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

指引資料

銀行業界
妥善處理客戶個人資料
指引

目錄

1. 引言

銀行及其他金融機構(統稱「**銀行**」)在本港市民的日常生活中擔當著重要的角色。它們在日常營運中收集、持有、處理及使用大量客戶的個人資料,包括姓名、聯絡資料、身份證明文件號碼、就業詳情、財務及信貸資料等。大多數人認為他們的銀行/財務資料屬敏感資料,應該特別小心處理。因此銀行在保障客戶的個人資料方面應確保其資料私隱政策及實務依從**《個人資料(私隱)條例》(第486章)**(「**條例**」)的規定。

本指引旨在協助銀行業界了解及遵從條例的相關規定,以及在客戶個人資料的收集、準確性、保留、使用、保安及查閱方面採取良好的行事方式。

2. 條例相關規定的概覽

2.1 何謂個人資料?

「**個人資料**」指與在世的個人有關並已記錄的資料(包括意見的表達),而從該資料可直接或間接確定該人的身份。常見銀行客戶個人資料包括姓名、地址、電話號碼、身份證號碼、出生日期、職業、帳戶資料、財務資料等。

2.2 誰有責任?

條例第4條規定,「資料使用者」不得作出違反保障資料原則的作為或從事違反任何該等原則的行為。除了保障資料原則,條例的其他條文亦對資料使用者具約束力,例如第V部有關查閱及改正個人資料、第VIA部有關直接促銷的條文等。根據條例,「**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。毫無疑問,就銀行持有其客戶的個人資料而言,銀行是資料使用者。因此,銀行必須遵守條例的所有規定,以保障客戶的個人資料私隱。

2.3 六項保障資料原則

條例附表1的六項保障資料原則載列資料使用者在處理個人資料時必須依從的公平資訊實務。這些原則規管個人資料的收集、準確性、保留、使用、保安、政策及實務的透明度,以及查閱及改正。

2.3.1 收集個人資料的目的及方式

保障資料第1原則(「**第1原則**」)規定個人資料只可為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;資料的收集對該目的而言是必需的或直接與該目的有關;及所收集的資料屬足夠但不超乎適度。此外,該原則規定個人資料須以合法及公平的方法收集,並列明資料使用者直接向資料當事人收集個人資料時必須向該當事人提供的資訊。

實例:

銀行收集客戶的個人資料時,應小心考慮收集的每項資料是否必需。例如:收集儲蓄戶口客戶的姓名及聯絡資料對於為客戶提供帳戶服務是必需的,但為這目的而收集客戶的所屬種裔或宗教信仰資料一般而言屬超乎適度。如客戶被要求提供其個人資料,他們應獲提供一份《收集個人資料聲明》。有關《收集個人資料聲明》的詳細指引,請參閱下文第3.1段。

2.3.2 個人資料的準確性及保留期間

保障資料第2原則(「**第2原則**」)規定資料使用者必須採取所有切實可行的步驟,以確保個人資料準確及不會保留超過所需的時間。如資料使用者轉移個人資料(不論是在香港境內或境外)予「資料處理者」代其處理,該資料使用者須採取合約規範或其他方法,以確保有關資料不會被保留超過所需的時間。「**資料處理者**」指代另一人處理個人資料及並不為本身目的而處理該資料的人。資料處理者的例子有資訊科技服務提供者、支薪服務公司及廢紙處理公司。

此外，條例第26條規定資料使用者須採取所有切實可行的步驟刪除已不再為使用目的而需要的個人資料，除非受任何法律禁止或不刪除該資料是符合公眾利益的。

實例：

(1) 銀行向客戶發出銀行結單前，採取所有切實可行的步驟以確保客戶的地址準確無誤是十分重要的。如寄發至錯誤的地址，客戶的財務資料便可能會被披露予無關的第三者。因此銀行應定期提醒客戶，如聯絡資料有變，應通知銀行，並提供渠道讓客戶作出通知。

(2) 銀行應制定政策及措施，指明保留客戶個人資料的期限。

2.3.3 個人資料的使用

保障資料第3原則(「**第3原則**」)規定除非事前取得資料當事人的「訂明同意」，否則個人資料不可用於「**新目的**」，即該資料的收集目的或與之直接有關的目的以外的任何目的。在這方面，「**使用**」包括個人資料的披露或轉移。根據條例第2(3)條，「**訂明同意**」指資料當事人自願給予的明示同意，而這同意並未被書面撤回。訂明同意可以由「**有關人士**」代下述資料當事人作出：

(a) (i)未成年人、(ii)無能力處理本身事務的人，或(iii)精神上無行為能力的人；及

(b) 無能力理解該新目的及決定是否給予訂明同意的人，

但條件是有關人士及資料使用者均有合理理由相信更改資料用途明顯是符合該資料當事人的利益。

「**有關人士**」指：

(a) 對該未成年人負有作為父母親的責任的人；

(b) 就無能力處理本身事務的人而言，由法庭委任以處理該等事務的人；

(c) 《精神健康條例》(第136章)第IIIA或IVB部所指的精神上無行為能力的人的監護人。

此外，根據條例第64條，任何人披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料，而該項披露是出於以下意圖的，該人即屬犯罪[1]：

(a) 獲取金錢得益或其他財產得益，不論是為了令自己或另一人受惠而獲取；或

(b) 導致該當事人蒙受金錢損失或其他財產損失。

如任何人，無論出於甚麼意圖，披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料，而該項披露導致該當事人蒙受心理傷害，該人即屬犯罪。

實例：

(1) 一般來說，除非銀行已取得客戶的訂明同意，否則不應向客戶的僱主或家人披露客戶的帳戶資料。

(2) 甲銀行的前職員不應將甲銀行客戶的個人資料用作促銷乙銀行(其現職僱主)的貸款轉讓服務。

(3) 銀行職員不應未得銀行准許而從銀行的紀錄拿取不利於客戶的財務資料，並在網上披露，令客戶蒙受心理傷害。

[1] 最高刑罰是罰款一百萬元(HK$1,000,000)和監禁五年。

2.3.4 個人資料的保安

保障資料第4原則(「**第4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。如資料使用者轉移個人資料(不論是在香港境內或境外)予資料處理者代其處理，該資料使用者須採取合約規範或其他方法，以確保有關資料受保障。

實例：

(1) 儲存於資料庫、電腦或便攜式儲存裝置的客戶資料應以足夠的資訊科技保安措施及存取管控措施加以保護。

(2) 銀行如聘用市場推廣公司進行客戶意見調查，須確保轉移至市場推廣公司的資料獲安全處理及在使用後妥善刪除，以避免有關資料被未獲准許的查閱或使用。

2.3.5 資訊須在一般情況下可提供

保障資料第5原則(「**第5原則**」)規定資料使用者須採取所有切實可行的步驟，以確保下述事項公開及具透明度：個人資料方面的政策及實務、他們所持有的個人資料的種類、資料的主要使用目的。

實例：

銀行應制定並向公眾提供其《私隱政策聲明》，詳細列明所持有的個人資料的種類、個人資料的主要使用目的，以及其私隱政策和實務。《私隱政策聲明》可於銀行的網站展示。

2.3.6 查閱個人資料

保障資料第6原則(「**第6原則**」)訂明資料當事人有權查閱及改正他們由資料使用者所持有的個人資料。根據條例第19及23條，資料使用者須於收到要求後40日內依從要求。條例第V部載列有關查閱資料要求及改正資料要求的詳細條文。

實例：

一名銀行客戶最近更改了他的國籍，並已通知他的銀行。為確認銀行是否已更改他的國籍紀錄，他可向銀行提出查閱資料要求以確認銀行是否在特定紀錄中(例如客戶資料庫)存有他的國籍資料，及在40日內獲提供有關紀錄的複本。有關查閱資料要求的進一步論述，請參閱下文第3.11段。

