法規名稱：僑務委員會指定特定非公務機關個人資料檔案安全維護辦法
發布日期：民國 111 年 03 月 11 日

第 1 條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第 2 條

本辦法所稱特定非公務機關，指僑務委員會（以下簡稱本會）主管之財團法人，其業務項目有金融業務性質或其保有個人資料筆數達五千筆以上者。

第 3 條

1 特定非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正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（以下簡稱本計畫及處理方法）。

2 特定非公務機關應於本辦法施行之日起六個月內完成本計畫及處理方法之訂定；本辦法施行後，本會主管之財團法人應於符合前條規定之日起六個月內完成本計畫及處理方法之訂定。

3 特定非公務機關完成本計畫及處理方法之訂定，除業務項目有金融業務性質者外，如因刪除、銷毀或其他方式致所保有之個人資料筆數減少，且連續二年期間所保有之筆數未達五千筆者，得停止本計畫及處理方法全部或一部之執行。但嗣後因直接或間接蒐集致所保有之個人資料筆數達到五千筆以上時，應於保有筆數達到五千筆以上之日起三十日內恢復本計畫及處理方法全部之執行。

4 本計畫及處理方法之訂定、修正、停止及恢復，應經由特定非公務機關董（理）事會決議或經其授權之經理部門核定，並於核定日起三十日內送本會備查。

5 特定非公務機關經本會要求提出本計畫及處理方法實施情形者，應於收受通知後三十日內，以書面方式提出。

第 4 條

特定非公務機關應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。

第 5 條

特定非公務機關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，並根據風險評估之結果，訂定適當之管理機制。

第 6 條

1 特定非公務機關為因應業務上所保有個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及預防機制：

一、事故發生後應採取之各類措施：

（一）控制當事人損害之方式。

（二）查明事故後通知當事人之適當方式。

（三）應通知當事人事故事實、所為因應措施及諮詢服務專線等內容。

二、事故發生後應受通報之對象及其通報方式。

三、事故發生後其矯正預防措施之研議機制。

2 特定非公務機關遇有前項事故者，應於發現後七十二小時內通報本會，未於時限內通報者應附延遲理由（通報格式如附件）。通報內容包括：

一、特定非公務機關名稱、通報人及聯絡方式。
二、通報時間及事件發生時間。
三、事件發生種類、個人資料類型、預估個人資料侵害總筆數、發生原因、損害狀況、個人資料侵害可能結果。
四、擬採取之因應措施、擬採通知當事人之時間及方式。

3 本會接受通報後，得依據本法第二十二條至第二十五條規定，爲適當之監督管理措施。

4 第一項特定非公務機關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。

第 7 條

特定非公務機關應定期對所屬人員，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、所屬人員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 8 條

1 特定非公務機關應就下列事項，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本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，並應確保符合本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，是否符合免爲告知之事由，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，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條之規定。
四、檢視一般個人資料之利用，是否符合本法第二十條規定蒐集之特定目的必要範圍；其爲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，並應確保符合本法第七條之規定。
五、利用個人資料爲行銷，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，對受託人依本法施行細則第八條規定爲適當之監督，並於委託契約或相關文件中，明確約定其內容。
七、對個人資料國際傳輸前，應檢視本會有無依本法第二十一條規定所爲之限制且遵循之，並告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方爲下列事項之監督：
（一）預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。
（二）當事人行使本法第三條所定權利之相關事項。
八、當事人行使本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，並遵守本法有關處理期限之規定。
（四）有本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，應依本法第十一條第一項、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，應依本法第十一條第三項規定刪除、停止處理或利用。

2 前項第七款之規定，特定非公務機關將個人資料作國際傳輸，如有本法第二十一條第一款至第四款情形，本會得限制傳輸。

第 9 條

特定非公務機關爲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 10 條

1 特定非公務機關使用資通訊系統蒐集、處理或利用個人資料，而保有消費者交易、使用商品或接受服務等過程之一般或特種個人資料，且具對外電子商務服務系統者，應採取下列資料安全管理措施：

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、個人資料檔案及資料庫之存取控制與保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行爲之監控與因應機制。

2 前項所稱電子商務，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 11 條

特定非公務機關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 12 條

特定非公務機關爲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，並與所屬人員約定保密義務。

第 13 條

特定非公務機關爲確保本計畫及處理方法之落實，應依其業務規模及特性，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；其依法令規定應建立內部控制及稽核制度者，並應將相關機制列入內部控制及稽核項目。

第 14 條

1 特定非公務機關執行本計畫及處理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。

2 特定非公務機關依本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。

3 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 15 條

1 特定非公務機關爲持續改善個人資料安全維護，其所屬個人資料管理單位或人員，應定期提出相關自我評估報告，檢視、修訂本計畫及處理方法等相關個人資料保護事項；並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。

2 前項自我評估報告，應經特定非公務機關董（理）事會決議或經其授權之經理部門核定

，並於核定日起三十日內送本會備查。

第 16 條

本辦法自發布日施行。