

2 在保護由「自攜裝置」器材轉移或收集所得的個人資料時，機構須留意，該「自攜裝置」器材亦載有僱員本身、其家庭成員以至其他個別人士的私人資訊。任何機構所採取的保障措施亦應尊重這些私人資訊。

3 為履行條例下的責任，機構應考慮：

(a) 是否已充分提醒僱員不要濫用下載或儲存於「自攜裝置」器材內的機構收集的個人資料；

(b) 是否已有足夠的技術措施，容許「自攜裝置」器材查閱或儲存機構收集的個人資料的同時，亦能尊重私人資訊，例如：

(i) 是否有其他方法代替將機構收集的個人資料直接儲存到「自攜裝置」器材 — 資料可否儲存於公司系統，只經由「自攜裝置」器材查閱(而非儲存於「自攜裝置」器材內)？

(ii) 是否備有有效的控制系統供查閱個人資料 — 僱員須以用戶名稱及密碼登入後方可查閱機構的個人資料，使與其共用該「自攜裝置」器材的家人及其他人士無法查閱有關資料；及

(iii) 是否有採取保安措施(包括獨立加密)，以保障經「自攜裝置」器材查閱或儲存於「自攜裝置」器材的機構收集的個人資料，令未獲授權人士查閱「自攜裝置」器材時只接觸到已加密的個人資料。

4 若機構計劃容許使用「自攜裝置」，亦應考慮下述的良好行事方式：

(a) 制定「自攜裝置」政策，詳述其規管內容(例如機構與僱員的角色及責任、核准使用的程序等)；

(b) 進行風險評估(例如決定如何落實「自攜裝置」政策及措施)；

(c) 採用技術方案以減少或控制風險；及

(d) 設立監察及檢討機制，以確保當業務上有任何改變時，「自攜裝置」政策仍行之有效。

引言

「自攜裝置」的做法在機構中越來越普遍。當僱員使用屬於其個人的流動裝置（例如智能電話及平板電腦）來查閱僱主的公司資訊以執行職務，這些資訊便會從具保安的企業系統轉移至保安程度較低的僱員自攜裝置。本單張重點指出機構在制定「自攜裝置」政策時所須留意的個人資料私隱風險，並建議就容許僱員以「自攜裝置」器材查閱載有個人資料的企業系統以執行職務時的最佳行事方式。

基於「自攜裝置」器材的不同特點，亦涉及處理不同種類的機構資訊，加上資訊及通訊科技的急速發展，本單張所指出的議題及措施未必放諸四海皆準，因此讀者須因應個別的「自攜裝置」器材及其使用方式來考慮本單張內容的適用性。

由於本單張主要集中於個人資料私隱範疇的保障，因此有關使用個別「自攜裝置」的資訊科技保安詳情，讀者應參閱相關的技術或業界指引。

「自攜裝置」與條例

除了本單張指出的具體風險及控制措施外，使用「自攜裝置」儲存或處理個人資料的機構亦應了解六項保障資料原則[1]及其他規定。

機構可能已根據條例及六項保障資料原則的規定，就保障個人資料私隱制定一般政策；但把個人資料轉移及保留於「自攜裝置」器材，會對有關資料構成特定的私隱風險，例如：資料由具保安的企業系統被轉移至「自攜裝置」器材會帶來資料保安的風險。儘管這些個人資料是儲存於由僱員所擁有的裝置內，但就該個人資料而言，機構仍有責任遵守條例的規定。如果機構要遙距管理僱員的「自攜裝置」器材或在器材遺失時追蹤其位置，僱員儲存於「自攜裝置」器材的私人資訊便會「反向」傳到機構的系統。此舉對僱員的個人資料私隱構成風險，而就這些個人資料而言，機構亦是完全有責任遵守條例的規定。

大體來說，「自攜裝置」的做法會對保障資料原則有下述影響：

(a) 保留及刪除資料（第2原則）

機構須確定是否應該把個人資料保留在「自攜裝置」器材內。如要這樣做，機構須確定保留及刪除資料政策是否同樣適用於這些保留在「自攜裝置」器材內的個人資料，以及這些政策如何有效地應用，例如延伸有關政策以涵蓋「自攜裝置」器材內的資料。