2.4 《個人信貸資料實務守則》

條例第12條賦權個人資料私隱專員(「**專員**」)可發出實務守則，為就施加予資料使用者的條例下的規定提供實務性指引。為規管信貸提供者透過信貸資料機構共用及處理個人信貸資料，專員發出《個人信貸資料實務守則》。這守則涉及現在或曾經是客戶或信貸申請者的個人資料的收集、準確性、保留、使用、保安、查閱及改正。這守則一方面涵蓋信貸資料機構；另一方面涉及信貸提供者與信貸資料機構和追收欠款代理的業務往來。如資料使用者沒有依從《個人信貸資料實務守則》的條文，則在根據條例相關規定進行的任何法律程序中，可作出不利於該資料使用者的推定。

因此，銀行作為信貸提供者在處理客戶的信貸資料時，應參考《個人信貸資料實務守則》作為指引。

2.5 條例第VI A部–直接促銷

2.5.1 直接促銷的新法例

《**2012年個人資料(私隱)(修訂)條例**》重整有關直接促銷的規管架構，條例第34條被新的第VI A部取代，於2013年4月1日生效。

在新機制下，資料使用者使用個人資料作直接促銷前，必須採取下述「**指明行動**」：

(1) 告知有關資料當事人：

(a) 該資料使用者擬如此使用有關資料；

(b) 該資料使用者須收到該資料當事人對該擬進行的使用的同意，否則不得如此使用該資料；

(c) 擬使用的資料的種類；

(d) 擬促銷的產品或服務的類別；及

(2) 向該資料當事人提供一個回應途徑，以傳達其同意。

上述資訊必須以易於理解及閱讀（如以書面作出）的方式展示。資料使用者未得資料當事人的同意，不得使用有關資料作直接促銷，而在得到資料當事人的同意下，如此使用只限於資料當事人許可的資料種類及物品或服務類別。

此外，資料使用者不得提供個人資料予另一人（「**接收資料者**」）以供用於直接促銷，除非該資料使用者已：

(1) 以易於理解及閱讀的方式以書面告知有關資料當事人：

(a) 該資料使用者擬如此提供有關資料；

(b) 該資料使用者須收到該資料當事人對該擬進行的資料提供的書面同意，否則不得如此提供該資料；

(c) 該資料是擬為得益而提供的（如是這樣的情況）；

(d) 擬提供的資料的種類；

(e) 該資料擬提供予甚麼類別的人士；

(f) 擬促銷的產品或服務的類別；

(2) 向該資料當事人提供一個回應途徑，以傳達其書面同意；及

(3) 收到該資料當事人的書面同意。

任何如此提供的資料只限於資料當事人許可的資料種類、資料承轉人的類別及產品或服務的類別。如資料使用者已以書面告知接收資料者他已遵從上述提供資料的規定，並指明許可的產品或服務類別，接收資料者在使用有關資料作直接促銷許可類別的產品或服務前，便不需要採取上述指明行動或再取得客戶的同意。不過，如資料當事人在任何時間提出要求，則資料使用者必須停止提供其資料予他人作直接促銷，而接收資料者必須停止在直接促銷中使用該資料。

資料使用者首次使用個人資料作直接促銷時，必須告知資料當事人，他有權拒絕資料使用者如此使用其個人資料。如資料當事人提出「**拒絕服務**」要求（不論他之前有否同意如此使用其個人資料，他有權隨時這樣做），資料使用者必須停止如此使用該資料。

以上概述了新直接促銷機制下的主要規定，條例亦有關於處理生效日期前的資料（即資料使用者於2013年4月1日前已控制使用的個人資料）的具體條文。有關直接促銷的詳細討論，請參閱專員發出的《**直接促銷新指引**》。

2.5.2 制定及落實政策、程序及指引以確保遵從規定

為確保遵從有關直接促銷的規定，銀行應制定及落實私隱政策、程序及指引，並採取所有切實可行的步驟，確保職員遵從規定。銀行必須遵守向客戶傳達擬使用或提供其個人資料作直接促銷的規定，及尊重客戶對如此使用有關資料的自決權。銀行應考慮採取《直接促銷新指引》所建議的保障私隱良好行事方式。更重要的是，最高管理層應知道銀行的責任，支持及推動銀行遵從相關規定，並制定標準營運程序及指引。

2.6 銀行就職員、代理及承辦商的作為所負的法律責任

2.6.1 僱主及主事人的法律責任

根據條例第65(1)及(2)條，僱員在其受僱用中或代理人在授權下所作出的任何作為或所從事的任何行為，須視為亦是由其僱主或主事人所作出或從事的。因此，銀行須為其職員在向客戶提供服務期間所作出的作為或所從事的行為負責。銀行亦須為其代理或承辦商，例如資訊科技承辦商、追收欠款代理或市場推廣代理在獲授權範圍內所作出的作為或所從事的行為負責。

對於僱員被指稱所作出的作為或所從事的行為，如僱主能證明已採取切實可行的步驟，防止僱員作出該作為或從事該行為，僱主可以此為免責辯護。

因此，銀行應採取下述預防措施。

2.6.2 有關職員的預防措施

銀行應採取切實可行的措施，確保能查閱客戶個人資料的職員得到有關個人資料處理及保障的培訓、謹慎應用銀行的個人資料私隱政策，以及受藉以依從此等政策的措施所規範。在制定及落實有關客戶個人資料的政策及內部程序時，銀行應留意下述事宜：

(1) 定期及有系統地傳遞有關政策予職員；

(2) 持續向職員提供保障個人資料的培訓；

(3) 向新入職職員提供保障個人資料的培訓以作為入職指導的一部分；

(4) 定期檢討及更新有關政策規程、培訓教材及手冊；

(5) 對個人資料的查閱及處理，採取只限於「有需要知道」及「有需要使用」的原則；

(6) 規定職員簽署保密聲明，該聲明清楚述明銀行在這些方面的工作期望及違規可能受到的處分，或將該聲明納入職員手冊或行為守則中；

(7) 如發生違規事件，應進行適當的調查程序，並對違規職員採取適當的行動；

(8) 制定適當的系統監控及進行定期內部稽核和隨機抽查，以確保職員遵從既定的政策及程序。

2.6.3 有關代理及承辦商的預防措施

如銀行委託第三者，例如追收欠款代理、數據程式編寫員、資訊科技承辦商或密件處置公司，以處理客戶的個人資料，應確保資料在處理過程中受到保障及安全地被刪除。銀行應考慮採取下述預防措施（如適用），以保障個人資料：

