

中華票券金融股份有限公司個人資料檔案安全維護辦法

(030九五八)

第一章 總則

第一條：本辦法係依據個人資料保護法(以下簡稱個資法)及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訂定。

第二條：本辦法係為確保本公司所涉及個人資料之合法蒐集、處理及利用，防止個人資料被竊取、竄改、毀損、滅失或洩漏，規劃採取適當安全維護措施，俾降低個人資料損害之發生，並維護當事人權益。

第二章 個人資料保護之規劃

第三條：本公司設置「個人資料保護管理小組」(以下簡稱個資小組)，以規劃、訂定、修正與執行本辦法所訂相關事項。

個資小組由總公司法令遵循主管擔任召集人，並由各單位主管組成，分別負責下列事項：

- 一、法務暨法遵室:擬訂本公司個人資料保護管理制度及相關規定、辦理個人資料保護相關法規訓練與本辦法之增修。
- 二、管理部:個資外洩事件對外通報。
- 三、資訊室:個人資料之資訊安全管理。
- 四、各單位主管負責各該單位之個人資料安全管理，應指定人員辦理各該單位下列個人資料保護事項：
 - (一)、本公司個人資料保護政策之執行。
 - (二)、個人資料保護事項之協調聯繫。
 - (三)、單位內個人資料損害預防及危機處理應變之通報。
 - (四)、其他有關單位內個人資料保護之規劃及執行。

第四條：本公司應依個人資料保護相關法令，每年查核確認所保有之個人資料現況，界定其納入本辦法之範圍。

第五條：本公司應依前條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。

第六條：本公司因應個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應依下列方式辦理：

- 一、事故單位於確認事故發生時，應立即通報個資小組採取應變措施，儘速查明事故發生之原因、採取證據保全措施、避免事故範圍擴大及控制當事人損害，並於事故查明後儘速以書面、電子郵件、傳真、電話通知或其他足以使當事人知悉或可得知悉之方式通知當事人，通知內容包括個人資料被侵害之事實及本公司已採取之因應措施。
- 二、事故發生後，由個資小組將事故原因、處理情形及影響範圍

簽報總經理，如屬重大個人資料安全事故時，則依本條第二項規定辦理。

三、事故發生後，由個資小組研議矯正預防措施，並督導改善情形。

本公司遇有重大個人資料安全事故時，應依金融監督管理委員會發布之格式於七十二小時內通報金融監督管理委員會。但於其他法令有規定時，並應依各該法令之規定辦理。依前項第三款所研議之矯正預防措施應經公正、獨立且取得相關公認認證資格之專家，進行整體診斷及檢視。

前項所稱重大個人資料安全事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及本公司正常營運或大量當事人權益之情形。

第七條：本公司應每年對員工施以個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、員工之責任範圍與各種個人資料保護事項之機制、程序及措施。

第三章 個人資料之管理程序及措施

第八條：本公司應就下列事項，訂定個人資料之管理程序：

- 一、蒐集、處理或利用之個人資料包含個資法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件；其經當事人書面同意者，並應確保符合個資法第六條第二項準用第七條第一項、第二項及第四項之規定。
- 二、檢視個人資料之蒐集、處理，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。
- 三、檢視一般個人資料之蒐集、處理，是否符合個資法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合個資法第七條之規定。
- 四、檢視一般個人資料之利用，是否符合個資法第二十條規定蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合個資法第七條之規定。
- 五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。
- 六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依個資法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。
- 七、進行個人資料國際傳輸前，檢視是否受金管會限制並遵循之。
- 八、當事人行使個資法第三條所定權利之相關事項：
 - (一)當事人身分之確認。

- (二)提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。
- (三)對當事人請求之審查方式，並遵守個資法有關處理期限之規定。
- (四)有個資法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。

九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依個資法第十一條第一項、第二項及第五項規定辦理。

十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依個資法第十一條第三項規定刪除、停止處理或利用。

第九條：本公司為維護所保有個人資料之安全，應採取下列資料安全管理措施：

- 一、訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。
- 二、針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。
- 三、作業過程有備份個人資料之需要時，對備份資料予以適當保護。

第十條：本公司如有提供電子商務服務系統，應採取下列資訊安全措施：

- 一、使用者身分確認及保護機制。
- 二、個人資料顯示之隱碼機制。
- 三、網際網路傳輸之安全加密機制。
- 四、應用系統於開發、上線、維護等各階段軟體驗證與確認程序。
- 五、個人資料檔案及資料庫之存取控制與保護監控措施。
- 六、防止外部網路入侵對策。
- 七、非法或異常使用行為之監控與因應機制。

前項所稱電子商務，係指透過網際網路進行有關商品或服務之廣告、行銷、供應、訂購或遞送等各項商業交易活動。

第一項第六款、第七款所定措施，應定期演練及檢討改善。

第十一條：本公司保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施：

- 一、實施適宜之存取管制。
- 二、訂定妥善保管媒介物之方式。
- 三、依媒介物之特性及其環境，建置適當之保護設備或技術。

第十二條：本公司為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與員工約定保密義務。

第四章 個人資料之安全稽核、紀錄保存及持續改善機制

第十三條：為確保本辦法之落實，本公司應依業務規模及特性，衡酌經營資源之合理分配，訂定適當之個人資料安全稽核機制，並將之列入本公司內部控制及稽核項目中。

第十四條：本公司執行本辦法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。
本公司依個資法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

- 一、刪除、停止處理或利用之方法、時間。
- 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

第十五條：為持續改善個人資料安全維護，各單位應每年提出相關自我評估報告，由個資小組彙整並檢視下列事項：

- 一、參酌法令增修、業務需求等因素，檢視、修訂本辦法相關個人資料保護事項。
- 二、針對評估報告中有違反法令之虞者，規劃、執行改善及預防措施。

前項自我評估報告並授權由總經理核定。

第五章 附則

第十六條：個資小組依本辦法研議之個人資料保護機制、程序、措施及相關規章之訂定或修正，授權總經理核定後施行或依本公司分層負責表所訂權限核定及處理。

第十七條：本辦法由稽核室辦理查核。

第十八條：本辦法應經董事會核定，修改時亦同。

103年2月25日第十二屆第21次董事會核定通過

103年12月16日第十二屆第31次董事會修正通過

105年8月15日第十三屆第16次董事會修正通過

111年2月24日第十五屆第8次董事會修正通過