妥善處理客戶個人資料：給保險業界的指引

內容

3.5 收集及使用個人資料作直接促銷
- 3.5.1 收集的方式合法及公平
- 3.5.2 不得改變資料的使用目的
- 3.5.3 個案研究 – 政府電話簿內的資料

3.6 保留客戶的個人資料
- 3.6.1 制定保留政策
- 3.6.2 個案研究 – 未能成功投保的申請人的資料
- 3.6.3 個案研究 – 前客戶的保險文件

3.7 使用客戶的資料作內部培訓
- 3.7.1 避免披露他人身份
- 3.7.2 個案研究 – 在培訓資料中披露保單持有人的身份

3.8 職員及代理查閱、儲存及處理客戶的個人資料
- 3.8.1 確保職員及代理具良好的操守、審慎的態度及足夠的辦事能力的措施
- 3.8.2 客戶個人資料的查閱及安全儲存的監控
- 3.8.3 安全傳輸載有個人資料的文件
- 3.8.4 保險代理或代表在家中或辦公地方以外工作
- 3.8.5 個案研究 – 客戶資料在互聯網上外洩

3.9 處理查閱資料要求
- 3.9.1 個案研究 – 醫療報告載有其他人士的資料
- 3.9.2 個案研究 – 不應就依從查閱資料要求收取超乎適度的費用
- 3.9.3 個案研究 – 法律專業特權

4. 結語

1. 引言

保險機構及保險從業員向公眾提供保險服務時，需處理大量的客戶個人資料。他們必須了解及依從《個人資料(私隱)條例》(下稱「**條例**」)就資料使用者處理個人資料的規定。

本指引旨在協助保險業界於進行保險活動時在處理客戶個人資料的收集、儲存、使用、保安及查閱資料要求方面依從條例的相關規定。

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的記錄資料(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。客戶個人資料的常見例子包括姓名、地址、電話號碼、身份證號碼、出生日期、職業、醫療記錄、財務資料、保單資料、索償資料等。

2.2 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基本規定。這些原則規管個人資料的收集、持有、處理及使用：

2.2.1 第 1 原則 – 收集個人資料的目的及方式

收集個人資料的目的必須與資料使用者的職能或活動有關；資料的收集對該目的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(第 1(1)原則)。收集方法必須合法及屬公平(第 1(2)原則)。資料使用者直接向資料當事人收集個人資料之時或之前，必須告知資料當事人：(a)他有責任抑或是可自願提供該資料；如屬有責任提供，不提供該資料的後果；(b)收集該資料的目的；(c)該資料可能轉移予甚麼類別的人；及(d) 他有權要求查閱及改正該資料，以及處理向有關資料使用者提出的該等要求的人的姓名(或職銜)及其地址(第 1(3)原則)。

實例：
保險機構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。如客戶須提供其個人資料，他們應獲提供一份《收集個人資料聲明》，清楚列明收集資料的目的、資料可能轉移予甚麼類別的人、不提供資料的後果，以

及查閱及改正資料的權利。《收集個人資料聲明》可夾附於收集個人資料的文件，例如保險申請表或索償表格。

2.2.2　第 2 原則 – 個人資料的準確性及保留期間

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準確(第2(1)原則)，及在達成資料的使用目的後，刪除該資料(第 2(2)原則)。資料使用者須採取合約規範方法或其他方法，以防止轉移予資料處理者[1]的個人資料的保存時間超過所需的時間(第 2(3)原則)。

此外，條例第 26 條規定資料使用者須採取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) 向客戶發出載有個人資料的文件前，確保客戶的地址正確無誤是十分重要的，否則有關資料可能會意外地披露予無關的第三者。
(2) 保險機構應制定政策及措施，指明保留客戶個人資料的期限。

2.2.3　第 3 原則 – 個人資料的使用

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。新目的是指以下目的以外的任何目的：– 在收集該資料時擬將該資料用於的目的；或與該目的有關的目的。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。這同意可由資料當事人以書面撤回。

實例：
在正常情況下，保險代理或代表不應向其他公司披露客戶的個人資料，以促銷有關公司的產品。他亦不應將客戶的資料用於與處理其保險帳戶無關的用途。在更改客戶資料的使用前，必須取得客戶的訂明同意。在這方面，保險機構應給予其職員、代表及代理適當的指導及培訓，並以適當的制裁措施執行有關規定。

[1] 例如 ： 獲保險機構聘請代為發出直接促銷信件的代理

2.2.4　第 4 原則 – 個人資料的保安

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、刪除或其他使用所影響(第 4(1)原則)。如資料使用者聘用資料處理者 (例如 ： 保險機構聘請代理代為刪除已不再使用的客戶資料)，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用(第 4(2)原則)。

