根據《個人資料（私隱）條例》（第 **486** 章）第 **48**（**2**）條

發表

調查報告：

坤麗（亞洲）有限公司收集指紋資料

報告編號：R15 – 2308

發表日期：2015 年 7 月 21 日

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

調查報告：坤麗（亞洲）有限公司收集指紋資料

個人資料私隱專員（下稱「**專員**」）根據《個人資料（私隱）條例》（第 486 章）（下稱「**條例**」）第 38 條進行調查，並根據條例第 VII 部行使賦權發表本報告。條例第 48(2)條列明，「*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

(a) *發表列明以下事項的報告－*

(i) *該項調查的結果；*

(ii) *由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及*

(iii) *由該項調查引致的、專員認為適合作出的任何其他評論；及*

(b) *以他認為合適的方式發表該報告。*」

蔣任宏

個人資料私隱專員

調查報告：坤麗（亞洲）有限公司收集指紋資料

一名曾經受僱於從事高級時裝貿易的坤麗（亞洲）有限公司（下稱「坤麗」）的人士，向個人資料（私隱）專員公署（下稱「公署」）投訴坤麗以安裝在辦公室入口的指紋識別裝置，收集她的指紋資料。專員在調查後認為坤麗收集指紋資料屬超乎適度，其收集指紋資料的方式亦屬不公平，裁定坤麗違反了香港法例第486章《個人資料（私隱）條例》（下稱「條例」）附表1的保障資料第1(1)及1(2)原則。專員並向坤麗送達執行通知，指令坤麗糾正違反事項和防止違反事項再次發生。

I. 投訴內容

投訴人於 2014 年 6 月初獲聘任為坤麗的時裝買手，而她於同年 6 月 23 日離職。 坤麗在投訴人履新的第一天透過安裝在坤麗辦公室入口的指紋識別裝置，收集她的指紋資料。

2. 根據投訴人所述，坤麗為了考勤及保安目的，安裝了兩部指紋識別裝置，一部安裝在辦公室入口，另一部在陳列室入口。坤麗的職員須先將手指放在指紋識別裝置上，才可進入辦公室及陳列室。

3. 投訴人認為指紋為敏感的個人資料，因此她不願意讓坤麗收集她的指紋資料。她曾要求坤麗採用其他方法代替收集她的指紋資料，但不得要領。投訴人在別無選擇的情況下，唯有讓坤麗收集她的指紋資料。翌日，投訴人向坤麗提交一份同意書範本，建議坤麗在收集員工的指紋資料之前，應先取得有關員工的書面同意。然而，坤麗沒有採納她的建議。

4. 投訴人認為坤麗沒有合理理據收集她的指紋資料，遂向公署作出投訴。公署根據條例第 38 條進行調查，以確定坤麗收集投訴人及其他員工的指紋資料是否違反條例的相關規定。

II. 條例的相關規定

5. 與本案相關的是條例附表 1 的保障資料第 1(1)及 1(2)原則，當中訂明：—

「*(1) 除非—*

(a) 個人資料是為了直接與將會使用該資料的資料使用者的職能或活動有關的合法目的而收集；

(b) 在符合(c)段的規定下，資料的收集對該目的是必需的或直接與該目的有關的；及

(c) 就該目的而言，資料屬足夠但不超乎適度，

否則不得收集資料。

(2) 個人資料須以—

(a) 合法；及

(b) 在有關個案的所有情況下屬公平，

的方法收集。」

6. 根據條例第 2(1)條，「個人資料」是指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分是切實可行的；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。」

