通過電子裝置進行實體追蹤及監察

PCPD
HK

PCPD.org.hk

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

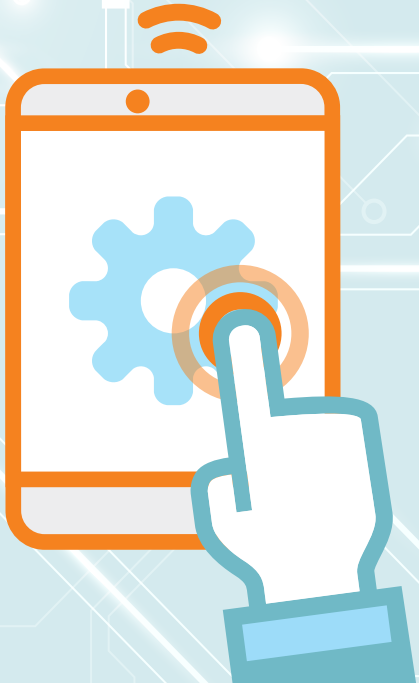
保障實體追蹤及監察所收集的個人資料
給電子裝置製造商的建議

智能手機製造商應：

- 讓用戶可選擇拒絕手機內的流動應用程式查閱及讀取其位置資料；
- 設定機制，防止用戶在不知情下被追蹤。

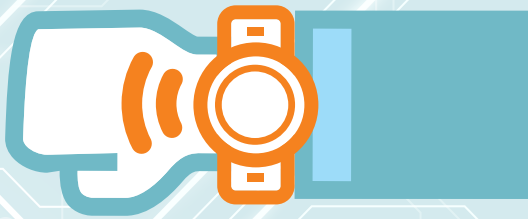
「物聯網」裝置製造商應：

- 提供簡單易明的私隱政策；
- 告知用戶所收集的個人資料類別、收集目的、資料承轉人和保安措施；
- 盡量減少收集資料，做好保安措施，並預設最低的侵犯私隱程度；
- 讓用戶可選擇拒絕提供與裝置功能無關的存取權限；
- 告知用戶如何刪除已儲存的個人資料；
- 向用戶提供查詢私隱事宜的聯絡資料。



穿戴式裝置製造商應：

- 確保裝置不能在未經用戶啟動或其不知情的情況下讀取、收集或記錄其資料；
- 確保資料不會被用於任何目的，除非用戶已獲清楚告知有關使用目的；
- 確保裝置的獨特識別資料不會在用戶不知情下被掃描器讀取；
- 在收集或記錄用戶以外人士的資料時作出警示。



裝有RFID標籤產品的製造商應：

- 清楚告知客戶其產品裝有RFID標籤；
- 向客戶提供停用或移除標籤的選擇；
- 避免在標籤儲存個人資料；
- 防止標籤上的資料被未獲授權人士讀取；
- 避免標籤載有任何可讀取的獨特識別碼；
- 在設定標籤的可被讀取距離時，充份考慮對個人資料及私隱的保障。

* 詳情請參閱《通過電子裝置進行實體追蹤及監察》資料單張內文

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

二零一七年五月初版

PCPD HK
PCPD.org.hk
資料單張
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

通過電子裝置進行實體追蹤及監察

摘要

通過電子裝置如Wi-Fi發射器或無線射頻識別（**RFID**[1]）標籤追蹤個人的實際位置及監察其行為已越來越普遍。通過掃描個人所攜帶的物品上的RFID標籤等方式，更有可能揭示該個人的私密資料，例如他的健康狀況，並侵犯其私隱。更重要的是，追蹤或監察所收集的資料可能揭露個人的身份，因而可能受到《個人資料（私隱）條例》（「**條例**」）的規管。本單張會闡述條例的主要規定。

任何個人或機構若打算利用電子裝置進行追蹤或監察，應先進行私隱影響評估，以減少 —

(a) 所收集的資料的範圍和敏感性；

(b) 對受影響的個人所帶來的詫異；

(c) 對受影響的個人所造成的私隱風險。

本單張會就進行私隱影響評估的最佳行事方式作出建議。

電子裝置製造商應採取一系列措施以減低裝置對個人資料私隱所帶來的負面影響。例如製造商應提高其私隱政策及其裝置的私隱設定的透明度。另外，製造商亦應採用「貫徹私隱的設計」（Privacy by Design[2]），例如減少收集資料，及採取足夠的保安措施以保障資料的安全。本單張的最後一節會討論保障資料的可行措施。

