PCPD.org.hk

指引資料

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

收集及使用生物辨識資料指引

導言

本指引旨在協助資料使用者[1]在收集生物辨識資料方面遵守《個人資料(私隱)條例》(條例)的規定。資料使用者應在決定是否收集生物辨識資料**之前**閱讀本指引；若已收集有關資料，則應定期參閱本指引。

生物辨識資料包括個人先天的生理資料[2]及後天形成的行為資料[3]。因此，生物辨識資料是直接與個人有關的。一般人只單憑觀看指紋影像或以其數字化描述(即模版[4])來確定某人的身份，未必是合理地切實可行；但當生物辨識資料與另一資料庫的個人資料連結後，便可識別個別人士(條例稱為「資料當事人」)的身份。有鑑於本指引的用途及上述原因，生物辨識資料亦會被視為條例下的個人資料[5]，因而凡收集及/或使用生物辨識資料的個體都屬於條例下的資料使用者。本指引旨在為收集及使用生物辨識資料提供良好行事方式建議。

謹慎處理敏感生物辨識資料的需要

生物辨識資料往往包含個人健康、精神狀況及/或種族[6]相關的私密資料，因而可屬敏感資料；而基於其獨特性，生物辨識資料通常在刑事調查中用作身份識別[7]。錯誤地披露任何生物辨識資料可導致嚴重後果，例如在無意/未經准許的情況下再次識辨出個別人士的身份[8]、身份遭冒認[9]，甚至在未經准許下披露個人切身的資料因而遭受歧視[10]。

收集生物辨識資料是否恰當及對所收集的資料應採取甚麼保障措施，會因應有關生物辨識資料的敏感程度而有所不同。

---

1 根據《個人資料(私隱)條例》，「資料使用者」指獨自或聯同其他人或與其他人共同控制個人資料的收集、持有、處理或使用的人。

2 例如，DNA樣本、指紋、手掌靜脈、手形、虹膜、視網膜及面部圖像。大多數生理資料是不能更改的。

3 例如，筆跡、打字節奏、步態及聲音模式。行為資料可由有關人士有意識或潛意識地改變。

4 數字化描述或模版為形容生物特徵樣本/圖像的主要特徵類型及位置的資料(例如指紋紋線的端點、轉向、匯合處等)。

5 根據條例，「個人資料」指符合以下說明的任何資料：(i)直接或間接與一名在世的個人有關的；(ii)從該資料直接或間接地確定有關的個人的身份是合理地切實可行的；及(iii)該資料的存在形式令予以查閱及處理均是合理地切實可行的。

6 DNA可揭示一個人的先天狀況、性別及種族，亦漸被認為可揭露精神健康狀況及個性傾向。視網膜圖像已被接納為可透露個人的健康狀況。有些人亦相信虹膜圖像可顯示個人的健康及性格。

7 指紋、DNA、面部圖像及筆跡早已被執法機構應用於刑事調查以作識別用途。

8 當生物辨識資料(連同或不連同其他資料)外洩時，或會發生身份再識別。例如，若戒毒中心的戒毒人士的面部圖像外洩，可能會直接識別出知名人士或引起人們識別這些人士的興趣。

9 例如，若指紋資料外洩，在資料足夠的情況下可製作假手指來冒充真人，以出入受指紋識別系統保護的區域。

10 如DNA排序或特徵外洩，可引致有關人士被假定為有可能有某些健康或精神問題(但該人士並未確診)，因而被拒絕獲得服務或工作的機會。

保存生物辨識資料的原來格式，相較於保存其模版或會構成較大的私隱風險，因為若與原來的生物特徵樣本/圖像[11]相比，模版通常載有較少詳細資料，因而未必能被使用在其他用途上。因此，資料使用者應盡快將原來的生物特徵樣本/圖像轉化成生物辨識模版，以作儲存及使用，並把原來的樣本/圖像安全地銷毀，及採用在技術上無法或難以重組原本圖像的方式儲存由生物特徵樣本/圖像轉化的模版。