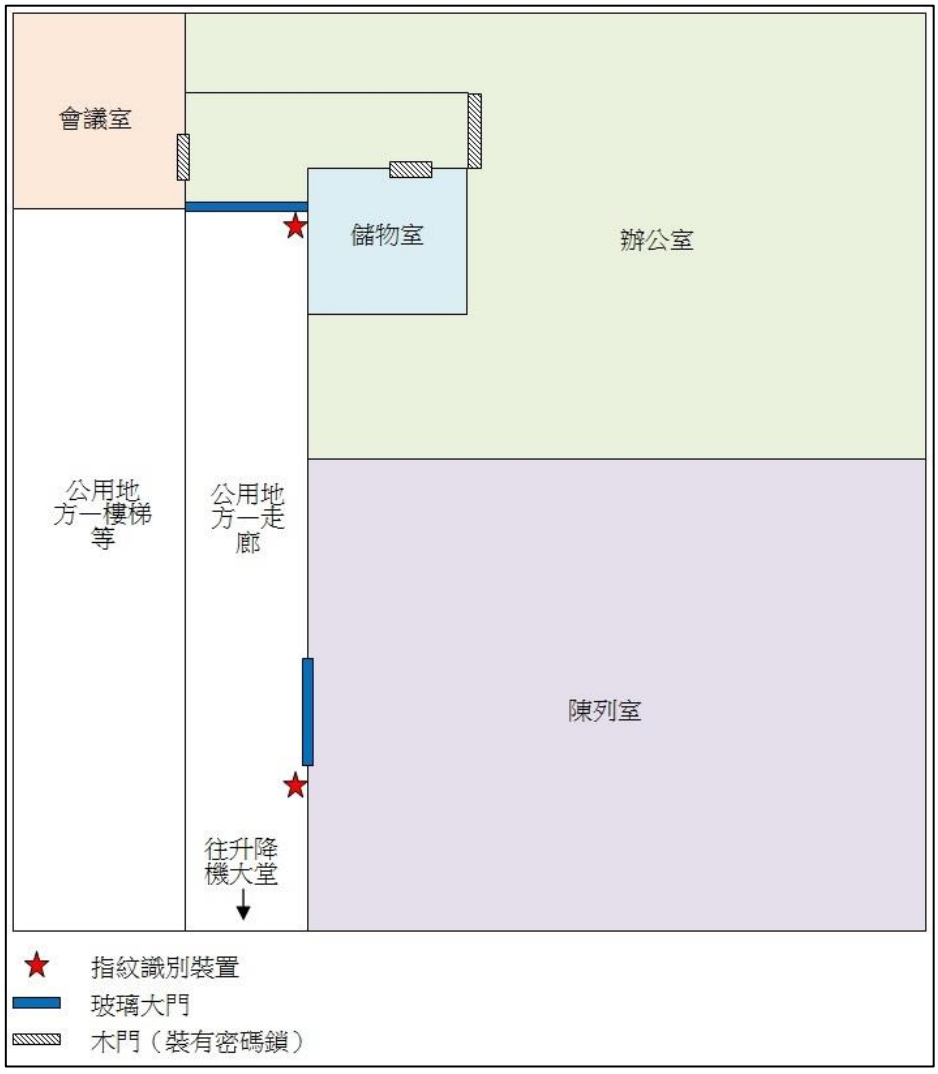
III. 調查所獲得的資料

7. 以下是公署在調查的過程中搜集的資料。

(a) 實地視察

8. 公署職員在坤麗的辦公室及陳列室進行了實地視察。該辦公室及陳列室位於一幢商業大廈的毗鄰單位，但各設有獨立的入口。坤麗的平面圖現呈如下（並非按真實比例繪畫）。

圖 1：坤麗的平面圖



9. 公署職員於某工作天上午約 10 時 30 分到達坤麗的辦公室視察，當時發現坤麗的辦公室及陳列室的大門半掩（見圖 2）。坤麗的職員可以無須使用指紋識別裝置自由進出辦公室及陳列室。一名郵差和速遞員亦可

以暢通無阻地進入坤麗的辦公室的範圍。在公署職員視察的約一個小時期間，辦公室及陳列室的大門一直只是半掩。

圖 2：坤麗的辦公室（上）和陳列室（下）的入口

(i) 陳列室

10. 視察期間，坤麗向公署職員表示安裝於陳列室的指紋識別裝置[1]只用於保安用途上。此說法與投訴人所述不符。據投訴人所指，此指紋識別裝置亦用於員工考勤的用途上。