實例：
載有個人資料的文件，例如保險申請表或保單，應受安全保管，避免未獲准許的人士查閱。儲存於電腦或便攜式儲存裝置的個人資料應以足夠的資訊科技保安措施及存取管控措施保護。

2.2.5　第 5 原則 – 資訊須在一般情況下可提供

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，以及資料的主要使用目的。

實例：
保險機構應制定並向客戶提供其《私隱政策聲明》，詳細列明所持有的個人資料的種類、每項個人資料的主要使用目的，以及其私隱政策和措施。《私隱政策聲明》可於公司網站或接待處的顯眼位置展示。

2.2.6　第 6 原則 – 查閱個人資料

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。資料使用者須於收到要求後 40 日內依從要求。條例第 18 至 25 條及第 27 至 29 條載列有關查閱資料要求及改正資料要求的詳細條文。

實例：
客戶可向保險機構提出要求，要求於 40 日內獲告知該機構是否在某保險申請表、醫療報告、風險評估問卷或索償表格中持有其個人資料，及獲提供有關資料的複本。

2.3 條例第 34 條 – 直接促銷

資料使用者首次使用個人資料於直接促銷目的時，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。如資料當事人拒絕服務，資料使用者必須停止如此使用該資料。

實例：
保險機構及保險從業員向客戶或潛在客戶作電話促銷時，須確保如此使用客戶的個人資料是與原本收集資料的目的相同或直接有關。他們亦須查核該些已在早前的電話促銷中表示拒絕服務的客戶的姓名，沒有留存在今次的致電名單之中。

保險機構及保險從業員於電話促銷時，客戶須獲告知其有拒絕服務的權利。對於行使拒絕服務權利的客戶，保險機構應把其姓名及電話號碼納入「拒絕服務名單」內，以便日後進行電話促銷前複查。

保險機構及保險從業員亦應留意《個人資料(私隱)條例》的相關修訂(將於 2013 年初生效)。根據修訂後條例的第 VIA 部，保險機構及保險從業員作出直接促銷前，須以口頭或書面通知客戶或潛在客戶，他們的個人資料會用於直接促銷及將會促銷的保險產品種類。保險機構及保險從業員未取得客戶或潛在客戶的同意前(包括表示不反對)不得使用他們的個人資料作直接促銷，或將這些個人資料提供予代理作直接促銷。不遵從有關規定則構成刑責(詳情請參閱條例第 VIA 部)。保險機構及保險從業員應不時參閱私隱專員就進行直接促銷活動發出的指引。

2.4 保險機構及保險從業員的法律責任

根據條例第 65(1)及(2)條，僱員或代理所作出的任何作為或所從事的任何行為，須視為亦是由他及其僱主或主事人所作出或從事的。因此，保險機構須為其職員、保險代理及代表在代其提供保險服務期間所作出的作為或所從事的行為負責。保險機構亦須為其承辦商或其他代理，例如資訊科技承辦商、市場推廣代理或理賠師在獲授權範圍內所作出的作為或所從事的行為負責。

此外，保險從業員就如資料使用者一樣，須對他們在以其身份處理客戶個人資料時的作為或行為負責，除非他們沒有為個人目的而持有、處理或使用該資料。

3. 實用建議

下文旨在協助保險從業員更了解條例在特定情況下的應用，以促進保險機構及保險從業員在處理個人資料方面能採取良好的行事方式去處理個人資料，及遵從條例的規定。

3.1 《收集個人資料聲明》

公署建議保險機構制定《收集個人資料聲明》，用以列明保障資料第 1(3)原則所訂明的資訊，並向客戶提供這份聲明。

3.1.1 《收集個人資料聲明》的內容

《收集個人資料聲明》應包含下述資訊：

(1) ***目的聲明：***這是關於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，使客戶可合理地確定其個人資料會被如何使用。

例子：
「從閣下收集的資料會用於處理閣下的保險申請、為閣下安排保險合約及管理閣下在本公司的帳戶。」

(2) ***承讓人聲明：***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讓人的類別。

例子：
「閣下在本保險申請中所提供的資料可能會轉移予：
(1) 風險評估機構，以進行客戶或反清洗黑錢的審查；
(2) 再保險機構，以承保閣下的申請或管理閣下的保單；
(3) 理賠師，以處理閣下就保單的索償。」

(3) ***自願或有責任提供資料：***除非情況明顯，否則保險機構應清楚告知客戶，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，但客戶沒有提供資料的後果。即使屬自願提供，亦建議列明不提供資料的後果。