資料使用者需要因應有關資料的敏感性，決定收集甚麼資料及以何種方式儲存。生物辨識資料閱讀器及掃描器的價格成本或是否易於在市面上採購並非首要考慮因素。

收集及使用生物辨識資料的良好行事方式

收集及使用生物辨識資料可以是為了不同的目的。例如，有生化危險的實驗室只容許已受培訓的專業人員進出，可能會使用與掃描器沒有任何身體接觸的視網膜或虹膜識別系統作出入監控。另一例子是使用手形識別系統以監控及記錄已取得所需技能/安全證書的建築地盤工人的出勤情況。在某些情況，面部識別或打字節奏分析器可在某人登入敏感的電腦系統後，持續核實使用者的身份。因此，是否可以收集某一類別的生物辨識資料，要視乎收集相關資料的目的及其收集方式。

(1) 必要性及相稱性

資料使用者須確保收集生物辨識資料的目的為合法的，並直接與其職能及活動相關的[12]，例如：執法機構為調查罪案而收集DNA資料、出入境部門為出入境監控而收集面部圖像，或僱主為了管制進出高度保安範圍及禁區而收集指紋資料。

就達到調查罪案、出入境監控，或管制進出禁區等目的而言，所收集的生物辨識資料必須是「足夠但不超乎適度」的[13]。因此，資料使用者須考慮可否收集敏感性較低的資料，但仍能同樣有效地達致相同目的。

在衡量使用生物辨識資料此措施以達致預期目的是否合符比例時，資料使用者可參考*希慎興業有限公司 訴 城市規劃委員會案*［2016］HKCFA 66（第134至135段）所設下的相稱性四步測試，其目的是衡量某侵犯基本權利的行為是否有足夠理據支持，當中要考慮：

- 該措施是否為追求**合法目的**；
- 該措施是否與推展該目的有**合理關連**；
- 該措施是否**不超乎為推展該目的所需**；及
- 是否已就侵犯行為所帶來的社會利益與受侵犯的個人的權利之間取得**合理平衡**，當中尤其要考慮追求社會利益會否對個人造成無法接受的、嚴苛的負擔。

(2) 資料最少化

資料最少化展現了「必要性及相稱性」原則。私隱憂慮的程度隨著收集生物辨識資料的數量（包括生物辨識資料樣本/圖像的特徵數量）而改變。資料使用者應收集最少的生物辨識資料以達致目的。例如，指紋資料及面部圖像是最常被收集的生物辨識資料，多用作身份識別和身份核實的用途，但用作識別與用作核實所需的樣本/圖像特徵數量可能會有所不同。

---

[11] 例如，指紋圖像外洩較其模版外洩會較大機會引致身份被識別、身份假冒及其他用途。面部圖像（而不是面部模版）外洩可更容易揭示資料當事人的性別及種族。

[12] 條例附表1的保障資料第1(1)(a)原則

[13] 保障資料第1(1)(b)及(c)原則

識別

身份識別過程涉及提供某人的生物樣本，讓識別系統從載有眾多人士數據的資料庫中進行搜尋及找出脗合的資料。由於資料庫中個別人士的數據有可能相似，往往便需要從樣本抽取更多參考數據，以便日後能肯定地找出脗合的資料。例如：有一間聘用1,000名僱員的公司使用面容識別出勤系統，當僱員返抵公司時，需要面對鏡頭，系統便會捕捉該僱員的面部特徵，然後與資料庫內1,000份數據資料作比對，直至確切識別出個別人士。為達此目的，鏡頭捕捉的特徵和儲存的特徵數據必須頗詳細，系統才不會錯誤識認某僱員。