(1) 揀選信譽良好及有能力保障個人資料的代理或承辦商；

(2) 在代理或承辦商的服務合約中加入下列要求：

(a) 列明代理或承辦商須採取的保安措施，以保障所收到、閱覽、處理或使用的個人資料；

(b) 代理或承辦商不得處理、使用或披露個人資料於合約沒有指明的目的上；

(c) 列明銀行及代理或承辦商須依從保障資料原則的責任；

(d) 代理或承辦商在完成使用個人資料作受聘提供服務的目的時，須適時交還及在系統中徹底刪除資料及任何備份；

(e) 適時報告任何與個人資料保安有關的不尋常徵兆或保安違規情況；

(f) 代理或承辦商應保證其職員已接受適當的個人資料處理培訓；

(g) 如分判工作涉及處理或使用個人資料，代理或承辦商在沒有銀行的明確同意下，不得分判工作；

(h) 代理或承辦商須負責分判商在處理個人資料方面的行為；

(3) 不應把載有個人資料的資訊發放予代理或承辦商，除非代理或承辦商必須得到該等資訊才可完成工作；

(4) 不應為系統測試的目的而把載有真實個人資料的資訊發放予資訊科技承辦商(而是利用虛擬資料代替)；

(5) 應妥善地標籤交予代理或承辦商而載有個人資料的資訊；

(6) 應對交予代理或承辦商的所有個人資料及其後的移轉歷程作出適當的記錄及予以保存；

(7) 應就交予代理或承辦商的個人資料的使用、處理、傳送、儲存及銷毀向代理或承辦商發出清晰的指示；

(8) 應不時對代理或承辦商作出審查，以確定他們在處理個人資料時有否執行所需的保安措施及責任；

(9) 應不時對代理或承辦商作出審查，以確定他們有否對負責處理個人資料的職員進行適當的核查。

如銀行聘用資料處理者，亦應參考專員發出的《**外判個人資料的處理予資料處理者**》資料單張。

3. 保障客戶的個人資料私隱權利

下文旨在協助銀行業界更了解條例在有關客戶個人資料的特定範圍的應用，以促進銀行遵從條例的規定，並採取良好的行事方式處理客戶的個人資料。

3.1 《收集個人資料聲明》

3.1.1 內容

為遵從第1(3)原則的規定，公署建議銀行制定包含下述資訊的《收集個人資料聲明》，並向客戶提供這份聲明。

(1) **目的聲明**：這是關於客戶個人資料在收集後的使用目的的聲明。雖然聲明可以一般或具體措辭作出，但有關目的必須明確列明。銀行不應使用寬鬆或模糊的字眼，因為這會令客戶不能合理地確定其個人資料會被如何使用。簡單的目的聲明例子：「從閣下收集的資料會用於處理閣下開立投資帳戶的申請。」

(2) **承轉人聲明**：這聲明須清楚列明個人資料可能會被轉移予的第三者類別，並應合理地清晰說明承轉人的類別。例子：「閣下在本帳戶開立表格中所提供的資料可能會為防止清洗黑錢的目的而轉移予執法機構。」

(3) **自願或有責任提供資料**：除非情況明顯，否則銀行應清楚告知客戶他們是有責任抑或是可自願提供個人資料；如屬有責任提供，銀行便要告知客戶沒有提供資料的後果。即使屬自願提供，良好的行事方式亦應列明不提供資料的後果。例子：「閣下在本投訴表格中就投訴銀行服務所提供的個人資料屬自願性質。不過，如閣下不提供資料，我們未必能處理閣下的投訴。」

(4) **查閱及改正資料的權利：**銀行必須清楚告知客戶其查閱及改正個人資料的權利，以及負責處理有關查閱及改正資料要求的人員的姓名(或職銜)及地址。例子：「根據《個人資料(私隱)條例》，閣下有權就本銀行持有閣下的個人資料提出查閱或改正資料要求。閣下的要求會由本銀行的客戶服務經理處理，其地址為……。如閣下希望提出有關要求或有任何疑問，請聯絡本銀行的客戶服務經理……(註明地址或聯絡方式)」

3.1.2 採取哪些切實可行的步驟

第1(3)原則規定銀行採取所有切實可行的步驟，在收集客戶的個人資料之時或之前向客戶提供上述訂明的資訊(有關查閱及改正資料的權利的資訊可在首次使用有關資料之時或之前才提供)。雖然條例沒有規定以書面提供有關資訊，銀行的審慎做法是以書面告示(即《收集個人資料聲明》)通知客戶。方法可以是把《收集個人資料聲明》納入於服務申請表格內，或以《收集個人資料聲明》作為獨立告示隨附申請表格給予客戶。如銀行是透過電話收集個人資料，除非在該通話前已向客戶提供《收集個人資料聲明》或這樣做不是切實可行的，否則在收集個人資料前仍須提供訂明資訊，例如以錄音訊息提供。在這情況中，良好的行事方式是隨後再向客戶補發書面的《收集個人資料聲明》。

銀行可能在不同情況為不同服務種類而向客戶收集個人資料，例如開立保險箱或處理貸款申請。因此，銀行應確保所使用的《收集個人資料聲明》適用於該特定的情況。

銀行應特別留意客戶的不同需要(讀寫能力、母語等)，因應收集個人資料的實際情況，以清晰簡單的語言，易於查閱、閱讀及理解的方式有效地傳達其訊息。

為確保《收集個人資料聲明》有效，銀行需要考慮下述因素：

(1) 《收集個人資料聲明》的描述和展示(包括字體的大小及距離、以及運用底線、標題、亮點及對比)，是否讓一般擁有正常視力的客戶易於閱讀；

(2) 《收集個人資料聲明》是否清晰表達(例如作為服務申請表格的一個獨立部分，其內容不混合在銀行提供服務的條款及細則之中)；

(3) 《收集個人資料聲明》中的用語是否易於理解(選用淺白的字詞，避免艱澀詞語、法律詞彙及晦澀難解的詞組)；

(4) 銀行是否有提供進一步協助，例如服務台或查詢服務，以協助客戶了解《收集個人資料聲明》的內容。

至於為相同目的而重複收集客戶的個人資料，如銀行曾在12個月內收集客戶的個人資料並已向客戶提供《收集個人資料聲明》，便無須再向客戶提供同樣的《收集個人資料聲明》[2]。

3.1.3 個案研究

(1) 向儲蓄戶口申請人收集額外資料[3]

投訴內容
一間銀行要求一名申請儲蓄戶口的客戶提供其「教育程度」及「婚姻狀況」。該銀行解釋，收集這兩項個人資料，是為了向客戶推廣其產品及服務。申請表格沒有註明這兩項資料屬「非必須」提供的資料。

結果
在為向客戶提供儲蓄戶口服務而言，「教育程度」及「婚姻狀況」並不屬於必須資料。即使有關資料有助銀行進行客戶分析，例如以便用於直接促銷，銀行也不應收集這些資料，除非這些資料是客戶自願提供的[4]。

縱使該銀行澄清客戶沒有責任提供這兩項資料，專員認為該銀行沒有採取所有切實可行的步驟確保以明確或暗喻方式將上述情況告知客戶，因而違反了第1(3)(a)(i)原則的規定。該銀行其後修訂了它的儲蓄戶口申請表，註明「教育程度」及「婚姻狀況」兩項資料屬非必須提供的資料，並提示前線職員此收集客戶個人資料的要求。

2 條例第35條。
3 請參閱專員於2011年12月15日發出編號R11-8371的調查報告。
4 請參考《直接促銷新指引》。

(2) 在街頭推廣活動中收集信用卡申請者的個人資料[5]

投訴內容

一名信用卡客戶投訴銀行轉移其個人資料予保險公司以向他進行促銷。該銀行在一個冬季的傍晚於街頭推廣活動中，透過該客戶簽署的一份信用卡申請表格收集其資料。該銀行以申請文件中的提示、聲明及條款和夾附於申請表的《私隱政策聲明》作為將客戶資料披露予保險公司的依據。《私隱政策聲明》當中列明：「[該銀行]會把其取得有關資料當事人的資料保密處理，但可能會把該等資料提供予：……(xi)會向資料當事人提供[該銀行]相信資料當事人會感興趣的服務資訊的特選公司。」

結果

在考慮到該客戶的視力問題、年紀及事件發生於一個冬季傍晚的街頭推廣活動，專員認為在如此情況下，該客戶亦難以仔細閱讀、考慮及理解申請文件所載的提示、聲明、條款及該《私隱政策聲明》。此外，專員發現該《私隱政策聲明》是以不合理地細小的字體印刷，而且以寬鬆及模糊的字眼描述資料承轉人的類別，令該客戶無法合理地確定誰可使用其個人資料。總的來說，該銀行沒有清楚告知該客戶其個人資料可能會轉移予甚麼類別的人士，因而違反了第1(3)(b)(i)原則的規定。