引言

通過電子裝置如Wi-Fi發射器或RFID標籤追蹤個人的實際位置及監察其行為已越來越普遍。追蹤及監察安排可以是為了物流管理、員工管理、人身安全、貨物保安、直接促銷活動，或者其他目的，例如在家居使用「智能」家電，包括智能溫度調節裝置[3]、智能雪櫃[4]及環境操控系統。這方面的創新科技發展一般稱為「物聯網」。「物聯網」增加了人、物件及環境之間的聯繫，提升效率、促進安全及令生活更寫意，但同時亦引發重要的個人資料私隱議題。

本單張旨在闡述這類追蹤及監察所帶來的個人資料私隱關注。然而，本單張不會探討為監察目的而使用閉路電視（或類似裝置）的私隱議題。有關議題另行在香港個人資料私隱專員（「**私隱專員**」）發出的《閉路電視監察及使用航拍機指引》[5]中探討。

1 RFID通常指裝備了無線電波傳輸功能的裝置，具有電子識別號（通常是獨特的編號），並能通過無線電波將該識別號傳送至其他裝置。此外，RFID或可儲存及處理資料。

2 「貫徹私隱的設計」（Privacy by Design）是在產品設計階段開始考慮私隱保障，並將保障私隱的措施融入設計中。

3 智能溫度調節裝置運用感應器及實時天氣預測以調節室溫，以達至減低耗電量、節省帳單費用及令室內溫度更舒適。

4 智能雪櫃內置相機及感應器，可提示用家哪些食品需要添加儲備，用家亦可利用智能雪櫃上網購物。

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

甚麼是電子裝置的實體追蹤或監察？

個人的行蹤、資料檔案或行為可以經由他所攜帶、穿戴或安裝在家中或工作地方的電子裝置（或具備Wi-Fi發射器或RFID標籤的貨品）直接或間接地追蹤或監察。

公司可透過提供的流動應用程式或智能手機監察員工的動向。類似地，購物中心可透過購物者攜帶的智能手機及附有RFID標籤的物件（例如信用卡、儲值卡或原本只用作供應鏈管理的內置RFID標籤的貨品）追蹤購物者的行蹤及為他們建立個人資料檔案。不論這類實體追蹤或監察安排的原本目的為何，其所帶來的不利私隱影響及風險是近似的。同樣地，在家電、環境操控系統及其他設備安裝資料傳輸裝置，雖可為用戶帶來極大好處，但同時亦涉及匯集大量有關用戶潛在的敏感個人資料。

實體追蹤或監察所收集的資料是否個人資料？

如實體追蹤或監察所收集的資料可用作識辨個人的身份，有關資料或會被視為條例下的個人資料[6]。因此，管控有關資料的收集、持有、處理及/或使用的人士及機構或會被視為條例下的資料使用者。

在追蹤個人動向或監察個人行為的過程中，追蹤者（個人或機構）未必能夠確定有關人士的身份，因此所收集的資料或會被視為匿名資料，例如用以評估購物中心內人流模式、只有時間標記而未能識別購物者身份的購物人流紀錄。不過，若把這匿名資料與其他資料（例如有時間標記的商舖銷售紀錄、在停車場閘口以信用卡付款的紀錄或在處所收集的Wi-Fi登入資料）結合，便可能識辨個人的身份。當某人的身份被確定，他的身份及其他透過追蹤或監察技術所取得有關他的資料會被視為條例下的個人資料。

追蹤者及監察者亦要留意，雖然很多追蹤或監察安排只是以識辨群體為目標，而非為識辨個別人士，但收集的資料可能讓追蹤者或監察者識辨群體中的個人的身份，尤其是當追蹤者或監察者把資料與其他已持有或可取得的資料結合。在此情況下，所收集得的資料可能屬個人資料。