(b) 控制個人資料的轉移及其後的使用（第3原則）

機構應就僱員如何查閱及使用機構收集的個人資料制定足夠的控制措施。資料使用的政策應同樣適用於機構的器材及個人的「自攜裝置」器材。如機構收集的個人資料可被轉移至及/或保留於「自攜裝置」器材，那麼相比於中央儲存的資料，機構對於僱員如何查閱或使用儲存於「自攜裝置」器材內的資料會有較少的控制。機構因而需要提醒僱員，並制定政策及控制措施（如適用），以確保僱員在未取得資料當事人的同意前不能把有關的個人資料用於新目的。

(c) 保障已轉移至並保留於「自攜裝置」器材的個人資料（第4原則）

機構對保障所收集的個人資料的保安政策，應同樣適用於轉移至並保留於「自攜裝置」器材的資料。

鑑於「自攜裝置」器材在設計或使用方式上可能並不安全[2]，在沒有額外保障措施下使用「自攜裝置」器材，未必能符合第4原則下的保安規定。

1 請參閱 www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html

2 很多智能電話在製造時未有考慮保安問題。即使有，亦可能因被用戶「越獄」而停止了保障功能。

若實行有關「自攜裝置」器材的保安措施時，沒有同時考慮僱員的個人資料私隱，或會引起公司及僱員之間的衝突。例如，機構為了保障「自攜裝置」器材內的個人資料，或希望能遙距查閱「自攜裝置」器材以追蹤其位置或確保器材中沒有安裝未經准許的應用程式(「**程式**」)。但這些安排讓機構可查閱到僱員在「自攜裝置」器材儲存的私人資訊，因而可能侵犯僱員的個人資料私隱。

因此，為抵禦因「自攜裝置」器材遺失或被入侵[3]所引致的風險，機構應採取保安措施以保障「自攜裝置」器材內的個人資料，而不是利用現行用於保障機構中普遍使用的流動器材的工具(例如流動裝置管理 Mobile Device Management)來保障或監察「自攜裝置」器材。因此在實際執行上，需要結合下述方法：

1. 避免在「自攜裝置」器材儲存機構收集的個人資料；

2. 控制查閱儲存於「自攜裝置」器材的個人資料(例如在使用屏幕鎖之外，再使用專屬的用戶名稱及密碼)；及

3. 把儲存於「自攜裝置」器材的個人資料加密，但要採用非由「自攜裝置」隨器材附屬的加密方法，而且須與個人資料的敏感程度匹配。

這些方法會在本單張「最佳行事方式」部分闡述。

(d) 查閱及改正保留於「自攜裝置」器材的資料的權利(第6原則)

不論個人資料是保留於機構的中央系統或於「自攜裝置」器材內，個人查閱及改正其個人資料的權利都是一樣。因此，機構需要確保在查閱及改正個人資料方面是否仍能履行其責任，尤其是在個人資料只保留於「自攜裝置」器材的情況下。故此，機構應考慮採取措施，把儲存於「自攜裝置」器材的機構資料備份至由機構控制的地方儲存。

最佳行事方式

機構應考慮下述做法，以確保使用「自攜裝置」的方式符合保障個人資料的規定。

(a) 制定「自攜裝置」政策

機構必須制定「自攜裝置」政策，詳列有關：

1. 機構及僱員在「自攜裝置」措施上分別擔當的角色、責任及職責；

2. 機構決定「自攜裝置」器材可查閱的資訊及程式的準則，以及決定哪類「自攜裝置」器材可獲允許使用的準則，例如器材的種類、作業系統及其他技術標準；

3. 用以保障屬於機構及僱員的個人資料的技術解決方案，例如不容許經「自攜裝置」器材查閱的個人資料被儲存到器材中；或者當有關資料被儲存到「自攜裝置」器材時，必須把資料與其他程式分隔(例如透過「沙盒」技術)或加密；及

4. 機構監察僱員遵從「自攜裝置」政策及措施的機制，及不遵從的後果。

(b) 進行風險評估

機構應進行風險評估，以確定「自攜裝置」器材可查閱或儲存的個人資料種類，及資料遺失或被未經准許而披露所造成的傷害及可能性。機構應根據風險評估的結果及其技術能力，檢討和決定各類「自攜裝置」器材可查閱的個人資料種類，及制定相應的存取控制和保安措施保障資料。

由於僱員的「自攜裝置」器材可能載有不少有關自己、家人及其他人士的個人資料，如沒有合理理由或在僱員不知情下查閱、監察或刪除僱員在「自攜裝置」器材內的個人資料，會導致僱傭關係不和。因此，風險評估須兼顧對機構的資料(包括機構收集的個人資料)與僱員的個人資料的私隱影響。