核實

另一方面，與身份識別的過程比較，身份核實所需的樣本參考資料會較少。身份核實涉及呈示生物樣本，再要求系統核實是否屬於某指定人士。過程中，系統只需從資料庫中檢索所指定人士的生物特徵資料，確認是否與生物樣本相同或相似。類似的例子是：當僱員到達公司時，除了面對鏡頭外，可輸入職員編號，通知系統他的身份。在此情況下，系統只需捕捉較少的面部特徵，再檢索該僱員的資料，然後確定是否脗合。系統在比對時，無需理會資料庫中是否有近似的資料及有多近似，因此相比於在對該僱員一無所知的情況下作身份識別，進行身份核實所需的資料相對會較少。

許多時商業機構收集生物辨識資料只為確定某人的身份，因此應選擇上述形式操作的生物特徵身份核實系統，以減少收集生物特徵的數目。

(3) 私隱影響評估

鑑於生物辨識資料屬敏感的資料，有意收集生物辨識資料的資料使用者須首先考慮有關收集是否必需的[14]。為此，公署鼓勵有關資料使用者進行私隱影響評估。私隱影響評估是一個有系統的程序，用以評估建議的做法對個人資料私隱的影響。進行私隱影響評估有助避免或減低對有關人士的不利影響。

以下是協助資料使用者進行私隱影響評估的一些指引。

(i) 收集生物辨識資料的需要

資料使用者應考慮下述問題，以決定收集生物辨識資料是否必需：

- 為何需要收集生物辨識資料？
- 若現有一套非生物辨識資料系統用作應付需要，但又未能勝任，該不足之處是否可以解決？如可以，應選擇解決現有系統的問題，而不是改為收集生物辨識資料。

(ii) 侵犯程度最少的選擇

每當有不同選擇可達致相同目的，應採用侵犯程度最少的選擇。在這方面，收集生物辨識資料普遍侵犯程度較高。

- 如有其他系統可以達到與收集生物辨識資料的同樣目的，應考慮該系統，並就其對私隱的侵犯程度進行評估。
- 應收集敏感程度較低及/或較少數量的生物辨識資料來達致同樣目的，以減少對有關人士的私隱侵犯程度。

倘有人依據條例向資料使用者提出法律上質疑時，上述考慮亦有助他們解釋為何需要收集生物辨識資料。

[14] 保障資料第1(1)原則

收集生物辨識資料的目的及理據在不同情況下亦有所不同。雖然個人資料私隱專員(專員)會按每宗個案的情況作個別考慮，但有些收集目的是常見的，並值得在此討論，作為一般指引。

- 記錄出勤/出席情況：要記錄僱員出勤或學生出席的情況，通常可採取由僱員或學生親自簽到，或由他們使用門卡的方法。資料使用者若不採取侵犯程度較低的措施，或在採用這些措施後仍額外收集他們的生物辨識資料，須具備充分的理由。
- 保安控制：雖然收集生物辨識資料可能是為了保安理由(例如要確保只有獲授權人員才可進入某些限制出入範圍或查閱機密資料)，但這未必是較佳的方案。要管制出入範圍或查閱機密資料，可以向獲授權人員提供密碼及門卡。此外，安裝攝錄機以監察限制出入範圍或電腦終端機，再加上定期檢查，或可進一步加強保安。

資料使用者須緊記，僅為記錄出勤/出席情況及保安控制，其實可以採用其他私隱侵犯程度較低的方法，只要對不遵從規則的人士施以足夠的懲罰，仍能達致阻嚇的效果。

此外，應該避免持續及無區別地使用生物特徵掃描器，例如避免在任何人都會經常出入的地方(包括洗手間)安裝指紋掃描器，因為有關做法不大可能有充份理據。

(iii) 誰人的生物辨識資料應被收集及可被收集

如要收集大批人士的生物辨識資料，需要持有更強的理據，因為資料外洩所帶來的後果可以是很嚴重。

因此，如收集資料的目的是確保只有獲授權人士方可出入某範圍，那便應局限只收集該等獲授權人士的生物辨識資料。

學齡兒童或自理能力較低的人士需要在資料私隱上有更大的保障。如向這些人士收集生物辨識資料而被質疑的話，專員會嚴格地審查相關的收集行為。無論如何，學齡兒童不應被置於其私隱可能被削弱的行為或行事方式下，因為這樣可能會降低他們對相關資料私隱的風險意識，對他們日後成長帶來不利影響。