換言之，如追蹤者或監察者已持有某些人士（例如客戶及僱員）的個人資料，並能將追蹤或監察所得的資料與這些個人資料結合，則追蹤或監察的資料整體上應被視為個人資料。

實體追蹤或監察有甚麼私隱風險？

實體追蹤或監察所帶來的私隱風險，包括透過追蹤或監察收集的匿名資料與其他個人資料結合從而識辨個人身份、建立個人資料檔案、標籤個人，追蹤者、監察者或第三者亦可能在追蹤或監察過程中有意或無意地對個人造成不利的影響。

若被追蹤及監察的個人不知道追蹤或監察安排的存在、有關安排的目的、有關安排對他們造成的預期或非預期的不利影響，以及他們是否可以拒絕有關安排，可能會引起個人資料私隱方面的憂慮。

追蹤或監察某人的動向和位置，以及他在每個地點逗留的時間，或可建立該人士的資料檔案，顯示其個人喜好、興趣、性別或消費力。這些檔案資料，不論準確與否，可能被追蹤者、監察者或第三者進一步使用，例如把該人士標籤以使他容易受到歧視，或基於該人士的資料檔案顯示他並非一名有價值的客戶而拒絕向他提供他有資格得到的服務或待遇。

---

[6] 條例下的「個人資料」定義為符合以下說明的任何資料 —
(a) 直接或間接與一名在世的個人有關的；
(b) 從該資料直接或間接地確定有關的個人的身份是切實可行的；及
(c) 該資料的存在形式令予以查閱及處理均是切實可行的。

很多附於貨品的RFID標籤會向RFID閱讀器發送產品電子代碼，披露某人所攜帶的貨品的詳細資料。這可令追蹤者、監察者或第三者掌握該人士更多資料，例如他的服裝品牌及尺碼、手錶品牌及款式、閱讀的書籍名稱、信用卡種類、身上攜帶的藥物種類，以進一步建立該人士的資料檔案。因此，追蹤個人攜帶的貨品亦可帶來私隱風險。

如追蹤者或第三者可在某人不知情下建立他的資料檔案或猜測到他不為人知的特徵，任何根據這些資料所作的決定可能會對該人士造成負面影響，例如根據不準確的資料對該人士作出不利的決定，甚至歧視。若該人士不知道這個不利的決定或其理據，可能無法作出補救。

遵從法規

資料使用者收集、處理及/或儲存透過追蹤或監察而取得個人資料，應熟悉和遵守條例的條文，以及六項保障資料原則。下文闡釋了有關規定及其應用：

保障資料第1原則 — 收集目的及方式

- 只可為直接與資料使用者的職能及活動有關的合法目的而收集個人資料；
- 就有關目的而言，所收集的個人資料應屬足夠及不超乎適度；及
- 應採取所有切實可行的步驟告知資料當事人收集及使用資料的目的[7]。

在此原則下，資料當事人應清楚獲告知收集及使用其位置及/或行為資料的目的。若追蹤或監察是自願性的，資料當事人應清楚獲告知他們可選擇拒絕有關安排。另一方面，如追蹤或監察是必須的，例如某些關於地盤安全的追蹤或監察計劃，資料當事人應獲告知他們若不接受被追蹤或監察的後果。如追蹤或監察是為進行直接促銷活動，資料當事人應清楚獲告知這項安排，而且在進行之前須取得當事人的同意[8]。

保障資料第2原則 — 準確性及保留期間

- 資料使用者必須採取所有切實可行的步驟來確保：
  - 個人資料在使用前是準確的；及
  - 資料使用者及其承辦商沒有把個人資料保存超過所需的時間。

舉例說，如資料使用者會根據在工作地方追蹤收集的出勤資料，對資料當事人採取不利的行動，資料當事人應獲給予機會就所收集的資料及擬對他採取的行動提出意見。

保障資料第3原則 — 使用收集所得的資料

- 除非資料當事人事前給予同意，否則個人資料只可用於原本收集資料的目的（或直接有關的目的）。

如追蹤或監察安排可能出現「用途改變」的情況，應進行私隱影響評估[9]（下一節「最佳行事方式的建議」會詳細闡述）。這項評估應衡量新的用途是否需要取得資料當事人的同意。