[3] 被入侵的器材包括被「越獄」的智能電話或植入惡意軟件的裝置。

如機構欠缺技術能力去妥善評估風險或確保在「自攜裝置」政策實行時個人資料獲得足夠保障，便應尋求外部協助。不過機構須謹記，承辦商或許有責任就「自攜裝置」提供保障個人資料的設計及程序，但若然承辦商導致或作出任何侵犯私隱的情況[4]，機構仍須為此負上責任。因此，機構須確保其承辦商符合它指明的保安規定。有關詳情，可參閱《外判個人資料的處理予資料處理者》[5]資料單張。

(c) 採用技術解決方案

機構可於「自攜裝置」器材利用控制軟件或程式，保護轉移至器材的個人資料及提高器材的保安。這些軟件或程式可遙距清除「自攜裝置」器材上的資料，或將「自攜裝置」器材鎖上，又或追蹤其實際位置、偵測是否被「越獄」或植入惡意程式，甚至追查曾瀏覽的網站。此外，機構亦可以採取措施，使器材在連續多次被輸入不正確密碼後封鎖登入，或自動刪除器材內的資料。由於這些保障措施涉及向機構交出「自攜裝置」器材的某些控制功能，僱員或會擔心在工作期間及下班後均被監察，以及暴露其個人資料。因此，在採取上述保障措施前，機構應非常清晰地向其僱員傳達，在「自攜裝置」相關的保障個人資料政策中他們的權利和責任[6]。另外，機構可考慮（如適合）讓其僱員控制這些措施。例如，僱員可擁有自己的帳戶，以找出、清除或尋找自己的「自攜裝置」器材。不過，在容許這做法之前，機構必須知道，僱員可能因而成為操控著刪除「自攜裝置」器材內的資料的人。機構因此應考慮採取適當的備份措施。

下述技術功能可保障機構及僱員的個人資料私隱。基於這些功能的技術性質，機構可能需要就是否及需如何落實這些功能向資訊科技人員徵詢意見：

1. 除了「自攜裝置」器材的預設屏幕鎖外，機構應額外加設獨立的密碼或存取控制，以保護儲存於器材內的機構收集的個人資料。專用密碼、雙重認證、休眠模式及其他提升的保安控制的措施，可防止僱員的家人或其他人士（他們可能共同使用或可接觸有關「自攜裝置」器材）查閱有關資料。此外，機構可能需要安裝軟件以加強僱員採用的密碼，或發出指引要求僱員只可採用複雜的密碼；

2. 機構收集的個人資料儲存於「自攜裝置」器材時，應以其他方式妥善地加密，而不是採用由器材本身附屬的加密方式，如此即使資料遺失或器材被入侵，取得資料的人也難以使用資料；

3. 機構收集的個人資料在傳出及傳入「自攜裝置」器材時，應妥善地驗證及加密，令其不能被未獲授權人士截取，例如當「自攜裝置」器材連接上不安全的Wi-Fi網絡，可能會把通訊內容轉移至假冒的伺服器；及

4. 如機構收集的個人資料敏感程度高並且已經備份，機構可在「自攜裝置」器材安裝自動刪除資料功能，作為預防措施。例如當「自攜裝置」器材因遺失而沒有在預定時間內連接機構的伺服器，或出現多次嘗試登入器材的情況，器材的自動刪除資料功能可防止資料外洩。

---

4 根據條例第65(2)條，任何作為另一人的代理人並獲該另一人授權的人所作出的任何作為或所從事的任何行為，須視為亦是由該另一人作出或從事的。

5 請參閱www.pcpd.org.hk/tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

6 關於電子監察僱員的詳情，機構應參閱《保障個人資料私隱指引：僱主監察僱員工作須知》www.pcpd.org.hk/tc_chi/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Chi.pdf

(d) 監察及檢討

由於資訊及通訊科技器材面對很多威脅，亦會有漏洞，因此容許「自攜裝置」的機構必須定期檢討和更新其政策及措施，監察其符規情況。機構應因應科技發展或業務改變而完善及修訂其保障政策，亦應定期評估儲存於「自攜裝置」器材內個人資料的性質及／或敏感程度的轉變，從而對政策作出相應修訂。

PCPD.org.hk

查詢熱線 ： **(852) 2827 2827**
傳真 ： **(852) 2877 7026**
地址 ： **香港灣仔皇后大道東248號陽光中心12樓**
電郵 ： **enquiry@pcpd.org.hk**

二零一六年八月初版