(iv) 收集資料的程度

資料使用者只需收集足夠的資料以達致其目的，而無需收集有關個別人士廣泛或詳盡的生物辨識資料。例如，在收集指紋資料時，通常無必要收集個別人士超過兩隻手指的指紋資料。

即使資料使用者只使用部份生物辨識資料以製作模版，也應視乎情況將參考資料數目降至最低。例如，資料使用者要從30人中區別個別人士所需的指紋參考資料數目，理應少於要從1,000人中區別個別人士的數目。

(4) 具透明度，可解釋性及知情的選擇

資料使用者在收集生物辨識資料時應給予資料當事人自主及知情的選擇，並詳細解釋收集其生物辨識資料對個人資料私隱的影響。在這方面，透明度及可解釋性非常重要。

(i) **透明度**

資料使用者在收集生物辨識資料時或收集前，應告知資料當事人下述事宜：

- 提供生物辨識資料是自願或是必須的[15]；
- 如必須提供其生物辨識資料，那麼若不提供將會有何後果[16]；
- 收集及使用生物辨識資料的目的[17]；
- 誰可查閱生物辨識資料，及在甚麼情況下其生物辨識資料可被查閱；
- 如生物辨識資料會被移轉予其他人，那麼會被移轉予甚麼類別的人士[18]；
- 所提供的生物辨識資料會否被用來對其個人作出不利行動；及
- 其查閱或改正生物辨識資料的權利，及應如何提出有關要求（處理相關要求的負責人姓名、職位及聯絡詳情）[19]。

(ii) **可解釋性**

為使資料當事人能作出知情的選擇及建立信任，資料使用者應就生物辨識資料的使用提供清晰的解釋。如清楚解釋：

- 為什麼需要收集生物辨識資料來達致所述目的；
- 這對個人權利和自由有甚麼影響； 及
- 採取了哪些補救措施，以減低不利影響。

(iii) **自主選擇，沒有不適當的壓力**

當資料使用者與資料當事人之間的議價能力懸殊，資料使用者在收集生物辨識資料時應格外小心。如資料使用者希望收集僱員的生物辨識資料，應確保已給予僱員自主及知情的選擇，讓他們自行決定應否提供該資料。即使收集僱員的生物辨識資料是「足夠但不超乎適度」，收集資料的方法亦必須在公平的情況下進行[20]；如僱員擔心不願或不能提供生物辨識資料會受罰，那麼向他們收集該資料便可能會被視為不公平收集；同樣地，暗中收集生物辨識資料需要非常充分的理由。

資料使用者應盡量避免予人有向資料當事人施加不當壓力之嫌。

若資料當事人已給予機會選擇是否容許收集或處理其生物辨識資料，並選擇同意的話，其選擇會受到尊重。因此，除非有關選擇並非自願地作出，或是處於不當的壓力下作出，否則專員是不會干預的。為免日後爭議，如果資料當事人選擇同意的話，資料使用者應以書面形式記錄該同意決定。

為避免予人有施加不當壓力之嫌，在切實可行的情況下，資料使用者應盡量讓每名資料當事人自由選擇以私隱侵犯程度較低的方案來代替收集其生物辨識資料（例如以智能卡加上閉路電視監察來代替指紋出勤系統）。資料使用者應採取所有切實可行的步驟來保障個別人士的資料私隱，以減低私隱對其的不利影響。專員在處理相關投訴時，如果資料使用者能提供已採取相關措施的憑證將會對資料使用者有利。資料使用者若以提供有關選擇會帶來一己不便作為原因而拒絕給予個人選擇，一般不會視為合理的理據。