11. 陳列室的面積大約為 1,500 平方尺。按公署職員視察時所見，陳列室內存放了大量不同類別的高級時裝物品，包括有衣服、飾物、鞋類等。坤麗聲稱存放於陳列室的貨品每件價值數千至數萬元不等。只有坤麗的銷售人員，以及在他們陪同下的顧客，才可進入陳列室。

12. 陳列室天花的四個角落均安裝有閉路電視監控鏡頭。坤麗表示在辦公時間過後，陳列室的大門會以門鎖及鏈鎖鎖上。

13. 在視察時，坤麗聲稱其陳列室及辦公室曾經發生數次失竊事件，其後憑藉閉路電視的錄影影像，找出犯案者全是坤麗的員工及參觀陳列室的顧客，並成功追回被盜的貨品，當中有每件價值三至四千元的飾物，以及每件價值介乎一百至一千元的公司紀念品（例如水瓶、手錶等）。坤麗表示沒有就事件向警方報案。

(ii) 辦公室

14. 公署職員看到坤麗的辦公室入口處裝有一部指紋識別裝置[2]，而辦公室裏則裝有一部對着入口的玻璃大門位置的閉路電視監控鏡頭，監察辦公室入口的情況。進入辦公室後，是一條通往儲物室、會議室和辦公室的通道。這三個房間的門均裝上了密碼鎖。公署職員視察期間，坤麗的會議室和辦公室的門都一直敞開。

15. 視察期間，坤麗表示安裝於辦公室外的指紋識別裝置是用於保安及員工考勤的用途上。坤麗並指出，其貨品主要存放於陳列室，但部分顧客退回的貨品會存放於辦公室範圍內，以待退回生產商。公署職員檢視了坤麗用作存放準備退回貨品的衣架，估計該衣架可掛上 20 至 30 件衣物。

[1] 安裝於陳列室的型號是「Fingertec R2」。

[2] 安裝於辦公室的型號是「Star Finger 007」。

(b) 坤麗的書面及口頭回覆

16. 坤麗自十多年前遷至現址時便開始採用指紋識別裝置。坤麗解釋：—

- 辦公室入口的指紋識別裝置是用於保安及員工考勤的用途上；及
- 陳列室入口的指紋識別裝置只是用於保安的用途上。

17. 坤麗表示陳列室外的指紋識別裝置沒有連接到任何電腦，而安裝在辦公室入口的指紋識別裝置則連接至一部設置於辦公室內，由坤麗的會計師使用的電腦，即主機電腦。該主機電腦設有密碼保護。會計師每月會從主機電腦編制出勤報告，當中包含員工的姓名及上下班的日期和時間。

18. 公署向坤麗查詢該兩部指紋識別裝置如何運作，例如：—

(i) 該兩部指紋識別裝置收集完整還是部分的指紋圖像；
(ii) 所收集得的指紋圖像是否會被轉化成數碼格式（亦稱為「模板」），並以此格式儲存及作日後核對之用；
(iii) 該兩部指紋識別裝置在儲存及傳送指紋資料時會否將資料加密；及
(iv) 指紋資料有否被轉移到其他裝置，例如伺服器或其他電腦。

19. 坤麗表示無法解答上述的問題。此外，坤麗亦無法確定至今一共收集了及仍保存多少名員工（現職及已離職）的指紋資料於其考勤系統中。坤麗已遺失了該兩部指紋識別裝置的使用說明書及為其安裝有關裝置的供應商的聯絡資料。坤麗表示若任何一部裝置失靈，便會將其更換。

(c) 從互聯網下載的使用說明書

20. 公署從互聯網[3]下載了坤麗所使用的兩部指紋識別裝置[4]的使用說明書。根據該兩份說明書，該兩部指紋識別裝置所收集的員工出勤紀錄可通過主機電腦編制成出勤報告。然而，該兩份說明書並沒有提及該兩部指紋識別裝置究竟收集整個還是部分的指紋圖像；到底指紋資料是以圖像還是數碼格式被儲存於指紋識別裝置中；以及指紋資料在傳送及保存期間有否加密。兩部指紋識別裝置均提供多種操作模式，包括使用內置識別碼的智能卡、密碼、指紋，以及任何以上兩種模式的組合。