保障資料第4原則 — 資料保安

- 資料使用者須採取所有切實可行的步驟，以確保個人資料免受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，當中尤其須考慮若發生此等事件時可能對當事人造成的損害。

資料使用者在傳輸或儲存由追蹤或監察所得的個人資料時，應採取適當的保安措施，例如資料加密，並防止儲存的資料被未獲授權複製，及防止傳輸中的資料被「略讀」。資料使用者亦應制訂內部政策及程序，以防止其僱員或其他可查閱有關資料的人士未獲准許地使用有關資料。

---

7 請參閱私隱專員發出的《擬備收集個人資料聲明及私隱政策聲明指引》
www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_picspps_c.pdf

8 請參閱私隱專員發出的《直接促銷新指引》
www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_DM_c.pdf

9 資料使用者如希望了解私隱影響評估程序的詳情及一般應用，請參閱私隱專員發出的《私隱影響評估》資料單張
www.pcpd.org.hk//tc_chi/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf

保障資料第5原則 — 政策及透明度

- 資料使用者應就處理個人資料制訂和提供政策及實務[10]。

舉例說，如購物中心透過購物者攜帶的物品收集購物者的位置資料，便應在適當地方（包括出入口）展示顯眼的告示提醒購物者這項安排，包括列明收集資料的目的及可能會將資料轉移予哪些人士，並且提供簡單的方法及清晰地告知購物者如何拒絕有關安排。

保障資料第6原則 — 查閱及改正資料

- 資料使用者應在條例所訂的時限內依從查閱資料[11]或改正資料[12]要求。

如購物中心計劃收集購物者的個人資料，應在事前制訂機制，讓購物者可查閱此等資料及提出改正資料的要求。

最佳行事方式的建議 — 進行私隱影響評估

任何人如計劃追蹤或監察個人，或進行任何涉及追蹤或監察個人的項目，應盡早在設計階段考慮進行私隱影響評估，以確保項目對個人資料私隱的影響得到小心及恰當的評估。私隱影響評估旨在找出對個人資料私隱的影響，並將影響降至最低。

即使透過實體追蹤或監察所收集的資料並不是打算用於識辨個別人士，或所收集的資料不能用於識辨個別人士，但個別人士可能會持相反的看法，認為其私隱被侵犯。例如利用匿名個人資料檔案發出的定向廣告，即使不涉及個人資料，但看來亦具侵犯性。因此建議進行私隱影響評估時留意潛在用戶的看法。

(i) 減少資料涉及的範圍及敏感性

主要步驟－考慮在追蹤或監察安排中所收集的每項資料是否必須

確定及檢視計劃收集的每項資料，然後評估所收集的資料在整體上會否被視為個人資料，以及能否減少收集資料而同時達到追蹤或監察的目的。

例子：

1. 如購物中心希望與店舖分享購物者進出該些店舖的動向資料，應考慮摒除分享智能手機的獨特識別碼、購物者在該些店舖外的所在位置資料，以及精確的時間標記，因為這些資料就有關目的而言並非必須，並可能讓店舖在購物者不知情下識辨購物者的身份及建立其資料檔案。
2. 僱員所使用與工作追蹤有關的智能手機應用程式，應在僱員下班後自動關閉。
3. 為防工人接近危險地點或器材而追蹤工人的位置，或為確定工人是否已穿戴所需的安全配備的地盤安全系統，只需在工人接近危險地點或沒有穿戴所需的安全配備時發出警告已可達致目的，未必需要識辨或記錄每名工人在非危險範圍的行蹤。
4. 偵測老人院住院者是否跌倒或離開院舍的行動感應安全系統，未必需要記錄每名住院者的過往行蹤。

[10] 請參閱私隱專員發出的《擬備收集個人資料聲明及私隱政策聲明指引》
www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_picspps_c.pdf

[11] 請參閱私隱專員發出的《資料使用者如何妥善處理查閱資料要求及收取查閱資料要求費用》
www.pcpd.org.hk//tc_chi/resources_centre/publications/files/DAR_c.pdf

