(翻譯本)

本局檔號： B1/15C
B9/29C

致： 所有認可機構
行政總裁

敬啟者：

保障客戶資料

金管局曾於 2008 年 7 月發出「保障客戶資料」通告，提醒認可機構關於客戶資料保密及實施保障客戶資料的主要管控措施的重要。因應過去幾年業界及科技的發展，本通告旨在更新該通告所載的相關指引。

防範及偵察客戶資料遺失或外洩的管控措施

為使客戶資料保密，認可機構應確保員工對保障客戶資料維持高度警覺。此外，認可機構應實施多重 (包括資訊科技及非資訊科技層面) 保安措施，以防範及偵察客戶資料遺失或外洩。儘管《監管政策手冊》多個單元 [1] 及本局發出的多份通告已涵蓋有助保障客戶資料的風險管理原則及管控措施，本通告謹就一些管控措施再作闡述及更新(載於附件)，特別考慮到的最新發展包括：

(i) 銀行界相繼採用系統管控措施 (即由自動化裝置實施的管控措施) 以防範或偵察客戶資料外洩，因此有關認可機構已作出更妥善的準備，防範及偵察客戶資料外洩事故，並採取迅速行動控制影響，以降低信譽及法律風險。舉例來說，這些認可機構可更迅速識別由個別員工引起的事故 (例如，涉

[1] 包括《監管政策手冊》之單元 TM-G-1「科技風險管理的一般原則」、OR-1「業務操作風險管理」及 SA-2「外判」。

事員工未經批准將客戶資料發送至個人電郵帳戶)，因而能夠及時採取行動，避免客戶資料進一步外洩；

(ii) 香港銀行公會最近制定，如成員銀行容許員工透過「自攜裝置」[2] 來處理工作，必須遵守的嚴格管控措施的最低標準。根據香港銀行公會，這套標準已顧及透過「自攜裝置」來處理工作所涉及的客戶資料遺失或外洩風險，並能提供近似成員銀行的電腦設備所提供的保障，尤其是有關查閱客戶或個人資料的部分。只要認可機構全面遵守嚴格管控員工透過「自攜裝置」來處理工作的標準，金管局支持這套標準並容許認可機構採納這個做法。但如果金管局發現未有遵守標準的情況，將會對有關認可機構實施適當的監管措施 (例如，若發現重大不足之處，金管局可能要求該認可機構中止使用「自攜裝置」來處理工作的做法，直至有關不足之處獲得糾正為止)。此外，金管局預期認可機構應按照資料分類及風險評估結果，就「自攜裝置」來處理工作的做法實施額外的嚴格管控措施，以保障其系統及網絡。

為免產生疑問，認可機構任何時候均須遵守《個人資料(私隱)條例》，以及個人資料私隱專員公署就保障客戶及員工個人資料 [3]發布或批准的任何相關實務守則、規則或指引 [4]。

<u>處理客戶資料遺失或外洩事故的管控措施</u>

為管控及盡量減少客戶資料被竊、遺失或外洩事故 (私隱資料事故) 可能造成的影響，認可機構應設立有效的事故處理及通報程序。具體而言，認可機構應指定一名有足夠權限的高級管理人員或一個由高級管理層擔任主席的管理委員會，負責監察私隱資料事故的處理及通報程序。認可機構應制定全面程序，以協助負責處理這類事故的員工，其中包括按適當情況向該指定高級管理人員及有關監管機構

---

[2] 「自攜裝置」指員工自攜電腦設備 (如個人電腦、平板電腦或智能電話) 來處理工作。

[3] 除《個人資料（私隱）條例》的條文外，認可機構應注意在未得客戶同意下，不得向客戶的有關人士披露該客戶的資料。

[4] 包括個人資料私隱專員公署於 2014 年 10 月發出的《銀行業界妥善處理客戶個人資料指引》。

(包括金管局及個人資料(私隱)專員(私隱專員)) 匯報事故；查明事故性質、事故原因及受影響客戶的身分；適當地通知受影響客戶 (若認可機構決定不通知受影響客戶，應提供理據說明為何不通知受影響客戶)；採取迅速的補救行動，以保障受影響客戶的權益，並防範類似事故再次發生。

若私隱資料事故的性質嚴重，例如該事故可能對認可機構的信譽造成重大影響、受影響客戶數目眾多，或被竊、遺失或外洩的客戶資料屬高度敏感，本局預期認可機構應於發現或獲通知該事故後盡快向金管局匯報該事故及通知受影響客戶。若受影響的客戶數目眾多，認可機構應考慮對外作出公布；這是迅速通知受影響客戶的有效方法，認可機構並可透過向客戶保證會採取補救行動管控及減少事故對客戶的影響，以挽回客戶的信心。此外，儘管現時並無法律條文規定認可機構必須向私隱專員呈報私隱資料事故，但認可機構應衡量事故的嚴重程度，並參考私隱專員發出的《資料外洩事故的處理及通報指引》，認真考慮向私隱專員呈報私隱資料事故。若認可機構決定不向私隱專員呈報事故，應提供理據說明。

認可機構重新評估現行的管控措施

鑑於保障客戶資料的重要，金管局預期認可機構應就本通告所載指引及《監管政策手冊》其他相關單元及通告，於 2015 年首季內完成對其現行管控措施足夠與否的嚴格評估。若評估結果顯示有不足或有待改善之處，認可機構應及時實施適當措施以加強管控。

若就防範及偵察客戶資料遺失或外洩的管控措施有任何疑問，請聯絡趙紫瑋先生 (2878 1389) 或朱嫣婷女士 (2878 1563)；至於有關處理客戶資料遺失或外洩事故的管控措施的疑問，請聯絡倪敏華女士 (2878 1370) 或張慧貞女士 (2878 1501)。

助理總裁(銀行監理)
鄭發

2014 年 10 月 14 日

連附件