21. 設於陳列室外的指紋識別裝置[5]具備多一種操作模式，即使用載有指紋模板的智能卡進行操作。

(d) 以指紋、智能卡及密碼操作坤麗的指紋識別裝置

22. 雖然坤麗不能說明該兩部指紋識別裝置如何通過指紋、智能卡及密碼操作，但公署有理由相信它們的運作模式如下：—

(i) 指紋

23. 在使用指紋去操作有關指紋識別裝置前，使用者須先行登記其指紋，方法是讓指紋識別裝置掃描他的其中一隻手指的指紋，然後裝置會將該指紋的某些特徵（例如紋理的末梢、分岔及匯合的位置）轉化成指紋模板。指紋模板最後會被儲存於裝置的模板資料庫中。此後，使用者只要將其已登記的手指放於指紋識別裝置上，裝置會再次將該手指上的指紋特徵轉化成指紋模板，然後將這個指紋模板與資料庫中的指紋模板作比對。如果這個指紋模板與資料庫中的任何一個指紋模板吻合，裝置會記錄進行比對的時間。如果裝置如本案中的一樣，接駁上電子門鎖，有關的門鎖會被打開。請參閱圖 3 的圖示解說。

---

[3] 網址：—

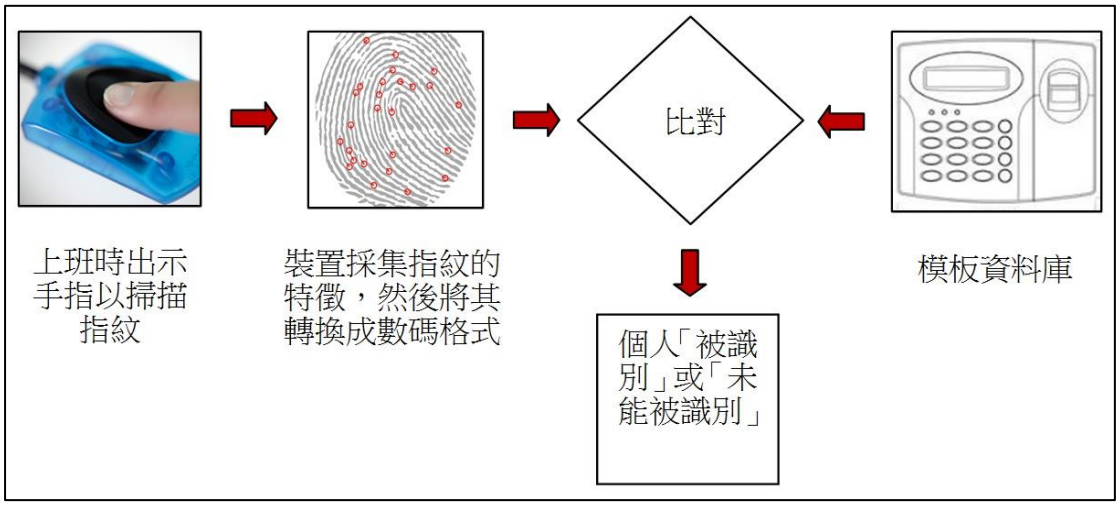
http://www.idteck.com/en/customer/customer/download/view/1135?p=1&d1=01&d2=01&m=06&t=3

http://www.fingertec.com/customer/download/postsales/HUM-AC900R2-E.pdf

[4] 型號為「Star Finger 007」及「Fingertec R2」

[5] 型號為「Fingertec R2」

圖 3：以指紋操作坤麗的指紋識別裝置



(ii) 密碼

24. 如選擇使用密碼以代替指紋，使用者須先行在指紋識別裝置中登記一組五位數字的自訂密碼，裝置會將密碼儲存於其資料庫中。此後，任何人士只要在指紋識別裝置上輸入密碼，而該密碼又與資料庫內的其中一個密碼吻合，門鎖便會被打開。此方法不涉及收集個人資料。

