固定及流動電訊服務營辦商保障顧客資料的實務守則

引言

固定[1]及流動[2]電訊服務營辦商在運作及提供服務的過程時，會收集大量的顧客個人資料，包括**顧客的電話號碼、住址及通話記錄詳情。**這些資料，在某些情況下可能屬敏感性資料，如被用作非法用途則可能具有出售價值。因此，服務營辦商須確保有關資料得到適當保護，免被濫用，否則機構的聲譽有可能因不誠實或貪污的行爲而蒙受損害。

目標

2. 本實務守則屬自願性質，目的是列出一些可防止員工在未經批准下向外披露顧客資料的良好管理措施，爲固定及流動電訊服務營辦商就制訂保障顧客資料的標準和措施提供一般指引。由於守則不能夠盡錄所有的良好管理措施，固定及流動電訊服務營辦商可採納其他標準和措施，爲顧客資料提供合理充足的保障。此外，固定及流動電訊服務營辦商亦須遵守《個人資料〔私隱〕條例》及《防止賄賂條例》的有關條文。

法例

個人資料（私隱）條例

3. 《個人資料（私隱）條例》（香港法例第 486 章）第 4 條規定，資料使用者不得作出違反該條例附表 1 所列的任何保障資料原則的作爲或從事違反任何該等原則的行爲，但如該作爲或行爲（視屬何情況而定）是根據該條例規定須作出或進行或准許作出或進行的，則屬例外。六項保障資料原則中的原則 4 與本實務守則尤其相關，該原則規定資料使用者：

---

[1] 就本實務守則而言，固定服務營辦商指獲電訊管理局局長根據《電訊條例》（第 106 章）發出固定傳送者牌照或固定電訊網絡服務牌照，以提供本地固定電訊網絡服務的持牌商。

[2] 流動服務營辦商指獲電訊管理局局長根據《電訊條例》（第 106 章）發出以下牌照的持牌商：

(a) 使用 1.9 吉赫至 2.2 吉赫頻帶的移動技術提供公共無線電通訊服務的移動傳送者牌照；

(b) 使用 800/900 兆赫、1.7 至 1.9 吉赫頻帶的移動技術提供公共無線電通訊服務的公共無線電通訊服務牌照或提供公共無線電傳呼服務的公共無線電通訊服務牌照；或

(c) 提供流動虛擬網絡服務的公共非專利電訊服務牌照。

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、刪除或其他使用所影響，尤其須考慮—

(a) 該等資料的種類及如該等事情發生便能造成的損害；
(b) 儲存該等資料的地點；
(c) 儲存該等資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；
(d) 爲確保能查閱該等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) 爲確保在保安良好的情況下傳送該等資料而採取的措施。

4. 違反保障資料原則本身並不構成罪行，但在某些情況下，個人資料私隱專員可以透過執行通知的方式要求資料使用者遵守有關原則。違反有關通知即屬犯罪。此外，如違反保障資料原則規定的行爲涉及的資料當事人因有關行爲受損，包括情感的傷害，有關人士有權索償。僱主須就僱員任何導致該等損害的行爲負上法律責任。

防止賄賂條例

5. 《防止賄賂條例》(香港法例第 201 章)第 9(1)條訂明，任何代理人無合法權限或合理辯解，索取或接受任何利益，作爲他作出以下行爲的誘因或報酬，或由於他作出以下行爲而索取或接受任何利益，即屬犯罪

(a) 作出或不作出，或曾經作出或不作出任何與其主事人的事務或業務有關的作爲；或
(b) 在與其主事人的事務或業務有關的事上對任何人予以或不予，或曾經予以或不予優待或虧待。