3.2 收集非帳戶持有人的身份識別文件號碼

3.2.1《身分證號碼及其他身分代號實務守則》

毫無疑問，銀行會向其帳戶持有人收集身份識別文件號碼。但非帳戶持有人偶爾要求銀行提供如貨幣兌換、簽發本票或電匯服務的情況便有所不同。在這情況下，銀行只可在交易金額超過訂明上限時才收集非帳戶持有人的身份識別文件號碼（見下文）。

根據第1(1)原則，銀行不得向非帳戶持有人收集個人資料，除非有關收集是向該客戶提供服務所必需或直接有關的。此外，收集身份證號碼或其他身份識別文件號碼受專員發出的**《身分證號碼及其他身分代號實務守則》**（「**身分代號守則**」）規管。除非屬身分代號守則第2.3段所准許的指定情況，否則資料使用者不得收集個人的身份證號碼或其他身份識別文件號碼。此外，根據身分代號守則第2.2.1段，有關個人應獲提供選擇，以提供其他身份識別文件號碼（例如護照號碼）來代替其身份證號碼。

與這方面特別相關的是身分代號守則第2.3.1段，以及**《打擊洗錢及恐怖分子資金籌集（金融機構）條例》（第615章）**（「**打擊洗錢條例**」）附表2關於就客戶作盡職審查及備存紀錄的規定。身分代號守則第2.3.1段列明，如法定條文要求資料使用者向個人收集身份證號碼（或其他身份識別文件號碼），則資料使用者可以如此收集。在考慮打擊洗錢條例是否要求銀行作為**《銀行條例》（第155章）**授權的機構（「**獲授權機構**」）收集非帳戶持有人的身份識別文件號碼方面，打擊洗錢條例附表2第3(1)(b)、3(1)(c)、12及20(1)條關於為客戶進行「**非經常交易**」（定義見打擊洗錢條例附表2第1(1)條）而為客戶作盡職審查及備存紀錄的責任與此相關。根據現行規定，獲授權機構如為非帳戶持有人進行的非經常交易總值涉及相等於12萬港元或以上的款額，而不論交易是以單一次操作執行，或是以該獲授權機構覺得是有關連的若干次操作執行，可收集該人的身份識別文件號碼；但如屬電傳轉帳的非經常交易，有關要求則是八千港元或以上的總值。

[5] 請參閱專員於2011年6月20日發出編號R11-1982的調查報告。

3.2.2 個案研究－貨幣兌換

投訴內容
投訴人到一間銀行把一張五百港元的紙幣兌換為五張一百港元的紙幣。由於他並無持有該銀行的帳戶，櫃台職員根據該銀行的政策記錄投訴人的姓名及身份證號碼。

結果
專員認為沒有表面證據顯示該次貨幣兌換(金額少於12萬港元)涉及清洗黑錢或恐怖分子資金籌集活動，因此沒有足夠理據證明在個案的情況下收集投訴人的姓名及身份證號碼是合理的。該銀行其後已停止有關做法。

3.3 客戶聯絡資料的準確性

3.3.1 避免披露客戶的個人資料予非預期的收件人

第2(1)原則規定銀行要確保客戶個人資料準確。如有關資料不準確，銀行應修正或刪除該資料。因此，銀行在聯絡客戶前(例如向客戶發出載有個人資料的文件)，確保其聯絡資料準確無誤是十分重要的，否則資料可能會被披露予第三者。

不過，這規定並非絕對責任。只要銀行已採取所有切實可行的步驟確保資料準確，即使資料原來是不正確，銀行也沒有違反這項規定。

3.3.2 個案研究－銀行文件被寄往錯誤及不完整的地址[6]

投訴內容
一名信用卡客戶向一間銀行提供其位於「石塘咀」的通訊地址。由於在輸入客戶地址的系統中地區一欄的下拉選項沒有「石塘咀」，銀行職員於是選取「小欖」作為地區。當該客戶收到該銀行的信件後(儘管地址錯誤)，她發現有關錯誤，於是透過該銀行的修改表格提出改正資料要求。該客戶之後沒有再收到該銀行發出的信用卡結單，其後從該銀行得悉她的結單被寄往一個沒有註明室號及樓層資料的地址，因為該銀行的職員在處理她的改正資料要求時，沒有在系統中輸入室號及樓層資料。在這兩次事件中，該銀行的複核程序均未能發現錯誤。

結果
專員認為該銀行出錯是因其僱員不小心及複核程序失敗所致。該銀行沒有採取所有切實可行的步驟，確保客戶的地址資料準確，因而違反了第2(1)原則。專員認為透過改善該銀行的電腦系統及自動／人手檢查程序，日後可避免再發生類似錯誤。

3.4 客戶個人資料的保留

3.4.1 制定保留政策

為了依從第2(2)原則及條例第26條有關保留客戶個人資料期限的規定，銀行應制定及實施清晰的私隱政策及措施，確保資料在完成收集目的後被刪除。在決定保留期限時，銀行應考慮資料的使用目的及相關的法定規定和適用的指引[7]。

舉例說，銀行可在建立相關資料後或與客戶結束業務關係後(視情況而定)，為依從各項法律或規管對保留帳目或客戶紀錄的要求、處理潛在訴訟等目的，保留客戶的個人資料七年。不過，不同類型的個人資料可有不同的保留期限，須視乎個別情況而定。某些例外情況可能需要較長的保留期限，例如：

(1) 為處理目前或即將進行的法律訴訟或索償；

(2) 為處理有關客戶或規管／執法機構目前的查詢或投訴；

(3) 為對有關客戶履行合約責任；

(4) 為保留證據，因為有合理理據相信有人已經干犯或將會干犯罪行，而銷毀證據會妨礙執法機構調查罪行；

(5) 為依從法律或法定責任而保留個人資料；

(6) 為依從規管機構發出的實務守則或指引，而有關的實務守則或指引並非與條例不相符。

6 請參閱專員的個案簡述編號2009C08(載於公署網站)。
7 例如，打擊洗錢條例附表2第20條關於保留客戶紀錄的規定。

銀行必須細心考慮收集資料的目的，以良好的判斷能力及謹慎的態度決定保留客戶個人資料的適當期限。任意地保留個人資料會增加個人資料外洩的風險，及增加保障資料免受未經准許的查閱或使用的成本，可能損害客戶的利益。如專員接獲投訴，有關銀行便須解釋及證明為何當時仍須保留有關個人資料。

有關如何永久刪除個人資料或將個人資料匿名化至不能再識別相關人士，銀行可參閱專員發出的《**個人資料的刪除與匿名化指引**》。

3.4.2 個案研究－保留客戶的破產資料[8]

投訴內容

投訴人投訴一間銀行在他獲解除破產後很久仍保留其破產資料。在跟進此投訴的過程中，揭示了該銀行的做法是保留客戶的破產資料99年。破產管理署署長會定期向該銀行提供破產資料，以進行調查及扣押破產者的資產。

專員展開調查後，該銀行把保留時間縮短至由結束客戶的帳戶日期起計的15年，並列舉多個理由解釋。

結果

專員認為該銀行所提出的理由不合理，故拒絕接納。專員認為破產資料不應被保留超過八年，因為破產人士通常在破產開始起計的四至八年後獲解除破產令。因此，該銀行保留有關資料的做法是超過所需的時間，因而違反了第2(2)原則及條例第26(1)條。該銀行其後修訂其政策，不會保留客戶的破產資料超過八年（由宣佈破產日起計）。