(iii) 內置識別碼的智能卡

25. 每張智能卡都載有一個獨特的、並已在指紋識別裝置上登記的識別碼。當有人將智能卡拍向指紋識別裝置，該裝置便會讀取智能卡上的識別碼，並將此識別碼與裝置的資料庫中的識別碼作比對。此方法同樣不涉及收集個人資料。

(iv) 內置指紋模板的智能卡

26. 使用此方法前須先將使用者的指紋特徵轉化成指紋模板，然後將指紋模板儲存於智能卡中，而此智能卡則由使用者自行保存。使用時，使用者須先將載有指紋模板的智能卡拍向指紋識別裝置，然後將相應的手指放於裝置的掃描器上，裝置隨即會將智能卡上的指紋模板與使用者的指紋作比對。指紋識別裝置不會保存使用者的指紋資料。

(e) 坤麗不向員工提供其他替代方法的理由

27. 坤麗表示若員工經常遲到，他可能會受到紀律處分（如書面警告）。坤麗依靠辦公室門外的指紋識別裝置去監察員工的出勤情況。坤麗為免員工相互替代「簽到」，所以不採用內置識別碼的智能卡或密碼的方法去操作該兩部指紋識別裝置。然而，坤麗未能向公署確定在使用指紋識別裝置前，是否曾有發生過員工互相替他人「簽到」的情況。坤麗強調，沒有員工反對坤麗收集他的指紋資料。

(f) 坤麗就指紋資料的收集、保存、使用及保安方面的政策

28. 坤麗承認沒有就指紋資料的收集、保存、使用及保安方面制定書面政策。每位坤麗的員工履新時均會被口頭告知以下事項：—

(i) 員工的指紋資料是用於保安及考勤的用途上；
(ii) 員工每天上班和下班時均須將登記了的手指放在辦公室入口的指紋識別裝置上以記錄上下班時間；及
(iii) 員工的指紋資料會於其離職後翌日從指紋識別裝置中被移除。

29. 坤麗同時承認沒有就儲存於主機電腦的員工出勤紀錄的保安及保存期限制定政策。

IV. 專員的調查結果

(a) 指紋識別裝置所收集的指紋資料屬於「個人資料」（條例第2(1)條）

30. 完整的指紋圖像是個人獨特的生理特徵，可用於識別有關個人，故屬於個人資料。不過，有人卻認為如果被收集的指紋資料被轉化成數碼格式，並以此格式儲存，則有關資料便只為一組無意義的數字，而不構成個人資料。專員並不認同此說法，因為當這組數字與其他可識別身份的資料串連（例如姓名），便可以識別有關個人的身份。畢竟，利用指紋識別裝置收集這些指紋資料的目的，正是要識別一個人，或核實他的身份。

31. 有意見認為，如果只收集指紋的部分特徵，這些指紋特徵便不屬個人資料，因為憑這些特徵重塑一個完整的指紋圖像是不可能的。因此，只收集及使用這些指紋特徵並不違反任何保障資料原則。就這點，專員參考了加拿大安大略省的資訊及私隱專員於 2008 年 11 月發表，名為《使用指紋資料前要解決的私隱問題》的文章。該文章指憑指紋特徵去重塑出仿真度極高的指紋圖像的情況並不罕見[6]。該文章進而闡述懷有惡意企圖的人若要利用指紋模板資料去仿製一個指紋，並利用此仿製指紋去瞞騙其他指紋識別裝置，並非難事[7]。

32. 簡而言之，不論坤麗收集的是員工的完整指紋圖像，或是由部分指紋特徵轉化成的指紋模板，此行為均構成收集條例第 2(1)條釋義下的「個人資料」。

(b) 指紋資料是敏感個人資料

33. 指紋是每個人與生俱來的獨有生理特徵，也是每個人獨特的身份標識符，而且終生不變，故指紋時常被用於刑事調查的用途上。與密碼及身份識別號碼不同，個人不能因其指紋資料被盜取或遺失，而將其指紋