[12] 請參閱私隱專員發出的《資料使用者如何妥善處理改正資料要求》
www.pcpd.org.hk//tc_chi/resources_centre/publications/files/dcr_c.pdf

(ii) 減少（對個人）造成的「詫異」

主要步驟－評估對個人造成的實質及潛在的「詫異」，知會有關人士及向他們提供拒絕的機會

提高追蹤或監察安排的透明度，及容許個人決定是否參與安排，以減少對個人造成的詫異，尤其是當追蹤或監察的目的並不明顯。

例子：

1. 如購物中心是以購物者的智能手機的獨特無線識別碼（即智能手機獨特的Wi-Fi MAC位址[13]）追蹤購物者的流向，應在購物者進入購物中心時告知有關追蹤安排，並向他們提供拒絕被追蹤的機會。
2. 如購物中心是根據購物者安裝在智能手機的應用程式追蹤購物者的流向，則該程式不應被包裝或推廣為純粹提供更好購物體驗的程式，而不清楚披露這項侵犯私隱的功能。
3. 如追蹤資料會與第三者分享，資料當事人應獲清楚告知。如追蹤者與第三者分享追蹤資料的目的不是與追蹤者的職能直接有關，當事人應獲提供拒絕分享資料的選擇。
4. 如機構計劃掃描個人的RFID標籤，以追蹤個人、建立個人的資料檔案或進行篩選程序，便必須清楚告知有關人士，包括有關安排是必須還是可自願選擇參與。
5. 如個人在處所登記使用免費Wi-Fi服務，而他們的登記名稱或電郵地址會被用作追蹤用途，有關人士應在登記使用Wi-Fi服務前獲清楚告知這項安排，以便他們決定是否希望繼續登記及被追蹤。為保安理由，他們亦應獲提醒在使用服務後將其「忘記」（即將有關Wi-Fi連線從他們的裝置上移除）。

(iii) 減少私隱風險

主要步驟－識辨實質或潛在的私隱問題，並制訂控制措施及採取補救方法應付

常見的私隱問題包括實質或感覺上的私隱侵犯、個人身份被識辨或重新識辨、被建立個人資料檔案及受到非預期的不利影響（例如被歧視），以及資料被用作直接促銷活動。

例子：

1. 如實體追蹤所收集的資料可用來識辨個人，應設有足夠的保安措施來保障資料的傳輸、儲存、查閱、保留及分享。
2. 如資料使用者擬將收集的資料用於直接促銷用途，便須遵從條例第6A部的規定，在符合所有相關條件前不會進行直接促銷活動。
3. 如在適當分析追蹤資料後，資料追蹤者打算把資料用於與原本收集目的不符的用途，便必須按條例的條文及保障資料原則，尤其有關使用個人資料的保障資料第3原則，適當地評估把資料用於這新用途的影響及保障有關人士的個人資料。

須注意的是，資料使用者（例如購物中心的追蹤者或監察者）應妥善記錄私隱影響評估，以顯示資料使用者已主動採取行動保障個人資料，並為日後的審核及檢討提供基準。在處理投訴方面，追蹤者亦可利用私隱影響評估的文件以顯示他們已採取步驟保障個人資料私隱。

[13] MAC位址是屬於備有Wi-Fi功能的智能手機的獨特編號。這位址通常會被智能手機「發送」至附近的Wi-Fi熱點，不論該智能手機會否使用或連接該熱點。

給裝置製造商的建議

直接或間接實體追蹤或監察個人的其中一個方法，是透過追蹤個人攜帶的無線物品或監察其居所內的家電或其他設備及裝置。這些無線物品包括：智能手機、「物聯網」裝置（例如智能溫度調節裝置及智能雪櫃）、穿戴式裝置（例如健康手帶）或附有RFID標籤的物品（例如付款卡、衣服、手錶、書籍等）。這些裝置的製造商應考慮產品對個人資料私隱的影響，並在產品的設計中應用「貫徹私隱的設計」這概念，以保障客戶的個人資料私隱。下述例子闡述這些製造商如何在不損害個人資料私隱保障或令用戶擔憂的情況下，建設聯通的世界。