---

15 保障資料第1(3)(a)(i)原則
16 保障資料第1(3)(a)(ii)原則
17 保障資料第1(3)(b)(i)(A)原則
18 保障資料第1(3)(b)(i)(B)原則
19 保障資料第1(3)(b)(ii)原則
20 保障資料第1(2)(b)原則

(5) 避免隱蔽式的資料收集

透明度及公平收集的另一種體現就是不應暗中收集生物辨識資料(除非有法律基礎授權，並在特定的情況下)。

生物辨識工具普遍要求資料當事人配合以提供資料(例如提供其指紋或DNA樣本)。然而，有些工具或許能夠以秘密方式收集資料(例如具面部辨識功能的攝錄機)。這些暗中收集生物辨識資料的行為具高度侵犯性，並可能對個人的尊嚴、私隱及其他權利產生負面影響。故此，除非有強而有力的理據，否則不應使用隱蔽式的攝錄機收集面部特徵資料。

(6) 有關自動化決策及人為干預的通知

不同的生物辨識技術在辨識個人身份的精密度及準確度各異。部份生物辨識技術(如面部識別技術)是或然性的－它只是提示使用者目標人物「可能」與資料庫中的某一個人資料匹配。而其他已長期沿用的工具(如指紋和DNA分析)的發展較為完善，亦被視為較可靠。此外，生物辨識工具的準確性亦取決於其用途和設定(例如：是要快速識別大量目標，或是逐一核實個人身份)。進行有關設定時可能要在假陽性和假陰性之間作出取捨[21]。

由於某些生物辨識系統無法完全可靠地識別個人身份，因此如事前沒有進行私隱影響評估，不建議採用相關生物辨識系統作自動化決策。

如自動化決策工具無可避免地需與生物辨識系統結合使用，作為良好行事方式，資料使用者應事先明確告知受影響人士此決策模式的存在及可能產生的影響。此外，當自動化決策可能會對個人產生重大或法律影響，應該為有關個人提供尋求人為干預的選擇。

(7) 保留生物辨識資料

對於一些已不再需要用於原來收集目的的生物辨識資料，資料使用者應定期並頻繁地將這些資料銷毀[22]。因此，如僱主收集僱員的生物辨識資料用以監控僱員出入其處所或登入電腦系統，僱主應於僱員離職後立即銷毀其生物辨識資料。

保留個人資料超過實際所需時間，不單違反條例規定，亦加重資料使用者保障資料安全的負擔，帶來不必要的資料外洩風險。

資料使用者如為了研究或統計目的而希望把個人資料保留超過實際所需時間，可把資料匿名化，令資料不能再識別個別人士，因而不受條例規管。然而，資料使用者應認真考慮匿名化的生物辨識資料對私隱可能造成的影響，及是否可以確實地把生物辨識資料匿名化。例如：DNA的樣本或排序，即使不與任何姓名連繫，亦可揭示種族、身體或精神疾患、彼此的家族關係等資料，這或可令個人的身份在某些情況下被再識別出來。

(8) 資料準確性

資料使用者須採取所有合理地切實可行的步驟，確保所收集的個人資料是準確的[23]。

由於所收集的生物辨識資料可能會對有關人士有所不利，有關資料的準確性便尤其重要。如僱員於每個工作天提供其生物辨識資料作為出勤記錄，任何不準確的資料可導致扣薪或被解僱。

---

21 當系統錯誤地將兩個不同的人辨識為同一個人，即出現假陽性。 當系統設置為低精確度時，發生這種情況的機會會增加(例如：在公共場所高速監控人群)。當系統將同一個人的生物辨識資料視為屬於不同的人，即出現假陰性。當系統被設置為需要高精確度的脗合時，發生這種情況的機會會增加。

22 保障資料第2(2)原則及第26條

23 保障資料第2(1)原則

要確保生物辨識系統的準確性，資料使用者須核實及滿意其生物辨識系統的假陽性及假陰性處於合理的範圍（視乎該系統所監控的人數）。此外，資料使用者在決定是否對個別人士採取不利行動前，應給予該人士合理的機會以解釋其違規行為。