---

[6] 「*直至最近為止，不能重組的觀點一直是生物識別技術界中的主流觀點。不過，過去數年發表的數項科學研究顯示，指紋其實是可以從枝節位模板重組的。最先進的研究是 Cappelli et al 於 2007 年發表的。作者分析兼容 ISO/IEC19794-2 標準的枝節位模板。在一個測試中，他們只用了基本的枝節位資料(即 X 位、Y 位及方向)。在另一個測試中，他們亦用了隨意的資料：枝節位類型、核心及變化數據，以及專有數據(在這個案是脊線方向範圍)。在所有的測試中，作者都能夠從枝節位模板重組指紋圖像。很多時，重組的圖像與原本圖像非常相似。儘管這重組只是約莫的，但在枝節位配對的個案中，超過九成的重組圖像足以錄得正向配對。*」

（以上為公署的中文譯本。英文原文可從以下網址下載：

https://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf）

[7] 「*這研究對指紋枝節位系統的保安及私隱的潛在影響如下：從枝節位模板重組的指紋圖像稱為「偽裝」圖像，因為它並非原本圖像的精確複本；在呈示後，很可能會瞞騙系統。偽裝圖像可以以數據的形式從指紋感應器後方輸入系統。懷有惡意企圖的人亦可以仿製指紋，放到感應器上。仿製指紋的技術便宜，而從文獻上是廣為人知的。能夠製造偽裝圖像會提升枝節位模板的相互運作程度。人們可以把偽裝圖像輸入其他需要輸入圖像(不是枝節位模板)的指紋系統，而無須進行枝節位模板的形式轉化。*」

（以上為公署的中文譯本。英文原文可從以下網址下載：

https://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf）

更改，故任何不當地收集或使用指紋資料均可導致嚴重後果，例如身份被盜用。由於指紋資料屬高度敏感的個人資料，所以在收集、使用及保存這些資料時都要加倍小心。因此，資料使用者在沒有其他對私隱侵犯程度較低的方法去代替收集指紋資料以達致有關目的時，才可有理據考慮去收集、使用及保存指紋資料。

(c) 坤麗收集指紋資料屬超乎適度（保障資料第1(1)原則）

34. 在決定坤麗收集指紋資料是否屬超乎適度時，須考慮以下問題：

(i) 就保障辦公室安全及員工考勤的目的而言，收集指紋資料是否必需？
(ii) 收集指紋資料是否達致上述目的之有效方法？
(iii) 收集指紋資料所帶來的好處與其對個人資料私隱帶來的風險是否合乎比例？
(iv) 是否有其他較不侵犯私隱的方法可達致上述 (i) 的目的？如有，資料使用者便應考慮採用其他方法以消除或減少對個人資料私隱的負面影響。

35. 就此，專員有以下觀察：

保安目的

(i) 坤麗的辦公室及陳列室曾於日間發生數宗失竊事件。然而，犯案者均是獲准進入坤麗的辦公室及陳列室的員工及顧客。既然如此，縱然坤麗安裝指紋識別裝置以防止外人擅自進入，但亦不能防止此類失竊事件。而這些失竊事件亦是在坤麗安裝指紋識別裝置之後才發生的。如上文所述，坤麗是透過閉路電視錄影的影像去追查這些失竊事件，並從中成功認出犯案者。安裝閉路電視鏡頭看來是更有效的保安方法。

(ii) 其實在辦公時間內把辦公室及陳列室的大門緊閉，已有助維持保安。遵守此基本的保安原則比採用以指紋操作的門鎖更為重要。

(iii) 坤麗在陳列室外安裝指紋識別裝置或許能防止在辦公時間外發生的盜竊，但一般的門鎖及鏈鎖亦能達致相同的效果，並且不涉及收集和保存個人資料。事實上，坤麗已採取了多項的夜間保安措施，此包括安裝閉路電視鏡頭、密碼鎖、門鎖及鏈鎖，安裝指紋識別裝置實屬多此一舉。