因此，固定及流動電訊服務營辦商的員工在未經批准下披露顧客的個人資料，以換取利益，可能違反《防止賄賂條例》的條文。

牌照條件

6. 各電訊牌照中的牌照條件規定，除非顧客以電訊管理局局長批准的形式同意，持牌人不得披露顧客的資料。另外，持牌人不得使用

其顧客提供或在向其顧客提供有關的服務過程中取得的資料，但與持牌人提供該服務有關而使用者則屬例外。

良好管理措施

7. 下列的良好管理措施，是爲固定及流動電訊服務營辦商在制訂標準及措施以防止其員工在未經批准下向外披露顧客資料時提供一般指引。這些管理措施可分成五個主要類別：

(a) 保障顧客個人資料政策；
(b) 保障顧客個人資料的技術措施；
(c) 資料儲存地點的保安；
(d) 提高員工保障顧客個人資料意識的方法；及
(e) 轉移顧客個人資料時應採取的保密措施。

(一) 保障顧客個人資料政策

資料分類政策

8. 當顧客選用固定或流動電訊服務時，營辦商會收集顧客的個人資料（例如姓名、身分證明文件號碼、住址等）。而營辦商在提供服務的過程中，亦會衍生其他個人資料（例如顧客選用的服務計劃、用量、帳項詳情和付款繳費詳情等）。由於此等個人資料在不同情況下有不同的敏感度，服務營辦商須設立一套資料分類政策，就資料的敏感程度和可能被洩露的風險，適當地將不同類別的個人資料分類。有關政策亦須就每一類別的資料訂明所需要採取的保密措施，無論該等資料是以電子形式或文件格式儲存。有關政策的目的是防止員工在未經批准下披露顧客的資料。

道德及個人資料私隱政策

9. 服務營辦商須設立一套企業操守政策，列明公司的道德標準及操守規定，特別是保障顧客個人資料的準則。這些準則及規定，可以透過資料私隱政策的方式，明確訂明基於道德責任及根據《個人資料（私隱）條例》的法律規定，公司會致力保障顧客的個人資料不會在未經批准下洩露。服務營辦商亦須就保密顧客資料向本地及海外的僱員提供明確指引。僱員亦須承諾（如以僱傭合約內相關條文的方式），會絕對保密其接觸的資料，亦不會使用有關資料於作爲履行服務營辦

商僱員身份指定的職務以外的用途。有關政策亦須闡明預防貪污的重要性。

10. 有關操守政策應向所有員工公布，並須定期提醒新入職及在職員工遵守有關規定。爲確保僱員遵守政策，服務營辦商須發出清晰的警告，述明如僱員違反有關規定將會受到紀律處分，及有可能負上刑事責任。

限制資料存取政策

11. 在日常業務運作上，不同的員工需要對不同種類的個人資料有不同程度的接觸。例如有些員工只可在電腦上閱讀，不可修改顧客的個人資料；有些則可透過電腦操作改動顧客的個人資料。如公司給予僱員的資料存取權限，超越其執行日常職務所需的權力，便會爲員工製造濫用權限的機會。因此，服務營辦商須設立一套限制資料存取的政策，對每一類別的個人資料，就員工的級別及職責範圍，定下存取資料的權限。總括而言，服務營辦商應按「知情需要」的原則給予員工取閱資料的權限。如使用電腦應用程式協助處理及檢索顧客個人資料，則應按「行事需要」原則給予員工系統功能的運用權。由於個人電腦被廣泛應用，服務營辦商亦應考慮限制員工列印或下載顧客個人資料至個人電腦或磁性媒體，因爲有關活動不能就資料列印或下載後的用途提供審查記錄。營辦商應明確規定顧客個人資料的儲存期限及方式，不論有關資料是以電子形式或文件格式儲存。

(二) 保障顧客個人資料的技術措施

取閱核准制度

12. 服務營辦商須就員工申請取閱客戶資料確立一套核准制度及相關程序，無論該等資料是以電子形式或文件格式儲存，並清楚界定適當的核准權限級別。所有員工的申請須獲正式核准才可給予取閱權。服務營辦商亦須制訂相關的措施保密往來申請書的內容（例如使用密封信封及規定須認收）。爲促使規定獲得遵從，服務營辦商須向所有員工清楚公布有關取閱核准制度的詳情。