此部份與使用自動化決策時作出通知的建議有密切的關係。

(9) 使用限制和避免改變用途

資料使用者未取得資料當事人的明確及自願的同意前，不得把所收集的個人資料用於新目的[24]，除非條例第8部的豁免條款適用。

某些生物辨識資料（例如DNA及視網膜影像）可以包含個人身體健康或精神狀況相關的豐富資料。資料使用者為某目的而收集此等資料，必須確保不會在未取得資料當事人的明確及自願的同意前把此等資料用於另一不相關的目的。例如：僱主在原本提供予僱員作醫療福利的年度身體檢查中所收集的DNA樣本或進行的DNA測試，不應在未取得資料當事人的同意前，用於決定該僱員是否適合長期聘用，這樣做會損害信任。

(10) 資料的保安

資料使用者須採取所有合理地切實可行的步驟，以確保由其持有的個人資料受到保障，不受未獲准許或意外地被查閱、處理、刪除、喪失或其他使用所引致的影響，尤其須考慮該等資料的種類及在資料外洩事故發生時可能造成的損害[25]。鑑於生物辨識資料為敏感的資料，資料使用者應在合理地切實可行的情況下實施有效的保安措施，防止生物辨識資料受破壞及盜用。有效保安措施的例子如下：

- 小心及定期評核儲存及處理生物辨識資料的資訊及通訊系統，以確保已採取足夠有效的保安及私隱保障措施；
- 生物辨識資料無論是儲存或傳送途中都應保持在加密狀態；及
- 只讓獲授權人士在「有需要知道」的情況下查閱該資料；同時，資料必須以強式密碼（例如由字母、數字及/或符號組成）保護，並記錄所有查閱/登入情況。

(11) 書面政策

資料使用者應制訂私隱政策及程序，清楚列出收集、持有、處理及使用生物辨識資料時須遵守的規則及實務措施，並讓所有相關各方知悉，例如僱員、承辦商及/或顧客。資料使用者應特別提醒受此等政策及程序影響的人士，並讓公眾檢視相關政策及程序[26]。

(12) 員工培訓

資料使用者應定期進行私隱循規評估及檢討，確保有關行動及做法符合條例的規定。負責收集及管理生物辨識資料的僱員必須得到適當的培訓、指導及督導。如僱員於執行職務時，沒有適當處理生物辨識資料，便可能受到適當的紀律處分。

尤其是，資料使用者應注意到某些生物辨識技術仍處於發展階段。其培訓應提高僱員對生物辨識系統的認識，了解此類系統可能存在不準確和錯誤識別的問題。系統操作員必須謹慎操作，並只應視該系統為輔助工具。

---

24 保障資料第3(1)原則

25 保障資料第4(1)原則

26 保障資料第5原則

(13) 聘用承辦商（資料處理者）

如聘用承辦商處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該承辦商的個人資料的保存時間超過處理所需的時間，及防止資料在未獲准許或意外地被查閱、處理、刪除、喪失或使用[27]。

資料使用者亦應留意，他們可能要對承辦商的誤用或保安缺失而引致的個人資料外洩事故負上責任[28]。

因此，有聘用承辦商的資料使用者除了在資料保安措施作相關和可行的考慮外，亦應遵從專員在《外判個人資料的處理予資料處理者》資料單張[29]內提出的建議。

(14) 審核和檢討

良好的做法是為生物辨識系統進行定期、獨立的審核和評估。評估系統是否需要進行修訂、改進或終止使用，無論是由於系統無法有效達致其預期目的，或是其最初的目的重要性已減低。在進行此類審核時，「必要性和相稱性」為首要考慮。

---

27 保障資料第2(3)及第4(2)原則

28 條例第65(2)條

29 請參閱http://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

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

私隱公署網頁

下載本刊物

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13樓1303室**
電郵 ： **communications@pcpd.org.hk**

二零一五年七月初版
二零二零年八月(第一修訂版)