3.5 集團內部共用客戶的個人資料

3.5.1 告知客戶任何擬進行的資料共用

在香港，銀行通常屬集團擁有，可以是集團的總公司，亦可以是由控股公司為首的集團的其中一間成員公司。這些機構主要涉及（但不一定是唯一的）提供金融服務，例如銀行、證券及保險。有時是有需要在集團內共用客戶的個人資料，以為客戶提供他要求的服務或進行直接有關的事宜。在這些情況中，銀行應在其《收集個人資料聲明》中告知客戶擬共用資料的詳情。除了第1(3)(b)(i)原則訂明的資訊，聲明中亦可包括擬共用的資料種類。在適當的情況下，良好的行事方式也包括告知客戶，銀行在共用資料的過程中所採取的保安措施及在使用後安全棄置有關資料之做法。

3.5.2 不要更改資料的使用目的或共用非必要的資料

根據第3原則規定，客戶的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。值得注意的是銀行在收集客戶個人資料時向其提供的《收集個人資料聲明》，並不是斷定銀行原先收集該個人資料的目的及是否有違第3原則的唯一考慮因素，其他考慮因素包括例如交易的性質及收集資料的情況。除非已取得訂明同意，銀行在集團內共用該資料應限於收集資料的目的或直接有關的目的，包括向客戶提供銀行服務，並基於「有需要知道」及「有需要使用」的原則。

此外，在考慮到共用資料的目的，被共用的資料應屬足夠但不超乎適度。共用非必要的資料可構成違反第3原則的規定。

[8] 請參閱專員於2011年12月15日發出編號R11-6121的調查報告。

3.5.3 記錄共用資料的去向及確保在使用後妥善處置資料

為確保集團內共用個人資料的保安及適時處置資料，銀行需要監察資料的去向。公署建議銀行適當地記錄資料的移轉歷程並保存紀錄。如共用資料的目的已達到，提供資料的銀行及收取資料的集團公司應確保適時從後者的檔案及紀錄中徹底刪除有關資料，除非有合理理由繼續保留資料。

3.5.4 就共用客戶個人的資料制定集團政策

如在集團內共用客戶個人資料是集團的慣常做法，則採取一套整體的資料保障系統明顯是明智的。因此，如一個銀行集團經常共用客戶資料，它應設有集團性的私隱政策及程序，規管集團內有關活動。有關政策及程序應涵蓋(i)客戶通知及(ii)共用資料的收集、持有、處理、準確性、查閱、使用、共用、傳輸、保安及棄置。銀行亦應清楚列明每間集團公司及其負責處理資料的人員的個別責任。

3.6 轉移客戶的個人資料至香港以外地方

條例第33條禁止個人資料轉移至香港以外地方，除非符合該條所列的其中一項條件。不過，這條文尚未實施。無論如何，轉移個人資料(不論在香港境內或境外)亦須遵從第1(3)原則(通知資料當事人資料承轉人的類別)、第2原則(不轉移不準確的資料；防止轉移予資料處理者的資料被保留超過所需的時間)、第3原則(不更改使用目的)及第4原則(保障資料安全)。此外，如在轉移個人資料後，資料使用者仍保留對資料的控制，則就轉移的資料而言，條例的所有條文繼續適用。舉例來說，如資料使用者轉移資料予香港境外的外判代理進行處理，該資料使用者須就其代理不當處理個人資料的所有作為負上法律責任。

全球性轉移資料在今日的銀行活動中是常見及重要的一環，對於轉移客戶的個人資料至香港以外地方，銀行應留意下述的建議(大部分亦適用於香港境內)。

3.6.1 在收集資料時告知客戶轉移資料事宜

如銀行擬把所收集的個人資料轉移至香港以外地方，在收集資料時，銀行應告知客戶資料承轉人的類別。此外，良好的行事方式亦包括告知客戶將轉移至香港以外的資料種類、轉移的目的，及資料被轉移至的地方(如銀行認為適合)。如銀行沒有轉移資料的意圖，亦可告知客戶。

3.6.2 不更改資料的使用目的及不轉移不準確的資料

為遵從第3原則，客戶個人資料的任何轉移必須符合資料原本的收集目的或直接有關的目的。

如有合理理由相信有關資料是不準確，除非及直至資料已被更正，否則不應轉移有關資料，這是第2(1)原則所規定的。

3.6.3 保障資料所採取的步驟

第4(1)原則的規定包括安全傳輸個人資料。在傳輸客戶資料時，銀行必須採取保安措施保障資料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。如資料是經互聯網傳送，銀行需要特別小心，確保設有足夠的保安措施，例如將資料加密。在這方面，銀行可參考專員的《**經互聯網收集及使用個人資料：給資料使用者的指引**》中「保障資料第4原則－個人資料的保安」一節。

如銀行轉移個人資料予資料處理者代其處理，該銀行須按第4(2)原則的規定採取合約規範或其他方法保障資料的安全。

3.6.4 確保在使用資料後妥善處置資料

如資料是轉移至銀行集團內的一間公司，該銀行應如上述第3.5.3段所建議，確保在達致轉移目的後適時徹底地刪除有關資料。

如資料是轉移予資料處理者代銀行處理資料，該銀行須按第2(3)原則的規定採取合約規範或其他方法防止有關資料被資料處理者保留超過所需的時間。

至於銀行可採取甚麼合約規範或其他方法以確保轉移予資料處理者的資料安全及獲得妥善處置，可參考《**外判個人資料的處理予資料處理者**》資料單張。

3.7 披露客戶的個人資料予執法機構及財經規管者

銀行應小心處理執法機構或財經規管者所提出的披露客戶個人資料的要求。如有關披露不是符合原本的收集資料目的或直接有關，只有符合條例第VIII部與第3原則有關的豁免情況才可作出披露，否則必須得到客戶的訂明同意。

3.7.1 是否屬獲豁免的目的

條例第VIII部載列一些豁免受第3原則管限的情況。其中最為相關的是第58及60B條。

如個人資料是用於第58(1)條所指明的任何目的及第3原則適用於該資料的使用便「相當可能會損害」任何該等目的，則第58(2)條豁免該個人資料受第3原則所管限。第58(1)條所指的目的包括(但不是全部)：

(a) 罪行[9]的防止或偵測；

(b) 犯罪者的拘捕、檢控或拘留；

(c) 任何稅項[10]的評定或收取；

(d) 任何人所作的不合法或嚴重不當的行為[11]、或不誠實的行為或舞弊行為的防止、排除或糾正(包括懲處)；

(e) 防止或排除因(i)任何人輕率的業務經營手法或活動；或(ii)任何人所作的不合法或嚴重不當的行為、或不誠實的行為或舞弊行為，而引致的重大經濟損失；

(f) 執行「財經規管者」的某些職能。

「財經規管者」包括香港金融管理局(「**金管局**」)、證券及期貨事務監察委員會(「**證監會**」)、香港交易及結算所有限公司、保險業監理專員及強制性公積金計劃管理局。

此外，如資料使用者在針對他違反第3原則使用個人資料而進行的法律程序中，能證明他當時有合理理由相信不如此使用該資料便相當可能會損害第58(1)條所指的任何事宜，即可以第58(2)條為免責辯護。

另一可獲豁免的情況是，如個人資料是由任何成文法則、法律規則或香港法院的命令所規定或授權使用的，或是根據任何成文法則而規定或授權使用的；或在與於香港進行的法律程序有關連的情況下被規定而使用的，則該資料獲第60B條豁免而不受第3原則所管限。