考勤目的

(iv) 保存準確的員工出勤紀錄是每個機構的基本行政工作。在考慮到上文第 33 段所述，有關收集指紋資料對私隱的侵害，以及指紋資料一旦外洩或被誤用所帶來的負面影響後，僱主並無充分的理據為達致此簡單的行政目的，而收集指紋資料。

(v) 由於坤麗只有 20 名員工，即使不採用指紋識別裝置，要監察員工的出勤情況亦相對容易。坤麗可採用其他無需收集或保存額外的個人資料的替代方法，例如上文第 24 及 25 段提到的密碼及載有識別碼的智能卡。此外，它亦可採用上文第 26 段提及的載有員工指紋模板的智能卡。然而，有關智能卡應該是不具名的，並且只由有關指紋所屬的員工持有。此外，監察辦公室入口情況的閉路電視鏡頭理應可對代人打卡的行為（如有）發揮阻嚇作用。

36. 經小心考慮上述所有因素後，專員認為坤麗為達致保安及員工考勤的目的，並非有絕對必要收集員工的指紋資料。坤麗當時已備有不涉及收集額外的個人資料的方法替代收集員工的指紋資料，例如智能卡及密碼。雖然採用指紋識別裝置來收集指紋資料，便利了坤麗在保障辦公室的安全及員工考勤方面的工作，惟此做法帶來的好處與其對員工構成的潛在私隱傷害不合乎比例。

37. 因此，專員認為坤麗在本案的情況下收集員工的指紋資料屬超乎適度，因而違反了條例的保障資料第 1(1)原則。

(d) 坤麗收集指紋資料屬不公平（保障資料第1(2)原則）

38. 雖然專員尊重資料當事人為不同的合法目的，而自願同意提供其指紋資料的意願，但是專員亦關注有關的同意是否在自願及知情的情況下作出。

39. 自願的同意是在沒受到不當的壓力或影響下自由地給予的同意。在雙方的談判實力不均等的情況下，例如在本案的僱傭關係中，如果員工除提供指紋資料外並無其他選擇，有關的同意不能被視作員工自由地給予的。由於坤麗並無向員工提供其他替代方法，而硬性規定員工必須提供指紋資料，專員因此有理由相信，坤麗的員工就如本案的投訴人一樣，並非自願地給予同意。

40. 至於同意是否在知情的情況下作出，則須考慮坤麗有否告知員工提供指紋資料對私隱的影響。然而坤麗並無向員工提供相關資訊，例如指紋識別裝置會收集部分還是完整的指紋圖像；指紋識別裝置如何運作；指紋資料可能會被轉移予甚麼類別的人士；收集及使用指紋資料的相關私隱風險；有甚麼措施防止資料被濫用或不當處理；員工有何渠道去查詢他的出勤紀錄的準確性；指紋資料的保存期限；以及誰有權存取指紋資料等。由於坤麗未能解答上述大部分問題，因此被視為無法採取措施防止員工的指紋資料外洩或被不當處理。

41. 簡而言之，坤麗員工就提供指紋資料所給予的所謂同意不是在自願及知情下作出。因此，專員認為坤麗在本案的情況下收集員工的指紋資料屬不公平，因而違反了條例的保障資料第 1(2)原則。

(e) 結論

42. 基於上述原因，專員裁定坤麗為保案及員考勤的目的而收集員工的指紋資料，違反了條例的保障資料第 1(1)及(2)原則。

V. 其他建議

43. 多年前，幾乎只有在政府施政項目及執法活動上才使用指紋識別技術，如簽發身份證明文件、邊境管制及刑事調查等。時移世易，科技的發展提升了指紋識別裝置的效能，亦降低了使用指紋識別技術來識別身

份的成本，此技術應用於一般消費者市場範疇上亦因而日趨普及。今天，指紋識別裝置俯拾即是，價格相宜及應用廣泛。任何人隨意地逛逛電腦商場或瀏覽 eBay 網站，也可以輕易地搜尋到不同型號的指紋識別裝置，價格可低至港幣 200 元。正因如此，有住宅及商業單位採用指紋門鎖。隨著指紋識別裝置的製造商標榜產品靈活方便，又可以有效地解決「相互替代打卡」的問題，越來越多的僱主為加強辦公室的保安及監察僱員出勤的目的而採用指紋識別裝置。另一個使用指紋識別技術的日常例子是以指紋代替密碼解除智能電話的屏幕鎖。