給智能手機製造商：

1. 智能手機用戶應獲提供及告知選擇權，以決定某流動應用程式應否查閱其智能手機內的位置資料，以及該應用程式可讀取的位置的精細程度。
2. 由於第三方可利用Wi-Fi組件追蹤智能手機的位置，智能手機製造商應設定機制，防止用戶在不知情下被追蹤。

給「物聯網」裝置製造商：

1. 「物聯網」裝置的用戶應獲提供以簡單語言撰寫的私隱政策，讓用戶容易明白及查找資料（例如私隱政策應簡短而清晰，並應分為不同部分及為每個部分加上標題）。
2. 「物聯網」裝置的用戶應清楚獲告知收集的個人資料類別、收集目的、個人資料的潛在承轉人及為保障資料而採取的保安措施。
3. 「物聯網」裝置的製造商應採取「貫徹私隱的設計」的做法，即減少收集的資料、在儲存及傳輸個人資料方面採取足夠保安措施，以及將裝置預設於對私隱侵犯程度最低的設定。
4. 如果「物聯網」裝置須與智能手機應用程式一起使用，而有關程式又會存取用戶智能手機內的資料，製造商應容許用戶切實可行地選擇拒絕向有關程式提供一些與該裝置的主要功能無關的存取權限（例如位置資料、通訊錄等）。
5. 「物聯網」裝置的用戶應獲提供清晰的指示，讓他們知道如何刪除儲存在裝置及在遠端媒體（例如製造商及其承辦商的後端伺服器）內的個人資料。
6. 「物聯網」裝置的用戶應獲提供聯絡資料（例如聯絡人、電話號碼、電郵地址及辦公地址）以供他們查詢私隱事宜，以及他們的私隱關注應得到及時回應。

給穿戴式裝置的製造商：

1. 穿戴式裝置的製造商應確保感應器所收集的資料只可通過獲認證的方式，並由用戶自行啟動後方能讀取。
2. 製造商應確保由裝置收集的，而製造商又可查閱的資料，不會在沒有全面告知用戶的情況下，用於任何目的。
3. 製造商應確保其裝置的獨特識別資料不會在用戶不知情下被掃描器讀取，以避免穿戴式裝置（以至用戶）被第三者追蹤。
4. 製造商應確保裝置不能在未經用戶啟動或其不知情的情況下收集或記錄其資料。
5. 如穿戴式裝置可以收集或記錄用戶以外人士的資料，應作出充份的警示。

給在產品加入RFID標籤的製造商：

1. 必須清楚告知客戶其產品裝有RFID標籤及有關用法。
2. 客戶應獲提供拒絕在產品加入RFID標籤、停止使用標籤或移除標籤的方法。
3. 製造商應避免在RFID標籤儲存產品擁有人的個人資料，但如標籤擬用來儲存個人資料[14]，有關的資料使用者（例如零售商）必須遵守條例的規定，包括採取所有切實可行的措施防止標籤內的個人資料被未獲授權的第三者讀取。
4. 載有貨品資料（例如一般的產品電子代碼）的RFID標籤，當中的資料可連同客戶的個人資料建立個人資料檔案，客戶應可選擇停止使用或移除該RFID標籤。如標籤必須保留作保用或查核貨品真偽的用途，則標籤上的資料應防止被未獲授權人士讀取。
5. 不論RFID標籤是否載有產品或個人資料，如客戶不能移除或停止使用標籤，則標籤不應載有任何可讀取的獨特識別碼（例如序號），令標籤（以至客戶）被永久追蹤。
6. 在選擇RFID標籤技術時，應小心及恰當地設定標籤可被讀取的距離，以保障個人私隱。

[14] 例如個人化的非接觸式付款卡

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

免責聲明

本刊物所載的資訊和建議只作一般參考用途，並非為《個人資料（私隱）條例》（下稱「條例」）的應用提供詳盡指引。有關法例的詳細及明確內容，請直接參閱條例的本文。個人資料私隱專員（下稱「私隱專員」）並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在條例下獲賦予的職能及權力。

二零一七年五月初版