視乎個案的特定情況，披露客戶的個人資料予執法機構或財經規管者可能屬於上述其中一項豁免情況。

---

9 根據條例第58(6)條，罪行是指香港法律所訂的罪行；或(如個人資料是在與香港和香港以外地方的法律合作或執法合作有關連的情況下持有或使用的)該地方的法律所訂的罪行。

10 條例第58(1A)條規定，如與香港以外某地區的政府有訂立根據《稅務條例》(第112章)第49(1A)條有效的安排；而該地區的某稅項屬該等安排中某條文之標的，而該條文是規定須披露關乎該地區的稅項資料的，則稅項 (tax) 包括該稅項。

11 根據條例第2(9)條，凡任何人按法律規定須擔任某職位、從事某職業或行業，而該人因任何行為而令他不再是上述適當人選或該行為會令他不再是上述適當人選，該行為須視為「嚴重不當的行為」。此外，根據判例，違反法庭命令及破產警務人員嚴重負債違反《警察通例》，亦屬「嚴重不當的行為」的例子。

舉例說，證監會可根據《**證券及期貨條例**》(**第571章**)第183(1)條向銀行發出通知，要求該銀行提供某些紀錄或文件，當中可能載有客戶帳戶資料。該銀行依據該通知披露有關個人資料是獲條例第60B條豁免而不受第3原則所管限，因為有關披露是由或根據《證券及期貨條例》所規定的。

在其他情況中，銀行可能收到執法機構索取客戶個人資料的要求，聲稱有關資料是用於條例第58(1)條所述的獲豁免事宜。為援引條例第58條有關第3原則的豁免，衡量不披露有關資料的後果是否嚴重至第58(2)(b)條所述「相當可能會損害」任何有關事宜，是十分重要的。如有疑問，銀行的審慎做法是向要求資料的機構查問資料的使用目的、為何有關資料是對該目的必需或重要的，尤其是，不披露有關資料會如何相當可能損害該目的。該銀行要求對方提供更多資訊，有利它在被指違反第3原則披露有關資料的法律程序或投訴中援引第58(2)條下的免責辯護。該銀行作為控制有關資料的資料使用者，應弄清楚其賴以披露有關資料的豁免的適用性[12]。

3.7.2 訂明同意

如向執法機構或財經規管者披露客戶的個人資料不是符合原本的收集資料目的或直接有關，及沒有豁免適用或可被援引，銀行是不應作出披露的，除非事前已取得有關客戶的訂明同意。訂明同意必須由客戶明確及自願地作出，並應清楚及具體地涵蓋有關披露。銀行亦應注意，專員並不接受「**綑綁式同意**」作為條例所指的訂明同意。「綑綁式同意」的例子如下：資料使用者透過服務申請表收集客戶的個人資料，但該服務申請表的設計是令客戶不能拒絕該資料使用者將其個人資料用於與提供予客戶的服務無關的目的。

3.7.3 個案研究－披露帳戶紀錄予警方作紀律調查

投訴內容

一間銀行收到警方一封信件，要求該銀行提供一名警務人員(投訴人)的帳戶資料。該信表示：「[警務]人員現正進行一項紀律調查，涉及[投訴人的]財務狀況。為協助我們調查，希望貴銀行能提供[投訴人]……至……的帳戶紀錄。本人證明所要求的資料是為了紀律研訊所需，這是獲《個人資料(私隱)條例》第58(1)(d)及(2)條所豁免的。」

該銀行沒有向警方進一步詢問便將載有投訴人個人資料的帳戶資料給予警方。

結果

專員認為該銀行原本收集有關資料的目的並不包括向警方作出有關披露，而且該銀行如此使用投訴人的個人資料亦不在投訴人的合理預期之內。

在調查期間，警方向專員解釋，要求的帳戶資料是關於對投訴人涉嫌涉及嚴重財困的紀律調查，這可能涉及違反《警察通例》第6章(行為及紀律)第8段。不過，根據所得資料，資料不足以令專員信納投訴人的情況是嚴重至條例第58(1)(d)條所指的「嚴重不當的行為」。此外，專員認為該銀行不能只依賴警方的信件而令銀行信納有關披露是符合第58(1)(d)條所述情況及相信不披露有關資料會相當可能損害警方的調查。

因此，專員認為該銀行向警方披露有關資料是違反了第3原則。

[12] 憑藉條例第51條，有關披露是依據某項豁免而獲准這個單純事實本身既不對任何人賦予任何權利，亦不對任何人施加任何規定披露或強迫披露有關資料。根據判例(見高等法院案件第HCMP 2487/2005號)，援引豁免的人完全有責任以充分證據證明已符合所有相關的先決條件。

3.8 在追收欠款中的個人資料處理

3.8.1 告知客戶其個人資料可能用於追收欠款

一般來說，銀行可將拖欠還款的客戶的個人資料用於向其追討欠款，包括轉移資料予追收欠款代理作追討欠款用途。在一般情況下，這項用途是與資料的原本收集目的直接有關。第1(3)原則規定，銀行須於收集資料之前或之時，把這項用途及可能的資料承轉人（例如追收欠款代理）告知客戶。良好的行事方式是銀行亦把有關追收欠款的政策及實務告知客戶，包括何時會把客戶的甚麼資料交予追收欠款代理、銀行就安全處理有關資料而對追收欠款代理所施加的控制等。

3.8.2 避免披露資料予不相關人士

顯示客戶的財務問題的資料（例如拖欠還款）通常被視為敏感資料，因此應特別小心處理。除非有真正需要，否則銀行不應將這些資料披露予任何第三者。

在追收欠款的過程中，銀行或其代理可能要透過郵遞或電話聯絡客戶（或其獲授權代表）（「債務人」）。在向債務人發出追款信時，應小心確保地址準確，這是第2(1)原則所規定的。此外，信件應密封，上面註明「私人及機密」或「只由收件人開啟」或類似字眼，以確保遵從第4原則有關資料保安的規定。這些做法可避免信內的債務人個人資料被非預期的收件人看到。如致電給債務人時接聽者是其他人（例如其家人或同事），則不應在電話中透露欠債的資料。

除非獲法律授權，否則不應公開展示債務人的個人資料（例如在債務人的住所門外張貼追款通知），因為這樣做很可能違反第3原則的規定。

3.8.3 聘用追收欠款代理

銀行或會聘用追收欠款代理代它向客戶追收欠款。根據條例第65(2)條，銀行的代理在追收欠款過程中所作的任何獲授權的作為會被視為亦是由該銀行作出的。當該銀行轉移個人資料予代理時，該銀行作為主事人並不會因此而可以免去其確保代理遵從條例規定的責任。因此，該銀行應小心謹慎地監察及規管其代理在追收欠款過程中處理客戶資料的行為。

銀行在聘用追收欠款代理時，應留意上文第2.6.3段所列的建議。特別是，銀行需要採取措施以防止其代理在追收欠款過程中違反條例的規定，例如透過公開展示或郵寄給鄰居等方式向不相關的第三者披露債務人、其諮詢人或家人的個人資料。銀行應注意，依賴簡單的合約要求代理遵守香港法律（包括條例的規定）是不會免除銀行在條例下的法律責任的[13]。銀行應就代理收集及處理個人資料這兩方面制定實際的指引或設立限制。

此外，銀行只應向追收欠款代理披露進行其工作所必需的資料。超乎適度的披露會構成違反第3原則。在這方面，獲授權機構應留意，香港銀行公會與存款公司公會聯合發佈並得到金管局認可的《**銀行營運守則**》第9.4及38.4段規定，它們不應把諮詢人（或債務人及擔保人以外的第三者）的資料提供予追收欠款代理。如獲授權機構需要聯絡諮詢人，以確定債務人或擔保人的所在，機構應委派本身的員工，在不對諮詢人造成滋擾的情況下與諮詢人聯絡。