識別及認證

13. 爲確保問責性，服務營辦商應給予每一位可取閱顧客個人資料

的員工一個專有的個人使用者帳戶，並在他們能進一步使用已獲授權的系統功能前，須以其專有的用戶標號登入系統以識別其爲有效的使用者，並以其有效的密碼加以認證。營辦商須定期提示員工切勿向他人透露他們的密碼，並在使用系統完畢後即時登出，以避免他人使用其帳戶。服務營辦商亦須定期核對有效的使用者帳戶名單，以免因人事變動而出現的過時使用者帳戶遭他人濫用。

密碼管理

14. 爲減少密碼外洩的機會，服務營辦商應實行密碼管理措施，例如：禁止使用日期或常用的字眼作密碼；設定密碼的最短長度；限制定期更改密碼；強制於首次登入系統或每次重新設定密碼後更改密碼；禁止於一定時限內重新使用舊密碼；及於系統登入失敗達一定次數後使帳戶暫時失效。

取閱客戶資料

15. 當顧客索取客戶服務時，服務營辦商一般的做法是先要求客戶提供資料以核實其客戶身分，然後才提供所需服務。例如：傳呼服務客戶通常需要說出自己的帳戶編號及密碼，才可查核其戶口內的訊息；流動電服務客戶通常需要提供其電話號碼及身分證明文件號碼，方可轉換服務計劃。爲防止前線客戶服務人員非因向顧客提供客戶服務而檢閱客戶的個人資料，服務營辦商應採用複合密碼以限制客戶服務人員檢索客戶個人資料。例如，當顧客於網上查閱其帳戶資料時，一種良好的保安方法是使用多重核證碼，而其中一組個人密碼應僅爲客戶所知。服務營辦商應備有配套設施，讓客戶自行更改其個人密碼。

16. 服務營辦商應在可行範圍內考慮對獲授權存取顧客資料的使用者的所有活動，包括查詢活動等，進行稽核記錄，以便能追查有關職員查閱客戶資料的活動。服務營辦商亦應在可行範圍內就試圖未經授權而查閱顧客個人資料的活動進行稽核記錄。該等記錄應保存一段合理時限，以協助日後的調查及監察。另外，服務營辦商應保障稽核記錄免被竄改，及派監督人員查核稽核記錄。

17. 我們鼓勵服務營辦商在可行範圍內主動採取上述取閱客戶資料的措施。第 15 及 16 段提出的措施的累積效果取決於營辦商有否採用所有或部分的措施。若未能實施上述任何較爲主動的預防措施，服務

營辦商至少應在接獲投訴指職員濫用取閱客戶資料的權限或發現有關問題時，可以毫不困難地以其他方法協助調查及防止員工進一步濫用權限。

連線保安

18. 分銷店的職員於履行職務時有可能需要遙距接達服務營辦商的電腦以取閱顧客資料。服務營辦商應檢查連線要求是否來自已知及獲授權的地點。若資料需要額外保護，服務營辦商應將資料加密後才傳送，令截取者無從識別當中的數據。

文件保安

19. 已填妥的服務申請表格、電腦編制的報告及其他文件都可能載有客戶個人資料。服務營辦商應採取所有可行步驟，防止該等文件被未經授權人士取閱，並確保銷毀該等文件時不會洩露客戶個人資料。例如，在商店搬遷或關閉時，服務營辦商應就任何載有客戶資料的文件保存一份完整的轉移記錄，列明有關文件、轉移日期及目的地。

身分證明文件的副本

20. 當顧客申請電訊服務時，服務營辦商或會收集顧客的身分證或其他身分證明文件的副本。若未獲授權而可取閱有關文件，則增加了資料濫用的機會。爲防止不當行爲，該等文件的副本應在必須及有理由的情況下才向顧客收集、在副本影像上蓋上「副本」(COPY)字樣、視有關副本爲機密文件及存放於有保安設施的地點、限制索閱並界定儲存期限，及採取穩妥的銷毀程序。關於收集及使用身分證明文件副本的進一步指引，請參閱由個人資料私隱專員公署發出的「身分證號碼及其他代號實務守則」。

