缺失態樣

對員工外寄電子郵件之過濾偵測作業或使用電子郵件之管理欠周延，不利防範客戶個資外洩風險。

缺失情節

- 雖已建置資料外洩防護系統，執行外寄電子郵件資料外洩防護 (DLP ,Data Loss Prevention)偵測作業，惟設定之郵件內容過濾原則欠完整，對加密檔、圖形檔等無法過濾之郵件，亦未建立阻擋審核機制。
- 員工可透過網際網路使用郵件軟體(如：outlook)收取公司電子郵件，且收取之郵件內容可另儲存於未受公司管制個人電腦或個人行動裝置，惟對收取之電子郵件內容是否含有客戶個資，尚未建立過濾機制或相關控管措施。

改善作法

- 應對含有客戶資料之外寄電子郵件，設定妥適之過濾規則及安全控管政策，並建立定期檢視機制，如：
  - 應確實將個人資料保護法規定之得以直接或間接識別個人之個人資料，完整納入系統設定之過濾原則。
  - 應針對附件為加密檔、圖形檔等無法辨識過濾之電子郵件，建立事前審核檔案傳輸是否合法之管控措施。
  - 應建立違規事件管理之規範，並建立定期檢視相關安全控管政策是否有效執行之機制。
- 應對員工於行外透過網頁郵件(Web Mail)服務，收取銀行含有客戶個資之電子郵件，另儲存於未受管制個人電腦或個人行動裝置，建立相關作業規範並進行妥適之使用管理措施。

缺失態樣

客戶資料之運用及處理有未臻妥適之情形。

缺失情節

- 對保有個人資料之特定目的消失或期限屆滿時，未訂定刪除、停止處理或利用之管理程序，核與「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」規定不符。
- 辦理客戶通訊地址資料異動作業，未留存客戶書面申請文件或電話紀錄等軌跡，不利事後勾稽核對。

改善作法

- 應定期盤點相關個資檔案，若客戶主動要求刪除，或個人資料檔案蒐集之特定目的消失屆滿保存期限，應由業務單位向資訊單位提出停止處理或利用該個人資料檔案。
- 個人電腦個資電子文件檔，由經辦單位使用人員將檔案內個人資料刪除後，應將刪除後檔案統一存放控管，以留存刪除軌跡備查。
- 辦理客戶通訊地址資料異動作業，應留存客戶申請文件或電話紀錄等書面文件備查。

缺失態樣

客戶資料之運用及處理有未臻妥適之情形。(續)

缺失情節

- 辦理個資清查及盤點作業對象，以最終保有管理者為標準，未包括業務涉及個人資料蒐集、處理、利用者，且未建立管理機制及留存評估紀錄，核與「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」規定不符。
- 未依「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」之規定，與接觸個資人員約定保密義務。
- 員工使用電子郵件傳遞資料，尚未建立有效安全控管機制。

改善作法

- 應切實辦理客戶個人資料檔案清查，建立完整之個資檔案清冊，並依規評估個資風險及訂定管理機制。
- 公司應查核確認所保有之個人資料現況，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管理機制，並應與接觸個資人員約定保密義務。
- 對員工使用電子郵件傳遞資料，應利用程式或工具軟體進行檢查及偵測是否含有個人資料，並留存相關紀錄，以防範客戶個人資料遭不當使用。

缺失態樣

客戶資料之運用及處理有未臻妥適之情形。(續)

缺失情節

- 資訊設備報廢或轉作他用時，未採取防範資料洩漏之適當措施，與本會「指定非公務機關個人資料檔案安全維護辦法」第 9 條第 1 項第 1 款規定不符。
- 對儲存含個資資料之檔案伺服器，未開啟稽核功能留存存取作業紀錄；另對核心主機執行批次作業產出可下載至周邊伺服器供業務單位自行查詢列印或轉寄之電子檔案，惟核心主機及周邊伺服器均未留存作業軌跡，不利追蹤個資使用情形。
- 辦理行動投保業務，提供業務員透過其行動裝置使用行動投保系統招攬業務，對儲存於伺服器資料庫之要保書、財務報告書、保險費繳款資料、電子簽名等要保資料，未以加密方式儲存，與「保險業經營行動投保業務自律規範」第 8 條不符。

改善作法

- 應切實建立報廢資訊設備及其轉作他用之管理措施，以維個資安全。
- 涉及個資之存取，應嚴格控管該等資料之存取權限，並應對資料之存取及傳遞建立申請、保管、使用及刪除等規範，並留存完整稽核軌跡、建立主管覆核及定期清查等控管機制。

缺失態樣

客戶資料之運用及處理有未臻妥適之情形。(續)

缺失情節

- 辦理個資清查範圍有欠完整，如對個人電腦及各系統中涉及個人資料之檔案與交易流程等均未予以盤點。
- 對利用客服應用系統查詢個人資料，未留存作業稽核軌跡及產製覆核報表；對個人電腦 USB 埠之存取，雖採防護軟體記錄存取軌跡，惟僅留存檔案名稱，不利判斷內容是否含有個人資料等機敏資料，亦不利追蹤覆核及確保資料安全。
- 對移動式儲存媒體(移動硬碟、USB)未訂定使用規範或管理欠妥。

改善作法

- 應切實辦理客戶個人資料檔案清查，建立完整之個資檔案清冊。
- 涉及個資之存取，應嚴格控管該等資料之存取權限，依職務需要覈實授權，並應對資料之存取及傳遞建立申請、保管、使用及刪除等規範，並留存完整稽核軌跡、建立主管覆核及定期清查等控管機制。
- 應訂定儲存媒體使用規範，另對移動式儲存媒體攜出檔案之使用紀錄，產製稽核報表及建立覆核機制。