缺失態樣

客戶資料之安全維護、運用及處理有未臻妥適之情形。

缺失情節

- 公司對外網頁，點選「聯絡方式」，畫面出現要求填寫個人資料(包括姓名、性別、聯絡電話、聯絡地址及電子郵件等)，惟未依個人資料保護法第 8 條及第 19 條相關規定於網頁揭示當事人蒐集目的並取得其同意。
- 向電腦室申請列印 1 年內有交易客戶個人資料，未經個資小組覆核。
- 開放員工或外部人員使用自有裝置(如筆電、個人電腦或平板等)，自網際網路連線至正式營運系統伺服器，未採用適足之使用者身分驗證機制（如雙因子認證），即可執行查詢與匯出個資檔案。

改善作法

- 應依法規及內部規定辦理蒐集、運用、處理個人資料作業。
- 應加強對外服務系統之使用者身分驗證機制，並重新檢視系統安全設計功能。

缺失態樣

未訂定個人資料檔案安全維護計畫，並辦理個人資料清冊盤點及風險評估。

缺失情節

- 辦理個資盤點作業有欠完整，如對個人電腦及各系統中涉及個人資料之檔案與作業流程，或新增業務流程及新系統啟用等未納入清查盤點範圍。
- 未依其業務規模及特性，規劃、訂定與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法。
- 未定期查核確認所保有之個人資料現況，界定個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，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。

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。
- 應確實依「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」第 3 至 5 條規定辦理，以落實個人資料保護。

缺失態樣

對以電子郵件傳遞個人資料之偵測作業有欠完備之情形。

缺失情節

- 員工使用電子郵件傳遞資料，尚未建立檢核所傳送之資料檔是否含有個人資料之控管機制，或過濾篩選原則不含帳號、電子郵件，有欠周延。
- 對於經由電子郵件系統對外傳送含有個資或機敏資料，未建立過濾機制，或雖已導入郵件過濾系統，惟過濾條件有欠嚴謹。
- 對電子郵件主旨與內容及附檔之偵測條件，未能涵蓋姓名及其他個人資料(如出生年月日、傳真、電子信箱、職業等)，有欠完整。
- 電子郵件之偵測功能，無法對已加密之附件檔案進行偵測，不利個人資料保護。

改善作法

- 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，且過濾原則應具有完整性，以防範客戶個人資料遭不當使用。
- 應建立電子郵件個資篩選監控機制及留存完整稽核軌跡；重新檢視電子郵件個資過濾條件之妥適性，及建立主管審核放行機制並定期檢討。
- 辦理對外傳送之電子郵件(含附件檔案)是否涉及個人資料之偵測作業，設定之偵測條件應能涵蓋其他涉及之個人資料，以維護個人資料安全。
- 對電子郵件之偵測範圍應包括已加密之附件檔案。