(三) 地點的保安

電腦中心

21. 備有電腦設施的電腦中心、設有工作站及存放文件的辦公室、電話機樓及電話線路經過的接線箱，都是可以被人盜竊、截取或竊聽客戶個人資料的地方。因此，服務營辦商必須管制及監察該等地點的出入情況，亦應只限獲授權人士進入。

周邊設備

22. 服務營辦商若容許以圖文傳真形式遞交服務申請表，應以指定的傳真機接收，但傳真機不應放在任何人都可進入的開放範圍。服務營辦商亦應留意工作站的擺放位置，*或考慮使用螢幕保護裝置*，免致客戶個人資料在資料處理期間被未經授權人士看到。

(四) 員工的保安

保安培訓

23. 保安措施是否有效取決於職員是否遵從。服務營辦商應推行一套企業培訓政策，爲員工提供足夠保安培訓及技術訓練，並定期向所有員工傳閱保安備忘錄。所有負責處理顧客個人資料的員工應完全明瞭該服務營辦商的保安及保障私隱措施及程序，並獲提供足夠的培訓。

電話簿查詢服務

24. 固定電訊網絡服務的服務營辦商須就所有客戶的電話號碼提供電話簿服務，除非有關客戶已申請電話簿除名服務。服務營辦商應爲電話查詢服務員制定清晰的營運指引，讓他們回應查詢有關申請電話簿除名服務的顧客的資料時有所依循，確保不會洩露該等客戶的資料。

員工的調配

25. 如某重要職位在日常職務中可取閱敏感的客戶個人資料，服務營辦商在挑選員工出任該等職位時，應考慮以員工的誠信作爲入選的標準之一。

監督

26. 例行及隨機的監督檢查是及早察覺出僱員不尋常／不當行爲的有效工具，例如在不尋常的時間進入電腦系統或異常地大量取閱系統的資料。監督者亦應密切監察擔任高風險職務的員工的活動，以便及早查出濫權的情況，例如大量編印客戶資料或下載客戶個人資料。

(五) 客戶個人資料的轉移

27. 服務營辦商可能會聘用承辦商或代理，代其向客戶提供（包括但不限於）安裝及維修等服務，及追收逾期款項。在這種情況下，營辦商或須向承辦商或代理提供有關的客戶個人資料。服務營辦商應明白他們須爲承辦商或代理的違規行爲負責。因此，服務營辦商：

(a) 應在收集客戶資料當時或之前，通知客戶該等資料或會轉交承辦商或代理；
(b) 只應轉移給承辦商或代理與其執行所委託的任務有關及所需的客戶資料；
(c) 應採取所有可行步驟，確保客戶個人資料在安全及保密的情況下轉交承辦商或代理；
(d) 應在其委託承辦商或代理代其執行有關任務的協議書內列明：

    (i) 禁止承辦商或代理及其僱員洩露在執行任務期間所獲得的客戶個人資料；
    (ii) 強制承辦商或代理遵守保障資料原則，以及營辦商在本港須予遵守的同一標準政策，以保護客戶個人資料。
    (iii) 要求承辦商或代理在無需再使用有關資料時，退回或銷毀所有客戶個人資料；
    (iv) 要求承辦商或代理若在服務營辦商要求時提交其遵守相應要求的稽查報告；
    (v) 承辦商或代理聲明不會複印營辦商轉交的客戶資料，或將有關資料使用於所委託任務以外的用途；及

(e) 應採取所有可行步驟，確保承辦商或代理遵守協議書中的條款及細則。

保安檢討及稽查

28. 由於營商環境及科技發展瞬息萬變，保安措施的有效性可能會隨時間減弱。服務營辦商應不時檢討系統的保安措施，以評估其實際效益，同時找出容易引致貪污的新範疇，以便採取適當的預防措施。服務營辦商亦可籍此機會，找出未能符合現行政策及程序的情況。

執行

29. 本實務守則屬自願性質，固定及流動電訊服務營辦商須自律遵守。業內各成員均有責任維持電訊業的誠信及信譽。

消費者委員會
廉政公署
個人資料私隱專員公署
電訊管理局
二零零二年六月十七日