此外，《個人信貸資料實務守則》第2.16至2.18段載列有關信貸提供者向追收欠款代理提供個人信貸資料的事宜。根據第2.16段，信貸提供者應以合約規範方法規定其追收欠款代理在追收欠款的活動上必須符合《銀行營運守則》的規定，及應滿意該代理的聲譽，相信該代理會依從規定行事。第2.17段規定可向追收欠款代理披露的債務人資料只限於識辨及找尋該人的資料、信貸的性質，及追收的數額及可收回的貨品之詳情。最後，第2.18段規定信貸提供者在核對資料的準確性後才可向追收欠款代理提供有關資料。

[13] 請參閱專員於2010年2月24日發出編號R10-11568的調查報告。

3.8.4 個案研究

(1) 向第三者披露債務人拖欠還款

投訴內容
一間受銀行委託的追收欠款代理致電到債務人任教的學校追收欠款。根據接聽電話的校工所述，致電者表示他要向債務人追數，要求該校工催促債務人回電。

結果
專員認為在表明來電目的是追收欠款後，債務人拖欠還款的事實已披露予第三者(即本個案的校工)，這違反了第3原則的規定。

在專員介入後，該銀行向其追收欠款代理發出書面指引，規定追收欠款代理的職員在接聽來電的人士不是債務人時，只需留下自己的姓名及電話號碼。如接聽者詢問來電目的及來電者的身份，職員應回答是「私人事宜」及只披露來電者的機構名稱。

(2) 公開展示債務人親屬的個人資料[14]

投訴內容
一間財務公司把債務人的貸款申請表(內載債務人親屬的個人資料)交予其追收欠款代理，指示該追收欠款代理代其追收欠款。該追收欠款代理在公共地方張貼有關親屬的個人資料以追收欠款。

結果
專員認為公開展示有關親屬的個人資料並不屬於資料的原本收集目的，因此違反了第3原則的規定。該財務公司作為資料使用者及主事人並不關心該追收欠款代理是否妥善處理有關個人資料。該財務公司沒有以合約或其他方式限制該追收欠款代理在追收欠款過程中披露有關親屬的個人資料。因此，專員認為該追收欠款代理的違反行為是在該財務公司授權追收欠款的範圍之內，憑藉條例第65(2)條，該財務公司須對違反第3原則的行為負上法律責任。

3.9 保障在外展促銷活動中所收集的個人資料

3.9.1 處理外展所收集的個人資料

銀行不時會舉辦外展促銷活動推廣其產品，例如信用卡服務。在過程中有時需要收集客戶的資料及身份證複本。由於這些活動是在銀行的辦事處以外進行，對於銀行作為資料使用者要履行第4原則中採取所有切實可行的步驟確保所收集資料的安全儲存及傳輸的責任，構成真正的挑戰。在這情況下，銀行應小心確保資料的安全。

在這方面，公署建議銀行為促銷職員就安全處理在外展所收集的資料制定及提供清晰的政策、程序及指引，這應包括確保下述事宜的措施：

(1) 在收集資料的過程中及之後，有關資料不會被不相關人士看見或查閱；

(2) 所收集的表格及文件(「**申請文件**」)必須妥善記錄，例如使用控制表；

(3) 申請文件應安全地存放於上鎖的文件箱，由指定人員看管；

(4) 儲存於便攜式電子儲存裝置內的資料應予以加密，以提供足夠的保障；

(5) 採取特定的預防措施，確保把申請文件安全傳送回儲存或處理有關文件的銀行；

(6) 禁止職員把申請文件攜帶回家；

(7) 委派指定人員監督申請文件的安全。

[14] 請參閱附註13。

3.9.2 個案研究－遺失申請文件[15]

投訴內容
一間銀行於星期六在一間書店進行促銷活動，招攬信用卡申請者。在活動結束後，銀行職員把所有申請表格連同申請者的身份證複本放進一個公事包帶回家，以便下個工作日再帶返辦公室。不幸地，該職員將該公事包遺留在一輛小巴上，因而遺失所有文件。

結果
調查顯示該銀行沒有就處理在外展促銷活動所收集的個人資料向職員提供足夠的指引。在考慮到所收集資料的敏感性及遺失資料可能對客戶造成的傷害，專員認為該銀行違反了第4原則的規定。

該銀行遵從專員的指示，實施相應的保安措施，包括在結束促銷活動後把申請文件傳送至附近的分行，而不是讓職員攜帶回家。

3.10 個人資料在電子銀行環境中的收集及保安

電子銀行服務對銀行有利，亦為客戶帶來方便，但同時互聯網環境本身亦有保安風險。在大多數情況下，電子銀行的運作涉及透過互聯網收集及傳輸個人資料，及儲存可經互聯網查閱的個人資料。在這方面，銀行應參考**《經互聯網收集及使用個人資料：給資料使用者的指引》**內有關經互聯網收集、展示及傳輸個人資料的詳細指引[16]。

下文重點指出銀行在電子銀行環境中就個人資料的收集及保安應注意的若干範疇。

3.10.1 經互聯網收集客戶的個人資料

當客戶登入銀行的電子銀行系統時，銀行應在收集其個人資料作交易指示前，按第1(3)原則的規定向客戶提供《收集個人資料聲明》。銀行可以清楚顯眼的方式在同一網頁或透過清晰的連結提供《收集個人資料聲明》。該聲明應易於閱讀和理解，其內容必須與印刷版本一致。

如客戶須在網上表格內提供其個人資料，該表格的設計應與印刷版(如有)一樣。特別是，必須填寫項目與非必要填寫項目應清楚註明。

如有使用cookies，良好的行事方式是明確述明cookies儲存甚麼種類的資料(不論是否涉及個人資料)。如銀行禁止不接受cookies的客戶使用其網站，應清楚告知客戶。如銀行容許客戶選擇不接受cookies而使用其網站，客戶應獲提供選擇及獲清楚告知拒絕cookies的後果(如有)。有關公署建議使用cookies的最佳行事方式，請參閱《經互聯網收集及使用個人資料：給資料使用者的指引》及專員發出的**《網上行為追蹤》**資料單張。

作為良好的行事方式，銀行亦應告知客戶應用於網上傳輸其個人資料的特定保安措施。公署亦建議銀行向客戶提供有關銀行的《私隱政策聲明》的連結，方便客戶查閱。

3.10.2 經互聯網傳輸或可查閱的客戶個人資料的保安

互聯網的保安具挑戰性，因此銀行需要特別小心保障經互聯網傳輸或可查閱的客戶個人資料。銀行應參閱《經互聯網收集及使用個人資料：給資料使用者的指引》，內載銀行為保障此等個人資料可採取的保安措施[17]。

3.10.3 個案研究－未獲授權而經電子銀行查閱其他客戶的帳戶資料

投訴內容
一名客戶登入一間銀行新提升的電子銀行系統後，發現可以查閱其他客戶的帳戶資料，包括帳戶號碼、帳戶餘額及所持股票的資訊。

結果
專員的調查顯示事件是因數據轉換問題、銀行資訊科技職員犯錯及系統在提升過程中測試失敗所致。該銀行因沒有在電子銀行環境中保障客戶的個人資料而違反了第4原則。其後，該銀行實施改善措施，防止違反行為再發生。

---

15 請閱覽專員的個案簡述第2003C07號。
16 請亦參考收錄於金管局《**監管政策手冊**》，標題為「**電子銀行的監管**」的章節(編號TM-E-1)內有關電子銀行風險管理的一般原則。
17 請亦參閱收錄於金管局《**監管政策手冊**》，標題為「**電子銀行的監管**」的章節(編號TM-E-1)。