例子：

(1) *「閣下在本保險申請表中提供的資料屬自願性質。不過，如閣下不提供資料，本公司可能因缺乏資料而無法評估閣下的申請。」*

(2) *「閣下必須填寫本索償表格 A 部的所有項目，以便本公司處理閣下的保險索償。如閣下不提供資料，本公司不會接受閣下的申請。」*

(4) ***查閱及改正資料的權利：***保險機構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要求的人士的姓名(或職銜)及地址。

例子：

「根據《個人資料(私隱)條例》，閣下有權就本公司持有閣下的個人資料提出查閱或改正資料要求。閣下可以書面向本公司的私隱循規主任提出有關要求，地址如下：…」

3.1.2 採取切實可行的步驟告知客戶

保障資料第 1(3)原則規定保險機構須採取所有切實可行的步驟，向客戶提供上述訂明的資訊。這些資訊可透過口頭或書面提供，但在可行的情況下，最好提供書面的《收集個人資料聲明》。方法可以是把《收集個人資料聲明》夾附於收集個人資料的表格，或在向客戶收集資料前，提供《收集個人資料聲明》予客戶。如保險機構是透過電話收集客戶的個人資料，就須在收集資料前向客戶提供《收集個人資料聲明》。保險機構可以口頭方式提供《收集個人資料聲明》，例如錄音訊息。在這情況中，良好的行事方式是隨後再補發書面的《收集個人資料聲明》。

保險機構可能在不同情況為不同目的而向客戶收集個人資料，例如在處理保險申請或保險索償。因此，保險機構應確保所使用的《收集個人資料聲明》適合用於該特定的情況。

為確保把《收集個人資料聲明》有效地告知客戶，公署建議保險機構：

(1) 留意《收集個人資料聲明》的設計(包括字體大小和行距，並適當地運用亮點)，確保一般擁有正常視力的客戶能易於細讀；

(2) 清晰地表達《收集個人資料聲明》，例如將它分開印刷為一份獨立通告或將它作為申請表格的一部分，其內容不應被埋藏在其他服務條款及細則之中；

(3) 使用易於理解的語言，例如選用簡單的字詞，及應避免使用行業術語及冗長難懂的句式；

(4) 提供服務台或電話查詢服務，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，根據條例第 35 條，保險機構如曾在 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》，便無需再向他提供同樣的《收集個人資料聲明》。

3.1.3 個案研究 – 印刷字體細小及承讓人類別含糊

投訴內容

一個服務供應商被控出售客戶的個人資料予一間保險機構作直接促銷用途。該服務供應商在有關收集及使用客戶個人資料的通知中表明，它可能會向對其「*有保密責任的任何人士*」轉移或披露個人資料。載列該通知的印刷字體較其他條款及細則所用的字體更為細小。

結果

鑑於該服務供應商的通知以細小字體印刷及沒有合理地清晰的字眼說明個人資料的承讓人類別，該服務供應商違反了保障資料第 1(3)原則的規定。

經調查該投訴後，該服務供應商承諾對違規行為作出補救，答應採用一般擁有正常視力的人士易於細讀的設計，及指明個人資料承轉人的類別，以便能合理地清晰說明個人資料可能轉移予甚麼人。

3.2 收集客戶的醫療資料

保險機構很多時在收到保險申請後或在處理保險索償時，會直接向客戶或第三者收集客戶的醫療資料。

3.2.1 收集的資料不超乎適度

保險機構在收集醫療資料之前，應先考慮將收集的各項資料是否必要。收集超乎適度的資料屬違反保障資料第 1(1)原則。例如，在索償人申索切除扁桃腺的醫療費用時，保險機構不需要收集索償人於 10 年前接受膝蓋手術的醫療資料，除非該保險機構能夠證明該資料與該索償相關。

3.2.2 收集的方式合法及公平

此外，保障資料第 1(2)原則規定，收集資料的方式必須是公平及合法的。公平是個廣闊的原則，要按各個案的特定情況而評估。一般來說，以欺詐或失實陳述的方式去取得資料不會被視為公平的方式。

3.3 收集身份證號碼及身份證副本

收集身份證號碼(及其他身份代號，例如護照號碼)及身份證副本是受保障資料第 1 原則及個人資料私隱專員(下稱「**私隱專員**」)發出的《身分證號碼及其他身分代號實務守則》(下稱「**守則**」)規管的。

3.3.1 身份證號碼

除非獲法律授權或是在守則第 2.3 段所載列准許的情況，否則資料使用者不得收集個人的身份證號碼(或其他身份代號)。守則第 2.3.3 段載列了與保險交易實際有關的情況。在該等情況下，資料使用者可以為下述目的而收集身份證號碼(或其他身份代號)，以正確識辨該名個人：為增進該人的利益，或為防止對資料使用者以外的其他人造成損害，或為避免對資料使用者造成損害或損失，而該損害或損失在有關情況下是超過輕微程度的。舉例來說，保險機構可能需要客戶或受益人的身份證號碼，以確保保險索償的償付款是給予正確的人士。

3.3.2 身份證副本

保險機構在收集身份證副本時必須依從守則第 3.2 段的規定。一般來說，保險機構不能收集身份證副本，除非有關收集是獲法律授權，或作為依從任何法定要求的證明。舉例來說，保險機構可能會收集人壽保險客戶的身份證副本，作為依從《打擊洗錢及恐怖分子資金籌集(金融機構)條例》附表 2 第 3 條的證明，該條規定保險機構在與客戶建立業務關係前，對客戶進行盡職審查時核實客戶的身份，或在該關係建立後，在合理地切實可行的範圍內盡快作出核實。

3.4 聘用私家偵探調查保險索償

3.4.1 就私家偵探的作為負上法律責任

保險機構或會聘用私家偵探調查可疑的索償個案。在這類的調查過程中，私家偵探或會使用各種監察或搜查方式，盡量收集有關個人的資料。私家偵探收集個人資料時必須遵從保障資料第 1 原則的規定，即收集的方式必須是合法及公平的，而且所收集的資料不得超乎適度。如私家偵探作出任何違規行為，依據條例第 65(2)條，聘用私家偵探的保險機構或須就有關行為負上法律責任。

3.4.2 收集的方式合法及公平

私家偵探收集個人資料的方式不得違反香港法律。例如，入侵電腦以取得索償人的資料，或盜竊載有個人資料的文件，可能會構成以不合法方式收集個人資料，甚至屬刑事罪行。

收集個人資料的方式亦必須屬公平，而方式是否公平，須視乎個案的所有情況。一般來說，以隱蔽方式去取得資料，不會被視為公平。不過，每宗個案的情況不同，有些特別情況或可有理據支持採用特別的方式去收集個人資料。舉例說，如保險機構合理地懷疑某客戶的人身傷害的保險索償有欺詐成份，而除了以人身監察的方式收集索償人的活動資料外，沒有其他實際可行方法可取得有關欺詐證據的話，以人身監察的方式收集資料或會被視為合理。如私隱專員收到投訴，會請該保險機構解釋及證明採用有關收集方式符合個案的特點。

3.4.3 資料屬足夠但不超乎適度

保險機構應確保私家偵探代其收集的資料屬足夠但不超乎適度。例如，在調查懷疑是虛假的人身傷害保險索償的過程中，不應收集與索償無關的索償人私生活資料。

3.4.4 私家偵探的監控

公署建議保險機構在聘用私家偵探調查可疑索償時，應採取措施防止私家偵探在調查過程中違反條例的規定。只依賴簡單協議，要求私家偵探遵守香港法律，包括條例，是不足夠的。保險機構應就私家偵探收集及處理個人資料

制定實務指引。保險機構亦應確保私家偵探以合法及公平方式代他們收集個人資料，及所收集的資料不超乎適度。

3.5 收集及使用個人資料作直接促銷

在此方面，公署建議保險機構及保險從業員參考由私隱專員發出的《收集及使用個人資料作直接促銷指引》(下稱「**直銷指引**」)及香港保險業聯會發出的(Code of Practice on Person-to-Person Marketing Calls)。此外，保險機構及保險從業員應留意條例經修訂後第 VIA 部有關收集及使用個人資料作直接促銷的新規定。現時的直銷指引將會於條例新增的第 VIA 部生效前再作出修訂。下述例子及個案研究說明一些應留意的地方。

3.5.1 收集的方式合法及公平

保險機構及保險從業員或會向潛在客戶收集個人資料，例如姓名及聯絡資料，以作促銷用途，但他們不得以不公平的方式收集該資料。例如：

(1) 保險從業員轉職至另一保險機構時，不可從前僱主的紀錄複印前客戶的保單或其他資料。
(2) 有些機構或政府部門會保存載有個人資料的登記冊或名冊，供公眾查閱，但查詢者須述明查閱的原因。如保險機構或保險從業員就查閱原因作出虛假陳述，從而獲得登記冊或名冊的個人資料作直接促銷，收集的方式會被視為不公平。

3.5.2 不得改變資料的使用目的

此外，保險機構及保險從業員須確保在促銷活動中所使用的個人資料的原本使用目的已包括直接促銷。否則須在事前就擬改變使用個人資料目的取得資料當事人的訂明同意。就上述第 3.5.1 段的例子(1)而言，將前客戶的個人資料用作促銷現職保險機構的產品或服務，不可能是該保險機構原本收集該前客戶的個人資料的目的。保險機構及保險從業員如需從公共登記冊或名冊摘錄個人資料，應確保該些個人資料的准許用途包括進行促銷。有關這方面的進一步資訊，請參閱公署於 2010 年 10 月發出的直銷指引第 II 部「從其他來源收集個人資料」的部份。

此外，請留意直銷指引的「在有疑問的情況下取得的同意」部份，及注意「綑綁式同意」(已在直銷指引中闡釋) 不可視作為客戶已接納改變其個人資料使用目的的訂明同意。

3.5.3　個案研究 – 政府電話簿的資料

投訴內容
投訴人是一名公務員，她不斷收到一間保險機構的保險經紀來電促銷保險產品，但投訴人之前已向該保險機構作出拒絕服務要求。致電者告訴投訴人，他們是從政府網站(www.directory.gov.hk)的政府電話簿中取得她的姓名及電話號碼。

結果
根據該網站展示的「*電話簿資料的使用限制*」，所提供的資料旨在方便市民與政府作公務上的通訊，而並非提供作任何的直銷活動。在這情況下，使用投訴人在電話簿中的資料作直接促銷有違保障資料第 3 原則的規定。該保險機構須為其保險經紀的違規行為負上法律責任。
此外，該保險機構沒有依從投訴人的拒絕服務要求，故違反了條例第 34 條的規定，亦須就此負上責任。

3.6 保留客戶的個人資料

3.6.1　制定保留政策

為了依從保障資料第 2(2)原則及條例第 26 條有關客戶個人資料的保留期限規定，保險機構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時的使用目的後被刪除。在決定保留期限時，保險機構應考慮資料的使用目的及相關的法定規定和適用的指引(例如《打擊洗錢及恐怖分子資金籌集(金融機構)條例》附表 2 第 20 條關於保留客戶記錄的規定)。

一般來說，保險機構可在與客戶結束業務關係後 (例如：客戶取消其保單)，保留客戶的個人資料不超過七年，以依從各項法律或規管對保留帳目或客戶記錄處理潛在訴訟等的要求。不過，不同類型的個人資料可有不同的保留期限，可以是少於或多於七年，須就不同情況而定。某些例外情況可能需要較短或較長的保留期限，例如：

(1) 為處理目前或即將進行的法律訴訟或索償；
(2) 為處理有關資料當事人或規管/執法機構目前的查詢或投訴；
(3) 方便對有關資料當事人履行合約責任；
(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，而銷毀證據會妨礙相關執法機構調查罪行；

(5) 為依從法律或法定責任，保留個人資料；
(6) 為依從相關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；
(7) 保險機構應留意，無限期地保留個人資料，會增加個人資料外洩及濫用的風險。如私隱專員接獲投訴，該保險機構便須解釋及證明為何當時仍須保留有關個人資料。

此外，為避免不必要地保留資料及減低資料外洩和濫用的風險，保險機構應就其保險代理或代表保留客戶個人資料而制定政策及措施。在制定政策及措施時，應考慮代理或代表保留及使用該資料的目的。

有關保險機構及從業員應如何永久刪除個人資料及將個人資料匿名化至不能再識別相關人士，可參閱由私隱專員發出的《個人資料的刪除與匿名化指引》。

3.6.2 個案研究 – 未能成功投保的申請人的資料

投訴內容
一名未能成功投保的申請人，向私隱專員投訴一間保險機構在拒絕其申請後，仍保留其申請資料。

結果
該保險機構一貫的做法是無限期地保留未能成功投保的申請人的個人資料。根據該保險機構所述，無限期地保留資料的原因是為了：(i)依從不同法律就保存帳目的規定；(ii)依從規管機構的指引及通告；(iii)處理潛在的訴訟、查詢及投訴；以及(iv)檢查日後同一申請人的申請資料的完整性及準確性。

至於未能成功投保的申請，通常有兩種情況：第一種涉及金錢交易(例如在申請時已繳交保費)，而第二種不涉及金錢交易。於第一種情況下，在有關條例規定的法定期間內保存帳目有關的資料是合理的。不過，如沒有涉及金錢交易，該保險機構便不能純粹因為申請人日後可能再投保，而無限期保留其個人資料。如是為處理日後的查詢、投訴或法律行動的目的，應設定合理的保留期。

如未能成功投保的申請涉及金錢交易，保留有關個人資料的期限應不超過七年。至於沒有涉及金錢交易的申請，兩年的保留期限一般已足以履行該保險機構所述的各項目的。

公署向該保險機構送達執行通知，要求它刪除保留超過上述期限的個人資料(除非出現特殊情況需要較長的保留期限)。該保險機構遵從執行通知的規定並刪除超過 7,000 個記錄。

3.6.3 個案研究 – 前客戶的保險文件

案情
一名保險代理人在受聘於不同保險機構期間收集了大量有關客戶資料的文件副本。他後來破產及喪失其保險代理人牌照。但他仍然保留該些文件副本。某天，他在其住宅的梯間棄置三箱載有超過二千名人士的個人資料的文件副本。一名鄰居報警求助，該些文件副本被警方檢走。

結果
經過調查後，該保險代理人被控違反條例第 26 條的規定。該代理人承認控罪，被判罰款。

3.7 使用客戶的資料作內部培訓

3.7.1 避免披露他人身份

保險業務無可避免經常涉及收集及使用客戶的敏感個人資料。保險機構及保險從業員有責任小心謹慎地處理客戶的資料。保障資料第 3 原則規定，客戶的個人資料只可用於原本的收集目的或與之直接有關的目的。保險機構應避免在職員或保險代理或代表之間共用客戶的個人資料，除非是有需要為有關客戶提供保險服務，並且是按「有需要知道」和「有需要使用」的基礎而作出。

保險機構向職員及保險代理及代表提供培訓時，以真實個案中的保單資料作解說，是常見的做法。但保險機構及培訓導師不應分享可以識別客戶或受益人身份的資料。該等人士的身份在大多數情況下與培訓目的無關。與保險代理或與保單無關的人士分享客戶或受益人的資料，屬侵犯私隱的行為。因此，保險機構及培訓導師在培訓時，應使用虛構的個人資料和情節。

3.7.2 個案研究 – 在培訓資料中披露保單持有人的身份

投訴內容
一間保險機構的區域總監在中國內地舉行培訓時，使用投訴人、其子女及前夫的保單作培訓材料，因而向出席培訓的 55 名保險代理披露他們的個人

資料。投訴人是該保險機構的前區域經理，為該區域總監的前下屬。該保險機構終止了投訴人的代理合約，聲稱的理由是投訴人不恰當地向與她有關的人士，包括其子女及前夫開出保單。

結果

該保險機構解釋，在培訓中使用有關保單資料是說明投訴人的不道德手法。該保險機構辯稱有需要指出有關人士是受訓者所認識的，令受訓者提高警覺及起阻嚇作用。

收集有關個人資料的目的明顯是向客戶提供保險服務。使用客戶提供作保險用途的個人資料作培訓之用，或向其他無關的保險代理披露該些資料，已超出了客戶的合理期望。為提高意識而在培訓中披露投訴人或其他客戶的身份資料，是不必要的。實際上，該保險機構只提述有關人士的職位或職責便已足夠。

因此，該區域總監作為該保險機構的代理，在培訓中披露個人資料，令該保險機構違反保障資料第 3 原則的規定。

3.8 職員及代理查閱、儲存及處理客戶的個人資料

就依從保障資料第 4 原則方面，保險機構應就其職員及代理持有的客戶個人資料，採取保安的預防措施。保險機構應因應資料的敏感程度及若出現保安違規時可能造成的傷害的嚴重性，而採取不同程度的保安措施。一般來說，保險機構可採取由上而下的方式，就着其本身及其職員及代理所持有的個人資料，制定保安管理措施、政策、準則及程序。此等措施可確保所持有的個人資料的保密性及完整性，以及維持查閱及使用該等個人資料的問責性。相關的保安措施應包括以下所述。

3.8.1 確保職員及代理具有良好的操守、審慎的態度及足夠的辦事能力的措施

職員及保險代理及代表

保險機構應採取合理地切實可行的措施，確保處理客戶個人資料的職員及保險代理及代表(統稱「**有關職員**」)，得到有關個人資料處理及保障的培訓、謹慎應用保險機構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。在制定及落實有關保障客戶個人資料的政策及內部程序時，保險機構應留意下述事宜：

(1) 定期及有系統地傳遞有關政策予有關職員；
(2) 持續向有關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份；
(4) 定期檢討及更新有關政策、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) 有關職員須簽署保密聲明，該聲明清楚述明保險機構在這方面的工作期望；
(7) 如發生保安違規事件，應採取適當的調查程序，並對違規的有關職員採取適當的行動；
(8) 作出隨機檢查，以確保職員遵從既定的政策及措施。

外判承辦商

如保險機構委託第三者，例如資訊科技承辦商及廢物處置承辦商，以處理客戶個人資料，應確保資料在處理及刪除過程中受到保障，及防止資料被用作進一步或其他用途。保險機構應考慮採取下述預防措施，以保障個人資料及以合約或其他方式以確保承辦商安全地處理及刪除資料：
(1) 揀選信譽良好及有能力保障個人資料的承辦商；
(2) 在承辦商的服務合約中加入下列要求：
    (a) 列明承辦商須採取的保安措施，以保障所收集、閱覽或使用的個人資料；
    (b) 承辦商不得使用或披露個人資料予合約沒有指明的目的上；
    (c) 列名保險機構及承辦商須依從保障資料原則的責任；
    (d) 承辦商在完成使用個人資料作其受聘提供服務的目的時，須適時交還及在其系統中刪除資料及任何備份；
    (e) 即時報告與個人資料有關的任何不尋常徵兆或保安違規情況；
    (f) 承辦商應保證其職員已接受適當的如何處理個人資料的培訓；
    (g) 如分判工作涉及處理或使用個人資料，承辦商在沒有保險機構的明確同意下，不得分判工作；
    (h) 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承辦商，除非承辦商必須得到該等資訊才可完成工作；
(4) 不應為系統測試而把載有個人資料的資訊發放予承辦商；
(5) 應妥善地標籤交予承辦商並載有個人資料的資訊；
(6) 應不時對承辦商作出審查，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；
(7) 應不時對承辦商作出審查，以確定他們有否對其負責處理個人資料的職

員進行適當的核查；
(8) 應對交給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；
(9) 應就交予承辦商的個人資料的使用、傳送、儲存及銷毀向承辦商發出清晰的指示。

公署建議保險機構及保險從業員就這方面參考由私隱專員發出的《外判個人資料的處理予資料處理者》的資料單張，以了解聘用資料處理者時所必須注意的事項。

3.8.2 客戶個人資料的查閱及安全儲存的監控

由於有關職員會接觸到客戶的個人資料，保險機構應採取適當措施，以確保資料免受未經准許或意外的查閱、處理或刪除。此等措施的例子包括：

(1) 只有獲授權的職員或保險代理或代表在有需要知道的情況下，才獲准查閱客戶的個人資料。
(2) 客戶資料庫的查閱，須受到保安技術如密碼的保護。
(3) 所有從資料庫複製資料/備份及輸出影像的活動，應在獲授權及監察下，並須記錄相關的理由才可進行。另外，應定期印製及檢討這些資料庫的運作報告。
(4) 每當資料庫被查閱時，資料庫應發出顯眼的警告通知；而除非有關用戶獲正式批准，否則不應從資料庫輸出或在資料庫儲存任何個人資料。
(5) 如使用便攜式儲存裝置(例如手提電腦、USB 記憶體)，應確保只儲存必需的資料，並把資料加密及在使用後刪除。
(6) 確保載有個人資料的文件不會被隨意棄置。銷毀有關文件時，可使用碎紙機。如電腦內的個人資料不會再使用，應徹底地刪除該資料。
(7) 如個人資料是以電子方式儲存，應確保個人資料得到足夠的資訊科技保安措施保護。

3.8.3 安全傳輸載有個人資料的文件

保險機構及保險從業員在傳送載有客戶個人資料的文件時，應確保資料受到保護，免受不相關的人士的未經准許或意外的查閱。例如：

(1) 以郵遞或專人傳送 – 應使用密封式的信封；敏感資料(例如身份證號碼)不能透過信封窗口查看得到；及如文件只限收件人拆閱，信封面應註明「私人及機密」；

(2) 以傳真傳送 – 如可能的話，應以專用傳真機接收文件；在發出傳真前，應通知收件人；及在傳送前檢查傳真號碼是否正確；
(3) 以電子方式傳送 – 把文件加密、使用「機密郵箱」及/或查閱密碼。

3.8.4 保險代理或代表在家中或辦公地方以外工作

保險代理及代表經常會將載有客戶個人資料的文件或保單帶離辦公室，以便在家中或其他地方工作。在此情況下，他們必須採取措施保護資料，以免資料遺失或被第三者在未獲授權下查閱。在公眾地方與客戶會面時，保險代理及代表應確保文件(如保險申請表及保單)中的個人資料不會被不相關的人士查閱，而有關客戶敏感資料的對話，亦不會被不相關的人士聽到。

保險機構應就在辦公地方以外處理客戶資料方面，向有關職員提供清晰的政策及指引，包括：

(1) 只有在指定情況下，才可將與工作所需的資料帶離工作地方；
(2) 如有關職員須使用其個人電腦，其電腦應具有足夠的保安措施，例如，應安裝最新的反惡意軟件及不可安裝檔案分享軟件，如 Foxy；
(3) 將儲存於手提電腦及其他便攜式儲存裝置的個人資料加密，以確保在保安方面有足夠的保障；及
(4) 在工作完成後，穩妥地刪除資料。

在決定是否讓有關職員把客戶的個人資料帶離工作地方時，應考慮下述因素：

(1) 是否有真正、合理或急切需要，將資料帶離工作地方；
(2) 為何在辦公地方處理資料並非合理地切實可行；及
(3) 資料的敏感程度及資料一旦外洩可能造成的傷害的嚴重性。

有關使用便攜式儲存裝置的個人資料保障，可參閱由私隱專員發出的《使用便攜式儲存裝置指引》。

3.8.5 個案研究 – 客戶資料在互聯網上外洩

事件
一個載有某保險機構約 600 名客戶的個人資料(包括姓名、出生日期、地址、電話號碼及保單詳情)的資料庫洩漏資料，致使公眾可以透過互聯網進入該資料庫。

結果

公署的調查顯示，是次個人資料洩漏事件主要是該保險機構不恰當地向其保險代理人，批予查閱該資料的權限。該名保險代理人把有關個人資料上載並儲存於家中一個網頁檔案伺服器內，最後導致任何人皆可以透過互聯網搜尋器查閱有關資料。

該保險機構向保險代理人發出的指引及採取的監控措施，明顯不足以防止客戶的個人資料不受未獲准許的查閱、轉移、儲存及在公司以外地方被處理，導致發生是次事件。最後，該保險機構因沒有採取足夠的措施保障該等資料而被裁定違反保障資料第 4 原則的規定。

公署向該保險機構發出了執行通知。該保險機構依從通知的規定，實施相應的補救措施，包括檢討其運作程序及就客戶個人資料的查閱、轉移及保安加強監控，尤其是加強管控在公司以外的地方處理客戶個人資料的情況。

3.9 處理查閱資料要求

個人可向保險機構提出獲告知該機構是否持有其個人資料的要求；如有的話，可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。「有關人士」是指：

(1) 獲該名個人以書面授權代表該名個人提出要求的人；
(2) 如該名個人是 18 歲以下，則指對其有父母親責任的人，例如父或母；
(3) 如該名個人是無能力處理本身的事務，則指獲法庭委託管理該等事務的人；
(4) 如該名個人是精神上無行為能力，則指其受託監護人、或獲授予其監護權的社會福利署署長或其他人士或根據《精神健康條例》履行受託監護人職能的人。

公署建議保險機構及保險從業員參考私隱專員不時就處理查閱及改正資料要求而發出的指引。私隱專員根據條例訂明的查閱資料要求表格(表格 OPS003)所載的「致查閱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。下述個案研究顯示保險機構及保險從業員應注意的一些範疇。

3.9.1 個案研究 – 醫療報告載有其他人士的資料

一名客戶向一間保險機構提出查閱資料要求，索取投保前的驗身報告副本。該保險機構表示不會向該客戶提供報告，因為該報告載有負責檢驗的醫生的個人資料。

一般來說，保險機構不能以投保前的驗身報告載有其他人的個人資料為由，而拒絕依從客戶索取報告內其個人資料的副本的查閱資料要求。該保險機構在向客戶提供資料的副本前，可刪除或遮蓋其他人的姓名及身份識別資料。

3.9.2 個案研究 – 不應就依從查閱資料要求收取超乎適度的費用

一名客戶向其保險經紀提出查閱資料要求，索取投保前按保險機構要求而驗身的「化驗報告」副本。有關檢查的醫療費用是由該保險機構支付的。該經紀告訴客戶，該保險機構會就提供報告副本而向他收取 464 港元，作為償還該保險機構所支付的醫療費用。

在依從客戶索取醫療報告(由保險機構支付費用)副本的查閱資料要求方面，該保險機構不可向客戶收取醫療費用。不過，該保險機構可收取不超乎適度的費用。有關費用只可涵蓋與依從該要求直接有關及必需的成本，此可以包括尋找、取出及複製所需資料的人工成本及實付費用，例如影印費及郵費。

3.9.3 個案研究 – 法律專業特權

一名僱員向僱主提出工傷索償。其僱主的保險機構聘請的理賠師要求他進行身體檢查。該僱員其後向該保險機構提出查閱資料要求，索取身體檢查的醫療報告的副本。該保險機構沒有回應該僱員的要求，因為他們認為，有關報告受法律專業特權保護，他們可以拒絕給予該僱員。

雖然根據條例，法律專業特權可以是拒絕依從查閱資料要求的理據，但該保險機構應根據條例第 21 條的規定，於收到要求後 40 日內，以書面通知該僱員他們不會依從該要求，及拒絕的原因。

4. 結語

公署希望本指引能重點指出有關處理客戶個人資料私隱的問題，及協助保險機構及從業員檢討其目前的個人資料系統及採取良好的行事方式。良好的私隱政策及措施有助建立客戶的信任及信心，對保險機構的業務及整個保險業界均有裨益。

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