44. 社會絕不能因指紋及其他生物識別技術的普及應用而對保障個人資料私隱作出妥協。坤麗為方便採用指紋識別裝置，卻忽略潛在的私隱問題正是當中活靈活現的例子。本案說明盲目尊崇科技，而沒有深究及評估衍生的私隱風險，私隱權便成為科技的犧牲品。我們追求卓越科技無可厚非，但我們不應接受以不負責任的態度使用科技。

45. 承上文第 33 段的討論，指紋資料是高度敏感的個人資料（其他很多生物辨識資料亦如是）。指紋是與生俱來的獨特生理特徵。它是一種無可置疑的身份標識符，而且終生不變。正因指紋具有獨特及不變的性質，指紋資料必須得到妥善保護以防止出現身份盜用及不當使用的情況。指紋資料僅限在有足夠理據的情況下收集，並須加以適當行政措施及技術加強保障，以避免未獲准許的存取或使用。

46. 在收集指紋資料前，機構必須確定他們具有實際需要，而又沒有其他替代方法可達致相同目的及減低侵犯私隱的程度，才應考慮收集指紋資料。指紋識別裝置不應只因在市面上輕易購得、方便使用及價格便宜而被隨意採用。舉例來說，在需要高度保安的情況下，指紋識別裝置或許是一個合適的選擇，但純粹記錄員工出勤而言，採用指紋識別裝置的必要性則往往是令人質疑。

47. 即使機構使用指紋識別裝置的目的合理，機構仍須要進一步思考，為識別或核實個人身份至某準確程度，究竟需要收集多少隻手指的指紋及指紋上多少的資料（即紋理特徵數據）。在此方面，機構須緊記識別與核實個人身份雖是相關的程序，但並非完全相同。

48. 作為識別身份而言，使用的裝置的運作方式是「以一對眾」，即將使用者的指紋，與儲存於資料庫中的眾多指紋模版進行比對，從而識別

其身份，所收集的指紋特徵數量應根據資料庫中的指紋模版的數目來釐定。換句話說，收集每個員工的指紋特徵數據的多寡，會與進出由指紋識別裝置監控的限制區域的員工的數目成正比。

49. 另一方面，如要核實某人是否有資格使用某設備或進出限制區域，監控系統並不需要每次都從一個資料庫中識別該人的身份。當該人首次使用某設備或進出限制區域的資格獲核實後，他可把其指紋模版儲存在智能卡中（請參閱上文第 26 段），而該智能卡便等同獲得授權和資格的證明。隨後的手續就會是「以一對一」的身份核實模式進行。該名獲授權人士只須證明其指紋與其手持的智能卡中儲存的指紋模版是吻合。在這情況下，機構毋須將指紋資料集中儲存在資料庫中，反而指紋資料是由資料當事人自己掌控。

50. 此外，僱主在收集員工的指紋資料時，不應該施加不適當的影響或威脅以獲得他們的同意，因為這種行為無異於不公平收集員工的個人資料。在這方面，僱主須要緊記他們和員工之間的談判實力並不均等，員工往往沒有勇氣拒絕僱主收集指紋資料的要求。除非僱主有提供收集指紋資料以外的其他選擇，否則僱員給予的同意也可能不是自願作出的。再者，同意須是清晰的及在知情的情況下作出的。換言之，員工須要獲告之收集及使用指紋資料的私隱風險。為避免誤會或事後爭議，員工給予的同意應以書面記錄。

51. 有關收集及使用指紋資料的行政措施及技術保障的詳情，請參閱公署發布的「收集及使用生物辨識資料指引」。該指引同時適用於其他生物辨識資料，例如脱氧核糖核酸（DNA）、視網膜掃描、面部圖像、掌型和寫字方式等。