臺灣金融控股股份有限公司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

103 年 3 月 27 日第 3 屆第 8 次董事會決議通過
104 年 3 月 19 日總經理核定修正
104 年 4 月 14 日總經理核定修正
105 年 5 月 26 日總經理核定修正
106 年 6 月 5 日總經理核定修正
107 年 12 月 6 日總經理核定修正
111 年 4 月 8 日總經理核定修正
(111 年 4 月 14 日金控法乙字第 11117400841 號通函)

第一章　總則

第一條　　臺灣金融控股股份有限公司(以下稱本公司)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」第三條規定，特訂定本方法。

第二條　本方法用詞，定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合；檔案形式包括實體紙本檔案及電子化檔案。

三、重大個人資料安全事故：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。

四、業務終止：指本公司停止部分業務、資產轉讓、與其他事業合併或解散等情形。

第二章　個人資料保護之規劃

第三條　　本公司應依個人資料保護相關法令，界定所保有個人資料納入本方法之範圍，並定期查核確認保管現況。

各單位應每年一次查核所屬業務之個人資料檔案清冊，列為自行查核之查核項目，由董事會稽核處實地查核各單位自行查核之辦理情形。

第四條　　本公司應依前條界定之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，根據「臺灣金融控股股份有限公司個人資料風險評估作業要點」執行風險評估之結果，採取適當之改善及預防措施。

第五條　　本公司因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故，應依「臺灣金融控股股份有限公司重大偶發事件危機處理須知」辦理。

本公司遇有重大個人資料安全事故者，事故發生單位應依「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」附件格式填具表單，簽奉總經理核定後通知法令遵循處通報金融監督管理委員會(以下稱金管會)。但於其他法令另有規定時，並應依各該法令之規定辦理。

前項通報作業，應於發現後七十二小時內完成，例假日均納入時效計算。

第六條　　本公司應對員工，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、責任範圍與各種個人資料保護事項之機制、程序及措施。

前項相關作業，由行政管理處負責對員工每年施以個人資料保護教育訓練，另法令遵循處於每半年辦理法令遵循自行評估作業時，納入法令遵循自評檢核表，由各單位進行認知宣導。

第三章　個人資料之管理程序及措施

第七條　　本公司各單位於執行業務時有蒐集、處理或利用個人資料之情形者，應就下列事項逐一檢視是否符合個人資料保護法（以下稱個資法）及相關法令之規定：

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、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。

六、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。

七、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。

八、當事人行使個資法第三條所定權利相關事項之處理程序：

（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。

前項程序，由各單位設置專責人員，於蒐集、處理、利用個人資料時，依照「臺灣金融控股股份有限公司個人資料蒐集、處理或利用標準作業流程(SOP)」辦理。

第八條　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。

前項管理措施，依本公司「資訊安全政策」、「資訊管理政策與指導原則」及「資訊作業管理辦法」及其他相關規定辦理。

第九條　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。

前項設備安全管理措施，依本公司「資訊安全政策」、「資訊管理政策與指導原則」及「資訊作業管理辦法」及其他相關規定辦理。

第十條　本公司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，並與所屬人員簽立保密書約定保密義務。

前項相關人員接觸個人資料之權限及控管其接觸情形之管理規範，除依本方法辦理外，並依本公司「資訊安全政策」、「資訊管理政策與指導原則」及「資訊作業管理辦法」及其他相關規定辦理。

第十一條　　本公司如有業務終止情事發生，除應注意遵守金融控股公司法及公司法等相關法令規定外，亦應遵循個人資料保護相關法令及本方法相關規定。

第四章　個人資料之安全稽核、紀錄保存、持續改善及應變演練機制

第十二條　　本公司應訂定適當之個人資料安全稽核機制，並應將相關機制列入內部控制及稽核項目。

前項相關機制，各業務管理單位應列入自行查核項目，董事會稽核處應列入內部稽核項目及督導業務管理單位辦理情形。

第十三條　　本公司執行本方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。

第一項及第二項管理機制，依本公司「資訊安全政策」、「資訊管理政策與指導原則」及「資訊作業管理辦法」及其他相關規定辦理。

第十四條　　本公司各單位每年一次進行自我評估後出具自我評估報告予風險管理處，由該處彙整後定期向風險管理委員會提出報告，並經本公司董事會決議或經其授權總經理核定。

第十五條　　本公司每年應辦理個人資料外洩應變演練一次，由法令遵循處於每年三月底前簽陳總經理核定當年度演練單位。

演練單位須擬具演練計畫、召開演練會議並辦理演練，演練結果應陳報法令遵循處，由該處簽報總經理。

前項演練計畫應包括演練目的、演練時間、演練單位（協辦單位）、演練內容。演練報告除包括演練計畫之項目外，另應包括演練情境、損失評估、應變措施、演練結果及檢討。

第五章　附則

第十六條　本方法經董事會通過後實施；修正時授權總經理核定後實施。