3.11 處理客戶的查閱資料要求

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**》指引(「**查閱資料要求指引**」)向資料使用者提供妥善處理查閱資料要求及收取查閱資料要求費用的一般指引。此外,專員根據條例訂明的**查閱資料要求表格(表格OPS003)**所載的「致資料使用者的重要通告」,提供了處理查閱資料要求的解釋說明。銀行在處理客戶的查閱資料要求時,應參考上述文件。下文扼要介紹銀行應注意的要點。

3.11.1 客戶及有關人士可作出要求

個人可向資料使用者提出要求,要求獲告知該資料使用者是否持有其個人資料;及如有,獲提供有關資料的複本。這項要求通常稱為「查閱資料要求」,可以由個人自己提出或由「有關人士」代他提出。就查閱資料要求而言,「有關人士」除了上述第2.3.3段所述的人士外,亦包括獲該名個人以書面授權代表該名個人提出要求的人。

因此,一名客戶或其「有關人士」可向銀行作出查閱資料要求,例如索取其按揭帳戶紀錄內的個人資料複本。

3.11.2 40日內依從客戶的要求

除某些例外情況及條件另有規定外,條例第19(1)條規定銀行在收到客戶的查閱資料要求後的40個曆日內依從該要求,視乎情況,方法是以書面告知要求者它持有要求的資料並提供資料的複本,或是以書面告知要求者它並無持有有關資料。

3.11.3 依從要求的費用

根據條例第28條,銀行可為依從客戶的查閱資料要求而徵收不「超乎適度」的費用。該費用應只限於與依從查閱資料要求直接有關及必需的費用[18]。

一般來說,銀行可根據為依從查閱資料要求而尋找、提取及複印資料所涉及的直接勞動成本及必需開支(例如影印費及郵費)而收回有關成本。如銀行需要從資料複本中刪除該客戶以外的人士的姓名及其他身份辨識資料,銀行可收回相關工作的成本。但有關費用不應包括銀行為刪除獲查閱資料要求有關規定所豁免的個人資料而執行編輯工作所涉及的成本。同樣地,尋求法律意見的成本及辦公室經常性開支不應包括在查閱資料要求費用之內。

銀行對依從客戶的查閱資料要求實施劃一收費在行政上會較為方便,只要收取的費用是低於與依從查閱資料要求直接有關及必需的成本便可。因此,劃一收費的銀行應保持警覺,就某一特別個案(例如一個簡單直接的個案中,只是向要求者提供一頁紙的資料)所收取的費用不得超乎適度。

3.11.4 個案研究－未能在時限內提供所要求的資料

投訴內容

一名客戶向銀行提出查閱資料要求,索取八年間「[該銀行]就[他的帳戶]所持有的所有紀錄,但不包括戶口結單、交易確認書及成交單據」。該銀行以書面向該客戶澄清要求資料的範圍(「第一次澄清」)。該客戶回覆該銀行,澄清資料的範圍是「他簽署的所有合約或其他文件、[該銀行]與他之間的溝通的所有書面紀錄(包括對話及會議的檔案紀要)、[該銀行]就該帳戶擬備的所有風險概況、投資目標紀錄及其他內部備忘錄或檔案紀要」。該銀行不滿意,要求該客戶進一步澄清範圍(「第二次澄清」)但不果。該銀行其後向該客戶提供一些文件。由於該客戶認為仍欠缺某些他要求的資料,因此向專員作出投訴。

結果

在專員介入後,該銀行向該客戶提供第二批文件。該客戶滿意提供予他的兩批文件符合他的查閱資料要求。

[18] 請參閱查閱資料要求指引。

根據行政上訴委員會的裁決，如查閱資料要求涉及的資料種類及範圍明顯不清晰，必須作進一步澄清才能夠依從，則該查閱資料要求可被視為無效，而依從該查閱資料要求的時間會在澄清要求資料的種類及範圍後才開始計算[19]。

專員認為該客戶對第一次澄清的回覆足以澄清要求資料的範圍。該回覆足以清晰地讓該銀行找出所要求的資料，因此依從該查閱資料要求的法定40日時限是由該客戶就第一次澄清所作出的回覆當日開始計算（儘管該銀行尋求第二次澄清）。要求資料的範圍究竟是否過寬或不清晰致令該查閱資料要求無效，須客觀地決定，而不是只根據該銀行尋求進一步澄清的試圖。由於該銀行是在該客戶對第一次澄清作出回覆後大幅超過40日才向該客戶提供該兩批文件，該銀行沒有在時限內依從查閱資料要求，因而違反了條例第19(1)條。

3.12 私隱政策及實務在一般情況下可提供

3.12.1 制定《私隱政策聲明》

根據第5原則，銀行須採取所有切實可行的步驟，以確保其個人資料私隱政策及實務、其持有的個人資料的種類及資料的主要使用目的可讓公眾得知。做法可以是透過制定告示（通常稱為《私隱政策聲明》）及在一般情況下可提供該告示。

《私隱政策聲明》可包括下述資訊（如適用）：

(1) 政策的一般聲明，述明銀行在保障個人資料私隱方面，為向它提供資料的個人所作出的整體承諾。例如：「我們承諾完全符合，並且在可能的情況下超越國際認可的個人資料私隱保障水平，並嚴格遵守《個人資料（私隱）條例》的所有規定。為履行此承諾，我們會確保屬下職員依從本聲明所載列的政策及實務和保安及保密方面最嚴格的規定。」；

(2) 銀行所收集及持有的個人資料的種類；

(3) 每類資料的主要使用目的；

(4) 銀行為確保其持有的個人資料的準確所採取的措施；

(5) 個人資料的保留政策；

(6) 有關向第三者披露及轉移個人資料（不論是在香港境內或境外）之披露資料政策及實務，及可能的資料承轉人的類別；

(7) 有關直接促銷、外展促銷活動、電子銀行、追收欠款、外判個人資料的處理、集團內部共用個人資料、資料核對、監察僱員等的政策及實務；

(8) 銀行為確保其持有的個人資料的安全所採取的措施；

(9) 處理查閱資料要求及改正資料要求的政策及實務；

(10) 可向其查詢銀行的私隱政策及實務的聯絡人的詳情。

《私隱政策聲明》所載的私隱政策及實務應涵蓋銀行會收集及持有的所有個人資料，包括客戶、職員、代理、業務夥伴等的個人資料。

3.12.2 聲明可供公眾閱覽

根據第5原則，銀行須採取所有切實可行的步驟，以確保任何人（不論客戶或非客戶）可查閱其私隱政策及實務。銀行可在其網站主頁或其他收集個人資料的網頁透過連結張貼其《私隱政策聲明》，以供公眾查閱或下載。該連結應清晰地標明，例如「你的私隱」或「私隱政策聲明」。此外，銀行亦應準備印刷版本的《私隱政策聲明》，以供公眾在其總行或分行索閱。

[19] 請參閱行政上訴案件第17/2004及16/2008號。

4. 結語

涉及收集、持有、處理及使用大量客戶資料的銀行應設有機構性的私隱策略，應用於所有業務過程及營運程序。銀行由收集客戶的個人資料至最後棄置資料的整個過程中，妥善管理資料是十分重要的，並應小心顧及資料的完整性、使用、保安及查閱。建立及維持健全的私隱與風險管理系統需要最高管理層的支持和承諾。保障私隱的銀行可以得到客戶加倍信任和支持，從而締造客戶、銀行業務及整個銀行業的三贏局面。

香港個人資料私隱專員公署
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12樓
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk