視察報告

（根據香港法例第486章《個人資料（私隱）條例》第 **48(1)**條發表）

香港某地產代理公司的

個人資料系統

報告編號： R17-2201

發表日期： 2017 年 12 月 18 日

本頁面乃故意留空以便雙面打印

香港某地產代理公司的個人資料系統視察報告

香港個人資料私隱專員根據香港法例第 486 章《個人資料（私隱）條例》第 36 及 48 條行使賦權對香港某地產代理公司的個人資料系統的視察發表報告。

條例**第 36 條**規定：

「*在不損害第38條的概括性原則下，專員可對 —*

(a) 資料使用者所使用的任何個人資料系統；或

(b) 屬於某資料使用者類別的資料使用者所使用的任何個人資料系統，

進行視察，目的在確定資訊以協助專員 —

(i) 在 —

(A) (a)段適用時，向有關的資料使用者；

(B) (b)段適用時，向有關的資料使用者所屬於的一個類別的資料使用者，

作出建議；及

(ii) 作出關於促進有關的資料使用者或有關的資料使用者所屬於的一個類別的資料使用者（視屬何情況而定）遵守本條例的條文（尤其是各保障資料原則）的建議。」

根據條例**第2(1)條**，「**個人資料系統**」是指「*全部或部分由資料使用者用作收集、持有、處理或使用個人資料的任何系統（不論該系統是否自動化的），並包括組成該系統一部分的任何文件及設備。*」

條例**第48條**的有關部分規定：

「*(1) 在符合第(3)款的規定下，專員在第36(b)條適用的情況下完成一項視察後，可 —*

(a) 發表列明由該項視察引致的、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）的任何建議的報告；及

(b)　以他認為合適的方式發表該報告。

…

(3) 除第(4)款另有規定外，根據第(1)款…發表的報告的擬訂形式，須以防止可從報告中確定任何個人的身分為準。

(4) 第(3)款不適用於屬以下人士的個人 —

(a) 專員或訂明人員；

(b) 有關資料使用者。」

香港個人資料私隱專員　黃繼兒

2017 年 12 月 18 日

視察報告
（根據香港法例第 486 章《個人資料（私隱）條例》第 48(1)條發表）

香港某地產代理公司的個人資料系統

摘要

背景

1. 為提升業界對保障個人資料的意識，香港個人資料私隱專員（「**專員**」）於 2008 年與地產代理監管局舉辦了一項聯合活動[1]，其後更合作出版一本小冊子[2]，旨在加深地產代理業界對保障客戶個人資料的實務知識。

2. 專員知悉香港樓價及整體的住宅樓宇買賣仍然持續活躍，認為現時審視地產代理業界在保障個人資料私隱這個範疇中的運作，符合公眾利益。因此，專員根據香港法例第 486 章《個人資料（私隱）條例》（「**條例**」）第 36 條對一間在市場具領導地位的地產代理公司（「**該地產代理公司**」）的個人資料系統進行視察（「**本視察**」）。

3. 為了解該地產代理公司在個人資料保障方面的強弱之處，本視察檢視了其個人資料系統中處理個人資料的整個流程，亦同時審閱了它的相關私隱政策。專員期望在本視察中所得出的視察結果及建議，亦可作為業界的參考標準，協助他們遵從條例及條例附表 1 的保障資料原則的規定。

[1] 地產代理業保障私隱活動

[2]《地產代理妥善處理客戶個人資料》，2009 年 5 月出版

視察結果及建議

4. 若要有效保障個人資料，機構不可只視有關政策為法律循規的事宜，而是應由董事會做起，將個人資料保障視為機構的管治責任，並將之納入處理業務中不可或缺的一環。

5. 專員注意到地產代理須根據香港法例第 511C 章《地產代理常規(一般責任及香港住宅物業)規例》（「**地產代理常規規例**」）收集顧客的個人資料。本視察結果顯示該地產代理公司已採取合理措施致力確保顧客的資料得到妥善管理。專員尤其滿意該地產代理公司最高管理層支持並承諾保障個人資料私隱，委任高級行政人員監察其個人資料系統的合規情況。在技術層面方面，專員欣賞該地產代理公司審慎地分割及監控其資料庫系統的權限，並按「有需要知道」的原則設置使用權限，以減少未獲授權查閱或洩露顧客個人資料的風險。

6. 在實際營運上，負責任的機構應建立及維持全面的私隱管理系統[3]；在機構中貫徹執行私隱管理，以涵蓋整體業務常規、操作程序、產品和服務設計、實體建築，以至網絡基礎設施。在策略層面，機構可採用私隱管理系統作為框架，輔以恒之有效的檢討及監察程序，建立健全的私隱保障基建，藉以配合機構遵從條例的規定。

7. 完成本視察後，專員注意到該地產代理公司已嘗試按其業務性質及運作模式致力私隱管理。公署未有發現該地產代理公司在保障個人資料私隱方面有嚴重缺失，但仍有改善空間。專員了解地產代理業界的日常操作及處理顧客個人資料的流程，並十分鼓勵地產代理建立自己的私隱管理系統。系統的建立不但能有效管理顧客的個人資料，更能有助機構遵從條例的規定、建立顧客的信任，並提升機構的名聲及商譽。專員參照一個全面的私隱管理系統的要求，認為地產代理業界在個人資料保障方面仍有改善的空間並作出下述主要的建議。以下的建議應可作為所有地產代理公司的指引或良好行事方式：

[3] 專員於 2014 年 2 月出版了一份《私隱管理系統：最佳行事方式指引》，扼述如何建立專員所提倡的健全私隱管理系統。

(1) *管理層的承諾及管治架構*

該地產代理公司最高管理層對保障個人資料私隱的承諾值得欣賞，其將個人資料私隱保障納入企業管治的做法是業界的模範。企業應從最高管理層中委任保障資料主任，以管理私隱管理系統及資料保障相關事務。

(2) *全面的私隱政策*

地產代理公司應制定全面的私隱政策，將保障個人資料納入機構內每個重要的操作環節，並定期檢討及更新有關政策。

政策應包括以下範疇：

(i) 個別地產代理收集最少的個人資料的方式；
(ii) 載有個人資料的文件及記錄的保存期限；
(iii) 個人資料的銷毀程序；
(iv) 保障載有個人資料的文件及記錄的行政措施及資訊科技保安的標準和要求；及
(v) 處理直接促銷活動及拒收訊息的要求及操作程序。

(3) *監控及持續的評核*

地產代理公司應建立定期及全面性的合規審核機制，並進行持續評核，以確保員工遵從有關的私隱政策。

(4) *資料外洩事故通報機制*

資料外洩事故通報機制是其中一項有效監控資料使用者遵從私隱管理系統的工具。地產代理公司應制定通報資料外洩事故的機制及指引，訂明處理及通報此等事故的流程。

(5) *處理賣方及買方的個人資料的方式*

若機構不能掌控個人資料，其個人資料系統永遠不能有成效及有效率地運作，不恰當地使用或洩露個人資料的風險便可能出現。地產代理公司應提供適當指引，要求個別地產代理應向公司提供他們所收集或處理的所有賣方及買方的個人資料。

(6) *技術層面的管治*

機構倚重資訊科技系統處理業務成交及保存有關記錄和資料庫。因此，保持資訊科技系統的健康運作以避免系統受網絡攻擊，與其他實體保安措施同樣重要。地產代理公司應指派高層管理人員負責監督資訊科技保安範疇，根據業務定位制定其具體的資訊科技保安政策。

(7) *培訓及教育*

若機構內沒有尊重私隱的文化，保障資料私隱的政策亦不會有成效及有效率地被施行。地產代理公司應採取積極主動的方式，促進員工遵守個人資料保障原則，並通過定期舉辦相關培訓及課堂培養員工之間尊重資料私隱的文化。

簡介

視察原因

1.1　有報導指，儘管政府近年推行了額外印花稅政策及新一輪的樓宇按揭貸款措施，但香港樓價仍然持續活躍， 整體的住宅樓宇買賣合約由2016 年的 55,000 宗上升至 2017 年的 65,000 宗[4]。

1.2　根據地產代理常規規例，任何人擬透過地產代理買賣或租賃物業，必須填寫訂明表格及向地產代理提供其姓名、聯絡資料及香港身份證（「**身份證**」）號碼。香港現時約有 37,000 個由個人持有的地產代理牌照[5]。

1.3　鑑於地產代理處理的個人資料數量龐大，種類繁多（包括敏感的個人資料），專員認為根據條例第 36 條對地產代理公司的個人資料系統進行視察，符合公眾利益。

[4] 資料來源：http://www.rvd.gov.hk/tc/property_market_statistics/index.html
[5] 資料來源：https://www.eaa.org.hk/zh-hk/Information-Centre/Key-Figures/Licensee-Population

視察

地產代理公司的業務

2.1　公署挑選了該地產代理公司作為視察對象，以協助專員對這個類別的資料使用者就收集、持有、處理及使用個人資料方面作出建議，藉以加強他們依從條例規定的認知。

2.2　該地產代理公司與一般的地產代理公司無異，同樣透過其分行及網站向顧客提供買賣及租賃住宅物業及車位等的地產代理服務，當中物業的買賣為該地產代理公司的核心業務。

視察的範圍

2.3　視察小組檢視了該地產代理公司從收集至銷毀顧客個人資料的整個流程，以了解他們在保障個人資料方面的強弱之處，並挑選了住宅物業買賣及租賃的個人資料流程作仔細分析，從而提出建議，以協助地產代理公司遵從條例附表 1 的保障資料第 1 至 6 原則的規定。

2.4　保障資料第 1 至 6 原則涵蓋個人資料的收集、準確性、保留期間、使用、保安、公開政策及查閱等方面。本視察亦就該地產代理公司在直接促銷活動中使用顧客的個人資料方面，檢視其依從條例第 6A 部相關條文的情況。

2.5　該 6 項保障資料原則及條例第 35B 至 35H 條有關在直接促銷中使用個人資料的條文分別載列於附件 1 及 2，以供參考。

視察的方法

2.6　本視察包括 5 項主要檢視工作：

神秘到訪

2.7　視察小組曾以神秘顧客的形式到訪該地產代理公司的分行，以全面了解個別地產代理的工作流程及表現，尤其是他們在日常工作中處理個人資料的方式。

審閱政策

2.8　一份詳細而全面的處理個人資料政策可確保員工的行事方式穩妥及一致。視察小組審閱了該地產代理公司就保障個人資料私隱制定的相關政策、指引、通告、表格和培訓資料。

現場視察

2.9　視察小組現場視察了該地產代理公司的總部、經揀選的分行、數據中心及一個貨倉。透過現場視察，視察小組可（i）親身檢視該地產代理公司收集、處理及儲存顧客個人資料的場所及保安措施；（ii）視察用作收集、處理及儲存顧客個人資料的設備和系統；及（iii）檢視場所和電腦系統內儲存的紙張記錄及電子記錄。

示範

2.10　在現場視察期間，該地產代理公司向視察小組示範了處理買賣物業、更新拒收直銷訊息名單、顧客查詢等程序，讓視察小組了解該地產代理公司向顧客收集個人資料的類別及如何收集和使用該些資料。

面談及查詢

2.11　視察小組曾分別在進行本視察之前、過程中及之後，向該地產代理公司作口頭及書面查詢。視察小組透過面談向該地產代理公司總部及分行的職員，包括管理層及前線職員，作出口頭查詢，以了解他們處理個人資料的情況、對有關個人資料私隱的內部政策及指引的熟悉程度，以及他們所提供和接受的培訓資訊。

2.12　視察小組透過向該地產代理公司作出書面查詢，了解他們的個人資料系統的運作，把所取得的書面證明與現場視察所得的資料作出核對，及識別當中需要關注的事項。

個人資料系統及資料流程

個人資料系統

3.1　本視察中審視的個人資料系統不但涵蓋用作處理個人資料的自動化系統，並包括不同部門及相關員工在收集、持有、處理或使用顧客個人資料的系統運作。

3.2　該地產代理公司會透過資料庫系統、總部和分行員工，以及文件棄置承辦商處理顧客的個人資料。

3.3　該地產代理公司的個人資料系統內所涉及顧客的個人資料種類載列如下：

個人資料種類	**例子**
姓名及身份代號	● 姓名 ● 身份證或護照號碼 ● 身份證或護照副本
聯絡資料	● 通訊地址 ● 聯絡電話號碼 ● 電郵地址 ● 傳真號碼
財務資料	● 信用卡號碼 ● 支票號碼
錄音／錄影	● 電話談話的錄音記錄 ● 分行的閉路電視錄影記錄

顧客的個人資料流程概覽

3.4　明顯地，地產代理公司所持有的個人資料大部分是來自買賣或租賃住宅物業的顧客。本報告的「賣方」指擬出售／出租住宅物業的顧客。「買方」指擬購買／承租住宅物業的顧客。

收集個人資料

3.5　顧客的個人資料流程始於個人資料的收集，收集個人資料的途徑包括透過其分行、電話及網站，個別地產代理亦會親身收取顧客的身份證號碼及／或其副本、通訊地址及財務資料。

(i)　分行

買方和賣方的個人資料紙張記錄

3.6　地產代理常規規例[6]規定地產代理為賣方出售／出租物業而作廣告宣傳前或為買方安排視察住宅物業前，必須與對方簽訂地產代理協議。因此，當顧客擬透過分行買賣或租賃住宅物業時，須在「出售／購買香港住宅物業用的地產代理協議」或「出租／承租香港住宅物業用的地產代理協議」（統稱「**訂明表格**」）填寫其姓名、聯絡資料及身份證號碼並簽署。

3.7　為避免賣方在身份方面作出欺詐成分的失實陳述，該地產代理公司亦會向賣方收集其身份證副本[7]，以確保賣方在住宅物業的臨時買賣合約上的姓名與業主的姓名相同。

---

[6] 第 6 條

[7] 第 13(3)條

賣方的個人資料電子記錄

3.8　地產代理在收到賣方已簽署的訂明表格後，會將賣方的姓名、聯絡資料及出售指示（例如物業的售價）輸入該地產代理公司的資料庫系統內。

買方的個人資料電子記錄

3.9　與賣方的記錄不同，個別地產代理視買方的個人資料，包括聯絡資料及購買偏好（例如物業座落的區域）是其重要資產。視察小組得悉大部分個別地產代理並不會把買方的個人資料輸入該地產代理公司的資料庫系統內，以避免其他地產代理查閱有關資料。

(ii)　透過電話

3.10　顧客如有意買賣或租賃住宅物業，可致電分行或個別地產代理並提供其姓名及聯絡資料。不過，顧客仍須先到分行簽署訂明表格，地產代理方可以為物業作廣告宣傳或為顧客安排視察物業。

(iii)　透過網站

3.11　與經由電話收集個人資料的情況類似，顧客可透過網站提供其姓名及聯絡資料以表示他有意買賣或租賃住宅物業。當顧客在網上提供其個人資料作出預約後，相關的地產代理便會收到訊息提示，並會聯絡顧客及邀請他們到分行填寫及簽署訂明表格。

使用個人資料

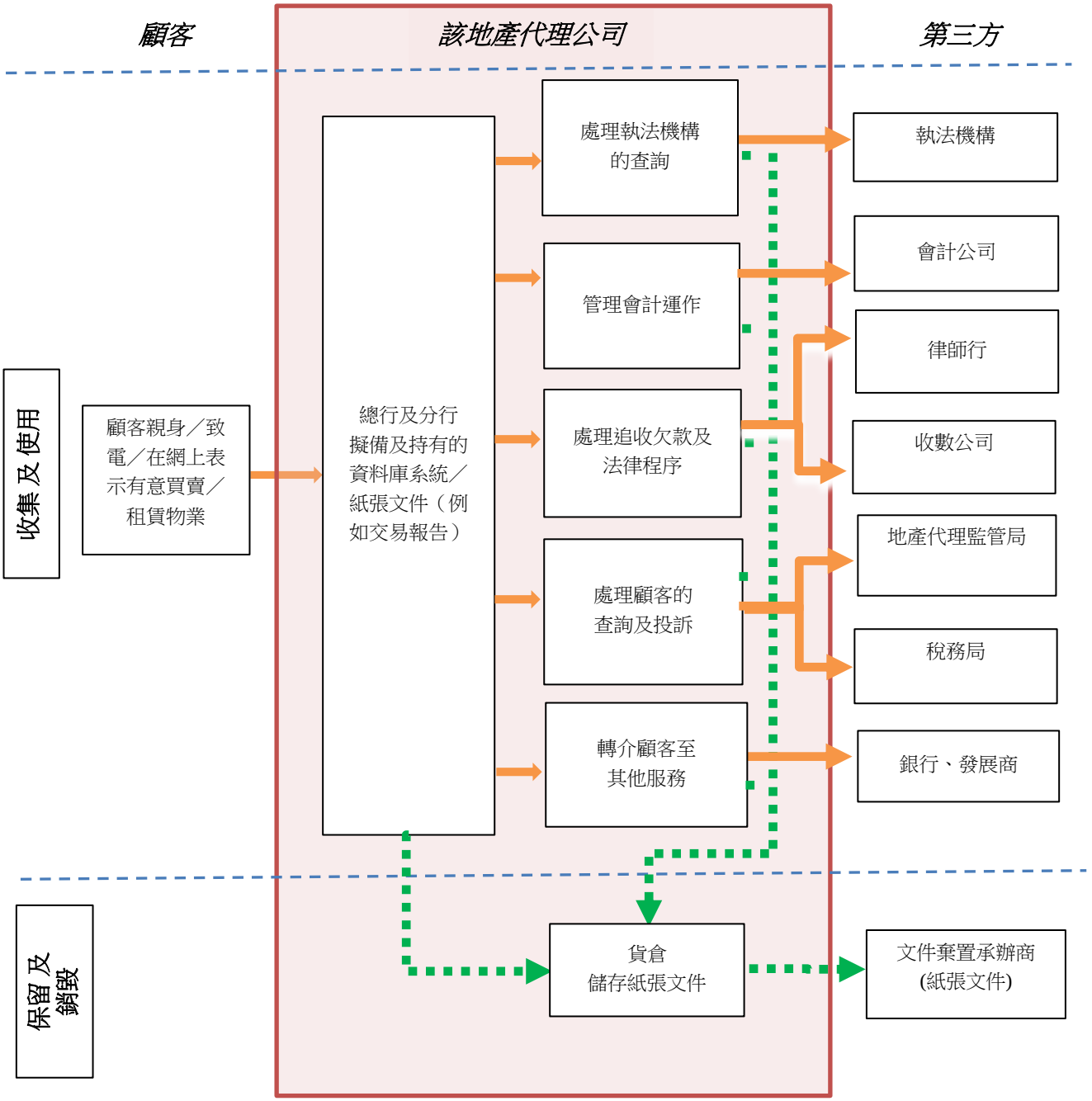
3.12　該地產代理公司會使用顧客的個人資料以提供地產代理服務及作市場推廣活動。此外，該地產代理公司亦會使用顧客的個人資料作以下用途：

(a)　處理執法機構的查詢；
(b)　管理會計運作；
(c)　處理追收欠款及法律程序；

(d) 處理顧客的查詢及投訴；及

(e) 轉介顧客至其他服務。

3.13 顧客個人資料的流程如下：



個人資料的保留

紙張記錄

3.14　該地產代理公司沒有書面政策訂明保留載有顧客個人資料的文件的期限，他們的一般做法是將這些紙張記錄（例如已簽署的訂明表格、臨時買賣合約等）保留最少 5 年及最多 7 年。在分行，載有個人資料的紙張記錄被存檔及儲存於服務台後限制區的文件櫃或儲物室內。在總部，紙張記錄被儲存於鋼櫃內。

電子記錄

3.15　該地產代理公司並沒有就顧客個人資料的電子記錄制定保留期限的政策。載有個人資料的檔案被儲存於總部員工的個人電腦或分行地產代理共同使用的電腦內。系統資料會定期備份到伺服器、網絡附加儲存裝置，以及數碼線性磁帶。

銷毀個人資料

紙張記錄

3.16　根據該地產代理公司的政策，當總部或分行的文件櫃沒有空間時，員工會要求總部提供快遞服務、塑膠箱及標籤，以便將紙張記錄運往該地產代理公司的貨倉儲存。負責員工會根據標籤上註明的棄置日期，安排文件棄置承辦商銷毀有關的紙張記錄。

電子記錄

3.17　該地產代理公司並沒有制定清除顧客個人資料的政策。個別員工須自行負責刪除儲存於個人電腦內載有顧客個人資料的工作檔案。另一方面，在棄置資訊科技器材前，伺服器／電腦內的硬碟機會被移除，然後再以刪除資料軟件永久刪除當中的資料。

視察結果及建議

導言

4.1 專員根據該地產代理公司於本視察時所提供的資料及視察小組的實地觀察，得出視察結果及作出建議。有關結果及建議只反映在視察時所見的循規情況，並不應被視為已全面涵蓋該地產代理公司的個人資料系統於各方面的運作。

個人資料保障措施概覽

4.2 若要有效管理及執行個人資料保障的政策，則機構不可只視有關政策為法律循規的事宜，而是應由董事會做起，將個人資料保障視為其企業管治責任，並將之納入處理業務中不可或缺的一環。

I. 管理層的承諾及管治架構

4.3 該地產代理公司委派了一名董事負責監督私隱事宜。他所管轄的部門的職責之一是處理執法機構的查詢，包括有關個人資料保障的事宜。專員欣悉該地產代理公司在業務運作中考慮到私隱事宜，並鼓勵其他地產代理公司作出同樣的企業承擔。

建議

1. 該地產代理公司最高管理層對保障個人資料私隱的承諾值得欣賞，其將個人資料私隱保障納入企業管治的做法是業界的模範。企業應從最高管理層中委任保障資料主任，以管理私隱管理系統及資料保障相關事務。

II. 全面的私隱政策

4.4 該地產代理公司曾以內部通告形式制定一些有關收集個人資料及在直銷中使用個人資料的實務指引，惟這些通告均是在 2012 年或以前以零

碎的方式發出或更新的，欠缺定期有系統的更新及檢討程序。專員建議地產代理公司應就保障個人資料私隱方面向員工提供指導，並制定全面及統一的政策、指引及程序。

(i)　個別地產代理收集個人資料的方式

4.5　當顧客聯絡該地產代理公司（或其個別地產代理）表達買賣或租賃物業的意願時，該地產代理公司與顧客的關係便開始建立。視察小組了解該地產代理公司制定了全面的私隱政策聲明及《收集個人資料聲明》，並已展示於其網站內，但若顧客親身到訪該地產代理公司的分行或透過電話與個別地產代理聯絡，則未必獲告知有關內容。

4.6　雖然該地產代理公司的內部通告訂明，個別地產代理在顧客簽署訂明表格或在接到顧客願意出售／出租物業的電話時，必須口頭解釋收集個人資料的目的，或在簽訂任何相關協議[8]時提供《收集個人資料聲明》的副本，但視察小組留意到大多數地產代理沒有這樣做，因為：

(i)　他們不知道該內部通告的規定及該《收集個人資料聲明》的存在；及

(ii)　他們只着重於解釋地產代理常規規例的規定（例如委任代理及佣金的安排）。

4.7　除了在該地產代理公司的分行簽署訂明表格外，個別地產代理在物業現場與買方會面，並在公共地方簽署訂明表格，亦是行業間的一般做法。該地產代理公司並沒有指引或程序，指示個別地產代理（或行政職員）如何安全運送文件及要求他們即日將訂明表格或其他相關文件交回辦公室。這種情況會構成保安風險，路過的途人可以在訂明表格上或在代理核實顧客身份的過程中看到個人資料，而訂明表格在運送的途中可能會遺失。

[8] 例如：臨時買賣合約，及臨時租約

(ii)　載有個人資料的文件及記錄的保存期限

4.8　視察小組注意到該地產代理公司下放權力予分行或分區行政小組自行處理一般的行政工作。視察小組視察的所有分行都把已簽署的訂明表格、臨時買賣合約、交易記錄及其他有關資料儲存於分行文件櫃內，由一名行政職員負責管理。

4.9　雖然大多數的分行知悉保留實體文件的最長期限（即 7 年），但分行銷毀文件與否主要是取決於其儲存空間。視察小組留意到有載有個人資料的文件被儲存超過保留期限。

4.10　該地產代理公司並沒有就保留電子化的個人資料制定書面政策或指引，亦沒有規管員工須何時刪除電腦硬碟或資料庫系統內的電子檔案。例如，視察小組留意到會計部從來沒有刪除電腦內交易報告的掃描副本，並發現其最早的掃描副本的檔案建立日期為 1994 年。在會談時，會計部員工曾表示不知道應在既定時間後刪除那些電子檔案。這是一個沒有合理原因下保存個人資料而超過所需時限的例子。

(iii)　個人資料的銷毀程序

4.11　該地產代理公司的文件銷毀程序是由文件棄置承辦商負責處理，惟該地產代理公司並沒有與有關承辦商簽訂任何正式協議，或就棄置文件的程序施加任何保安要求或設立監察機制。

(iv)　保障載有個人資料的文件及記錄的行政措施及資訊科技保安的標準和要求

4.12　該地產代理公司將載有個人資料作不同營運用途的紙張文件儲存於總部或分行儲物室的鋼櫃或上鎖的抽屜內。雖然員工無須用密碼進入總部或分行的儲物室，但儲物室是位於受限制區域內，只有該地產代理公司的員工方可進入。個別員工亦會存放文件於總部或分行的上鎖抽屜內。由於工作空間有限，視察小組留意到有部份紙張文件被隨意放置在員工枱面或辦公室地上。

4.13　在某些分行，一名行政職員會被委派管理數間分行的行政工作，而不會與地產代理駐守同一辦公室。行政職員每日需要到訪分行多次，向地產代理收集文件（例如臨時買賣合約），作存檔及擬備交易報告之用。 在送遞過程中，他們會將文件放入 A4 尺碼的信封中。

4.14　有些分行的可用空間有限，故分行的管理層會盡量利用座位空間，部分電腦屏幕會因而面向分行的公共地方，以致到訪的顧客可以看到屏幕顯示的內容。此外，視察小組留意到有分行向會計部遞交文件時使用循環再用的紙張（當中載有土地查冊結果）。

(v)　直接促銷

4.15　該地產代理公司與顧客簽訂臨時合約（即租賃或買賣）時，顧客可選擇表明是否反對該地產代理公司使用其個人資料作直接促銷。該地產代理公司的網站在收集顧客個人資料的介面亦有提供空格，讓顧客表明是否同意使用其個人資料作直接促銷。專員對於有關做法表示滿意。

4.16　該地產代理公司備有一份以試算表形式載列的拒收直銷訊息的顧客名單，此名單由該地產代理公司的總部負責管理。另一方面，地產代理透過更改資料庫系統內的物業記錄狀況，亦可表達賣方拒絕收取該地產代理公司的直銷訊息的要求。專員在評估管理拒收直銷訊息名單的程序後，認為現行的措施不能有效地顯示所有已接獲的拒收直銷訊息的要求。原因包括：

(i)　個別地產代理管有某些顧客的聯絡資料卻沒有登記在資料庫系統內，故當他們接獲那些顧客所提出的拒收直銷訊息後，或未會向該地產代理公司作出反映；及

(ii)　地產代理透過更改資料庫系統的物業狀況以更新顧客的拒收直銷訊息要求後，在大部份情況下不會再將有關要求告知總部，讓他們更新所持有的拒收直銷訊息名單。

建議

2. 地產代理公司應制定全面的私隱政策，將保障個人資料納入機構內每個重要的操作環節，並定期檢討及更新有關政策。

政策應包括以下範疇：

(i) 個別地產代理收集最少的個人資料的方式；
(ii) 載有個人資料的文件及記錄的保存期限；
(iii) 個人資料的銷毀程序；
(iv) 保障載有個人資料的文件及記錄的行政措施及資訊科技保安的標準和要求；及
(v) 處理直接促銷活動及拒收訊息的要求及操作程序。

III. 監控及持續的評核

4.17 該地產代理公司依靠及信任各部門及分行自行處理個人資料，但沒有定期及有系統地監察或審核個人資料的保障情況。例如，視察小組發現該地產代理公司沒有審核及檢查貨倉的舊文件是否妥善地儲存於紙箱內，並於 7 年後銷毀。視察小組亦留意到載有個人資料的文件被置於貨倉地上無人理會。專員認為要確保所制定的政策能於運作上被有效施行，適時進行全面性的審核是必須的。

建議

3. 地產代理公司應建立定期及全面性的合規審核機制，並進行持續評核，以確保員工遵從有關處理個人資料的政策、指引及程序。

IV. 資料外洩事故通報機制

4.18 視察小組注意到該地產代理公司並沒有書面指引或程序，規管處理資料遺失的程序或外洩的情況。專員認為制定清晰詳細的書面指引及程

序可迅速回應此等事故，並能採取適時的補救措施，避免嚴重損失。

建議

4. 地產代理公司應制定資料外洩事故的指引及程序，訂明處理此等事故的流程，當中應包括：

（i） 向負責部門或管理層匯報資料外洩事故的情況；及
（ii）遏止資料外洩及減少損失的即時評估及補救措施。

V. 處理賣方及買方的個人資料

4.19 作為地產中介，該地產代理公司會處理來自賣方及買方的個人資料。然而，該地產代理公司處理這兩類個人資料的程序是不同的。

4.20 如上文第 3.6 段所述，擬出售或出租其物業的業主（即賣方）必須簽署訂明表格，該地產代理公司才會安排宣傳其物業。該地產代理公司會在相關的資料庫系統開立物業檔案，並在系統內輸入所收集得的資料，包括賣方姓名、聯絡資料，及出售／出租物業的詳情。物業詳情是資料庫系統的基本參數，在指定工作區域內的地產代理均可以查閱得到。上述將賣方資料輸入資料庫系統是一項強制性的做法。

4.21 不過，該地產代理公司並沒有嚴格規定個別地產代理須在資料庫系統登記買方的個人資料，只是鼓勵他們採取有關做法。視察小組了解地產代理擔心所登記的買方資料會被其他職員（例如其上司）查閱得到，因而失去由自己達成交易的機會。因此，視察小組發現大多數地產代理均自行保存買方的個人資料（尤其是聯絡資料），而不在資料庫系統作出登記或告知該地產代理公司他們收集了有關資料。

4.22 專員認為個別地產代理是以該地產代理公司代表的身份收集買方的個人資料。因此，該地產代理公司是資料使用者，負責（i） 控制此等資料的收集、持有、處理或使用及（ii）地產代理其後作出的任何違反條例

的行為[9]。若買方的個人資料沒有被登記在資料庫系統或該地產代理公司沒有獲告知有關資料的收集，該地產代理公司便會失去對此等資料的控制權。有關情況會帶來下述（非全面性）的風險，甚至會導致違反條例的規定，故不容忽視：

(i) 個別地產代理過度收集個人資料，例如尋找合適的物業並不須要收集買方的出生日期（保障資料第 1 原則）；
(ii) 沒有告知買方收集及使用其個人資料的目的 （保障資料第 1 原則）;
(iii) 個別地產代理沒有合理原因而保留買方的個人資料超過所需時限（保障資料第 2 原則）；
(iv) 個別地產代理為個人目的而不當使用個人資料（保障資料第 3 原則）；及
(v) 個別地產代理沒有採取保安措施（例如流動儲存裝置內的資料沒有以密碼保護或加密）保障其持有的個人資料，提高了遺失有關資料的潛在風險（保障資料第 4 原則）。

4.23 即使已考慮到個別地產代理將潛在顧客的聯絡資料視作其重要資產是行內的常規（尤其這是以佣金為本的行業），但專員認為個人資料私隱的權利絕不應因個人的業務利益而受到損害。

建議

5. 地產代理公司應提供適當指引，要求個別地產代理應在相關的資料庫系統輸入賣方及買方的個人資料，以重新掌管所有顧客個人資料的收集、持有、處理或使用的控制權。

[9] 條例第 65(2)條規定，任何作為另一人的代理人並獲該另一人授權(不論是明示或默示，亦不論是事前或事後授權)的人所作出的任何作為或所從事的任何行為，就本條例而言須視為亦是由該另一人作出或從事的。

VI. 技術層面的管治

4.24 視察小組在檢視該地產代理公司的資訊科技保安系統[10]後，欣賞他們審慎地就其資料庫系統設置不同的使用權限。在一個資料庫系統中，地產代理只獲准查閱其工作地區的物業詳情及相關的個人資料。此外，但凡地產代理在系統中查閱賣方的電話號碼，系統都會將有關行為記錄下來，同時亦會限制代理每日可查閱有關資料的次數。

4.25 不過，專員認為該地產代理公司的資訊科技保安仍有改善空間。以下列出一些作為一所具備正規資訊科技保安管治架構的機構應該備有，但卻未有被該地產代理公司採用或實施的範疇：

(a) 機構應指派一名資訊科技部門高層管理人員負責監督資訊科技保安政策的制定、執行及檢討；

(b) 機構應具備一套適用於個人資料私隱的機構性資訊科技保安政策及適當的指引和程序，以規管下述事宜：

(i) 定期更改密碼及設定密碼複雜度的要求；
(ii) 發送載有個人資料的電郵時採取加密或保護措施；
(iii) 正確使用沒有加密設置的便攜式儲存裝置；
(iv) 操作系統及應用程式的保安修補程式管理；
(v) 就棄置具儲存功能的器材制定相關政策；及
(vi) 系統開發的保安風險評估程序及指引。

建議

6. 機構倚重資訊科技系統處理業務成交及保存有關記錄和資料庫。因此，保持資訊科技系統的健康運作以避免系統受網絡攻擊，與其他實體保安措施同樣重要。地產代理公司應指派高層管理人員負責監督資訊科技保安範疇，根據業務定位制定其具體的

[10] 包括資訊科技設備的實體保安、處理個人資料的操作保安、存取權限的機制、保安漏洞管理及棄置資訊科技設備的管理。

資訊科技保安政策。

VII. 培訓及教育

4.26 大部份員工在與視察小組會談時，均表示不知道該地產代理公司就處理個人資料發出的內部通告及實務指引內容。一般情況下，他們只根據部門或分行的一貫做法或自己的行事方式處理個人資料。例如，視察小組在本視察中留意到下述做法：

(i) 個別地產代理在填寫訂明表格時，會詳細地依據地產代理監管局的規定向顧客解釋訂明表格的目的及用途，但卻沒有向他們說明收集及使用其個人資料的目的及用途；

(ii) 部份分行保留載有個人資料的文件的期限是視乎存檔範圍的可用空間而定。視察小組檢測到有文件保留時期過長的情況出現；

(iii) 有員工在未經准許的情況下，從電腦下載載有個人資料的文件至未經加密的個人便攜式儲存裝置內，以便帶回家繼續處理其工作；及

(iv) 有員工會循環再用載有個人資料的紙張。

建議

7. 地產代理公司應適時及定期傳閱有關處理個人資料的政策、指引及程序，並應以有效的方式向職員傳達該些政策、指引及程序上的資訊，讓他們知悉相關規定（例如提供政策、指引及程序資訊的紙本並規定員工簽署，同時透過電郵及內聯網提供相同資訊，以方便參閱）。

地產代理公司應考慮委派部門或小組負責建立尊重私隱文化及促進個人資料保障的符規情況。地產代理公司應經常舉辦個人資料

保障的全面培訓及複修課程，當中應包括於入職培訓內講述有關處理個人資料的政策、指引及程序中的規定和措施，以及就資料保障的特定範疇，舉辦技術培訓（例如根據資訊科技保安政策使用互聯網及便攜式儲存裝置）。

總結

5.1　專員欣悉該地產代理公司已致力按其業務性質及運作模式進行私隱管理。視察結果反映該地產代理公司在個人資料私隱保障方面仍有改善的空間，這正是一個合適的機會讓專員評估該地產代理公司的現有個人資料系統並提供上述建議，以提升及加強其私隱管理，有關建議亦對這個類別的資料使用者極具參考價值，藉以協助他們遵從條例的規定。

5.2　專員經常提倡採納私隱管理系統的好處。藉是次的視察行動，專員強烈鼓勵所有地產代理公司推行私隱管理系統，除了能更有效地管理顧客的個人資料外，亦可協助他們遵從條例的規定，建立顧客的信任，提升機構的名聲及商譽。

5.3　專員鳴謝該地產代理公司及其員工的合作，令視察小組得以詳細了解其資料流程，以及其收集、保留和處理個人資料的原因。專員尤其感謝他們為視察行動提供超越其職責範疇的協助。

5.4　專員希望本報告對該地產代理公司及其他地產代理公司有所裨益，及有助他們建立「保障與尊重個人資料私隱」的文化。

附件1 － 保障資料原則

1. 第1原則－收集個人資料的目的及方式

(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。

(3) 凡從或將會從某人收集個人資料，而該人是資料當事人，須採取所有切實可行的步驟，以確保—

(a) 他在收集該資料之時或之前，以明確或暗喻方式而獲告知—

(i) 他有責任提供該資料抑或是可自願提供該資料；及

(ii) (如他有責任提供該資料)他若不提供該資料便會承受的後果；及

(b) 他—

(i) 在該資料被收集之時或之前，獲明確告知—

(A) 該資料將會用於甚麼目的(須一般地或具體地說明該等目的)；及

(B) 該資料可能移轉予甚麼類別的人；及

(ii) 在該資料首次用於它們被收集的目的之時或之前，獲明確告知—

(A) 他要求查閱該資料及要求改正該資料的權利；

(B) 處理向有關資料使用者提出的該等要求的個人的姓名(或職銜)及其地址，

但在以下情況屬例外：該資料是為了在本條例第8部中指明為個人資料就其而獲豁免而不受第6保障資料原則的條文所管限的目的而收集，而遵守本款條文相當可能會損害該目的。

2. **第2原則－個人資料的準確性及保留期間**

(1) 須採取所有切實可行的步驟，以—

(a) 確保在顧及有關的個人資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，該個人資料是準確的；

(b) 若有合理理由相信在顧及有關的個人資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，該個人資料是不準確時，確保—

(i) 除非該等理由不再適用於該資料(不論是藉着更正該資料或其他方式)及在此之前，該資料不得使用於該目的；或

(ii) 該資料被刪除；

(c) 在於有關個案的整體情況下知悉以下事項屬切實可行時—

(i) 在指定日當日或之後向第三者披露的個人資料，在顧及該資料被使用於或會被使用於的目的(包括任何直接有關的目的)下，在要項上是不準確的；及

(ii) 該資料在如此披露時是不準確的，

確保第三者—

(A) 獲告知該資料是不準確的；及

(B) 獲提供所需詳情，以令他能在顧及該目的下更正該資料。

(2) 須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的(包括任何直接有關的目的)所需的時間。

(3) 在不局限第(2)款的原則下，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者的個人資料的保存時間超過處理該資料所需的時間。

(4) 在第(3)款中—

資料處理者 (data processor) 指符合以下兩項說明的人—

(a) 代另一人處理個人資料；及

(b) 並不為該人本身目的而處理該資料。

3. 第3原則－個人資料的使用

(1) 如無有關的資料當事人的訂明同意，個人資料不得用於新目的。

(2) 資料當事人的有關人士可在以下條件獲符合的情況下，代該當事人給予為新目的而使用其個人資料所規定的訂明同意—

(a) 該資料當事人—

(i) 是未成年人；

(ii) 無能力處理本身的事務；或

(iii) 屬《精神健康條例》(第136章)第2條所指的精神上無行為能力；

(b) 該資料當事人無能力理解該新目的，亦無能力決定是否給予該項訂明同意；及

(c) 該有關人士有合理理由相信，為該新目的而使用該資料明顯是符合該資料當事人的利益。

(3) 即使資料使用者為新目的而使用資料當事人的個人資料一事，已得到根據第(2)款給予的訂明同意，除非該資料使用者有合理理由相信，如此使用該資料明顯是符合該當事人的利益，否則該資料使用者不得如此使用該資料。

(4) 在本條中—

新目的 (new purpose) 就使用個人資料而言，指下列目的以外的任何目的—

(a) 在收集該資料時擬將該資料用於的目的；或

(b) 直接與(a)段提述的目的有關的目的。

4. 第4原則－個人資料的保安

(1) 須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料(包括採用不能切實可行地予以查閱或處理的形式的資料)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，尤其須考慮—

(a) 該資料的種類及如該等事情發生便能做成的損害；

(b) 儲存該資料的地點；

(c) 儲存該資料的設備所包含(不論是藉自動化方法或其他方法)的保安措施；

(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及

(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

(2) 在不局限第(1)款的原則下，如資料使用者聘用(不論是在香港或香港以外聘用)資料處理者，以代該資料使用者處理個人資料，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。

(3) 在第(2)款中—

資料處理者 (data processor) 具有第2保障資料原則第(4)款給予該詞的涵義。

5. 第5原則－資訊須在一般情況下可提供

須採取所有切實可行的步驟，以確保任何人—

(a) 能確定資料使用者在個人資料方面的政策及實務；

(b) 能獲告知資料使用者所持有的個人資料的種類；

(c) 能獲告知資料使用者持有的個人資料是為或將會為甚麼主要目的而使用的。

6. 第6原則－查閱個人資料

資料當事人有權—

(a) 確定資料使用者是否持有他屬其資料當事人的個人資料；

(b) 要求—

(i) 在合理時間內查閱；

(ii) 在支付並非超乎適度的費用(如有的話)下查閱；

(iii) 以合理方式查閱；及

(iv) 查閱採用清楚易明的形式的，

個人資料；

(c) 在(b)段所提述的要求被拒絕時獲提供理由；

(d) 反對(c)段所提述的拒絕；

(e) 要求改正個人資料；

(f) 在(e)段所提述的要求被拒絕時獲提供理由；及

(g) 反對(f)段所提述的拒絕。

附件 2 －在直接促銷中使用個人資料（條例第 35B 至 35H 條）

35B － 適用範圍

本分部並不就要約提供以下服務或就有以下服務可予提供而進行廣告宣傳而適用—

(a) 由社會福利署營辦、資助或津貼的社會服務；

(b) 由醫院管理局或衞生署提供的醫護服務；或

(c) 符合以下說明的任何其他社會或醫護服務：該項服務擬向某名個人提供，而如不向該名個人提供該項服務，便相當可能會對以下人士的身體或精神健康造成嚴重損害—

(i) 該名個人；或

(ii) 任何其他個人。

35C － 資料使用者將個人資料用於直接促銷前，須採取指明行動

(1) 除第35D條另有規定外，資料使用者如擬在直接促銷中，使用某資料當事人的個人資料，須採取第(2)款指明的每一項行動。

(2) 資料使用者須—

(a) 告知有關資料當事人—

(i) 該資料使用者擬如此使用有關個人資料；及

(ii) 該資料使用者須收到該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；

(b) 向該當事人提供關於該擬進行的使用的以下資訊—

(i) 擬使用的個人資料的種類；及

(ii) 該資料擬就甚麼類別的促銷標的而使用；及

(c) 向該當事人提供一個途徑，讓該當事人可在無需向該資料使用者繳費的情況下，透過該途徑，傳達該當事人對上述的擬進行的使用的同意。

(3) 不論個人資料是否由有關資料使用者從有關資料當事人收集的，第(1)款均適用。

(4) 根據第(2)(a)及(b)款提供的資訊，須以易於理解的方式呈示，如屬書面資訊，則亦須以易於閱讀的方式呈示。

(5) 除第35D條另有規定外，資料使用者未經採取第(2)款指明的每一項行動，而在直接促銷中，使用某資料當事人的個人資料，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(6) 在為第(5)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

(7) 凡有法律程序為第(5)款所訂罪行而提起，在該程序之中，有關資料使用者負有舉證責任，證明由於第35D條，本條並不適用。

35D ─ 在何種情況下第35C條不適用

(1) 如在本部生效日期之前─

(a) 某資料當事人已獲某資料使用者以易於理解和(如以書面方式告知)閱讀的方式明確告知，其個人資料擬在或在直接促銷中，就某類別的促銷標的而被使用；

(b) 該資料使用者已如此使用該當事人的任何資料；

(c) 該當事人沒有要求該資料使用者停止如此使用該當事人的任何資料；及

(d) 該資料使用者沒有就該項使用而違反於該項使用時有效的本條例的任何條文，

而該資料使用者在本部生效日期當日或之後，擬在或在直接促銷中，就該類別的促銷標的而使用該當事人的不時更新的有關個人資料，則第35C條並不就該項擬進行的使用或使用而適用。

(2) 如─

(a) 某資料當事人的個人資料是由該當事人以外的另一人(*第三者*)提供予某資料使用者的；及

(b) 該第三者已書面通知該資料使用者─

(i) 就提供該資料而言，第35J及35K條已獲遵守；及

(ii) 該資料使用者可在直接促銷中，就何種類別的促銷標的(該當事人已同意者)使用該資料，

而該資料使用者擬在或在直接促銷中，就該類別的促銷標的而使用該資料，則第35C條並不就該項擬進行的使用或使用而適用。

(3) 在本條中─

本部生效日期 (commencement date) 指本部開始實施的日期；

有關個人資料 (relevant personal data) 就資料當事人而言，指該當事人的符合以下說明的個人資料：在緊接本部生效日期前，該資料的使用，受某資料使用者控制。

35E ─ 如無資料當事人同意，資料使用者不得將個人資料用於直接促銷

(1) 已遵守第35C條的資料使用者不得在直接促銷中，使用有關資料當事人的個人資料，但如以下條件獲符合，則不在此限—

(a) 該資料使用者已收到該當事人對擬如此使用(如該資料使用者根據第35C(2)(b)條提供的資訊所描述者)該個人資料的同意，不論是一般的同意或是選擇性的同意；

(b) (如該項同意屬口頭同意)該資料使用者已自收到該項同意起計的14日內，向該當事人發出確認以下事宜的書面確認—

(i) 收到該項同意的日期；

(ii) 有關許可種類個人資料；及

(iii) 有關許可類別促銷標的；及

(c) 該項使用符合該當事人的同意。

(2) 就第(1)(c)款而言，如—

(a) 有關個人資料屬某許可種類個人資料；及

(b) 該資料是就某促銷標的而使用，而該促銷標的屬某許可類別促銷標的，

則該項使用即屬符合該當事人的同意。

(3) 資料當事人可透過回應途徑或其他方法，向資料使用者傳達對使用個人資料的同意。

(4) 資料使用者違反第(1)款，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(5) 在為第(4)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

35F ― 資料使用者首次將個人資料用於直接促銷時須通知資料當事人

(1) 在將某資料當事人的個人資料首次在直接促銷中使用時，資料使用者須告知該當事人，如該當事人要求該資料使用者停止在直接促銷中使用該資料，該資料使用者須在不向該當事人收費的情況下，停止在直接促銷中使用該資料。

(2) 不論個人資料是否由有關資料使用者從有關資料當事人收集的，第(1)款均適用。

(3) 資料使用者違反第(1)款，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(4) 在為第(3)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

35G ― 資料當事人可要求資料使用者停止將個人資料用於直接促銷

(1) 資料當事人可隨時要求資料使用者停止在直接促銷中使用該當事人的個人資料。

(2) 不論有關資料當事人—

(a) 是否已自有關資料使用者，收到第35C(2)條規定須就使用有關個人資料提供的資訊；或

(b) 有否在較早前，向該資料使用者或第三者給予對該項使用的同意，

第(1)款均適用。

(3) 資料使用者如收到資料當事人根據第(1)款作出的要求，須在不向該當事人收費的情況下，依從該項要求。

(4) 資料使用者違反第(3)款，即屬犯罪，一經定罪，可處罰款$500000及監禁3年。

(5) 在為第(4)款所訂罪行而提起的法律程序中，被控告的資料使用者如證明自己已採取所有合理預防措施，並已作出一切應作出的努力，以避免犯該罪行，即可以此作為免責辯護。

(6) 本條不影響第26條的施行。

35H － 第3保障資料原則規定的對在直接促銷中使用個人資料的訂明同意

儘管有第 2(3)條的規定，凡根據第 3 保障資料原則，資料使用者在直接促銷中使用某資料當事人的任何個人資料，須獲該當事人的訂明同意，該資料使用者如沒有違反第 35C、35E 或 35G 條，即視為已取得該項同意。

— 本報告完 —