# 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

| 條　　文 | 說　　明 |
| --- | --- |
| 第一章　　總則 | 章名 |
| 第一條　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。 | 明定本辦法訂定之依據。 |
| 第二條　本辦法所稱非公務機關,包括下列各款：<br>一、金融控股公司。<br>二、銀行業。<br>三、證券業。<br>四、期貨業。<br>五、保險業。<br>六、電子票證業。<br>七、其他經金融監督管理委員會(以下簡稱本會)公告之金融服務業。<br>八、本會主管之財團法人。<br>前項第一款所稱金融控股公司,依金融控股公司法第四條第一項第二款之規定。<br>第一項第二款至第五款所稱銀行業、證券業、期貨業及保險業之範圍,依金融監督管理委員會組織法第二條第三項規定。但不包括依信用合作社法第十條規定組織之全國性信用合作社聯合社。<br>第一項第六款所稱電子票證業,指電子票證發行管理條例第三條第二款之發行機構。<br>第一項第八款所稱本會主管之財團法人，依金融監督管理委員會主管財團法人監督管理要點第二點規定。 | 一、明定本辦法之適用範圍，包括本會主管之各金融服務業及財團法人等非公務機關。<br>二、又各該金融服務業組成之商業團體，其個人資料保護法目的事業主管機關為內政部;信用合作社依法組織之全國性信用合作社聯合社,目前係以維護社員社之權益與輔導社員社之業務發展為主要工作，爰均無本辦法之適用。 |
| 第二章　　個人資料保護之規劃 | 章名 |
| 第三條　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 | 一、配合本法施行細則第十二條第二項第一款之規定,非公務機關為落實個人資料 |

| | |
|---|---|
| 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)。<br>本計畫及處理方法之訂定或修正，應經非公務機關董(理)事會、常務董(理)事會決議或經其授權之經理部門核定。但非公務機關為外國在臺分行、分公司，或未設董(理)事會者，應經其負責人簽署。 | 保護目的，應考量組織規模與保有個人資料之數量或內容，依比例原則建立技術上及組織上之措施，俾規劃、訂定、修正與執行本計畫及處理方法之相關事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。<br>二、關於本計畫及處理方法之訂定或修正，是否須經非公務機關之董(理)事會等決議，或經其授權之經理部門核定，本法及施行細則未有明文，爰於本條第二項明定之，以利遵循。另考量本辦法適用範圍甚廣，如保險經紀人、保險代理人等業，尚有個人執業情形；外國金融服務業在臺分行、分公司，其組織亦未必與本國業者相同，此等非公務機關訂定或修正本計畫及處理方法，自不適用上開決議方法，爰參考金融控股公司及銀行業內部控制及稽核制度實施辦法，規定應經其負責人簽署，併此敘明。 |
| 第四條　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。 | 配合本法施行細則第十二條第二項第二款之規定，非公務機關規劃、訂定本計畫及處理方法，應界定個人資料之範圍，亦即定期查核確認所保有之個人資料現況，並依個人資料保護相關法令確認是否納入，俾利後續風險評估作業之進行。又所稱個人資料保護相關法令，解釋上包括非公務機關執行業務所應適用之各種法令，不以本法及本法施行細則為限。 |
| 第五條　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。 | 配合本法施行細則第十二條第二項第三款之規定，非公務機關應依據前條所界定適用本計畫及處理方法之個人資料範圍，及相關業務流程，評估於蒐集、處理、利用之過程中，個人資料可能遭遇之危險及危險性之高低，於本計畫及處理方法訂定適當之管理機制。 |
| 第六條　非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定下列應變、通報及預防機 | 一、配合本法施行細則第十二條第二項第四款，明定應於本計畫及處理方法中訂定之個人資料安全事故應變、通報及預防 |

| | |
|---|---|
| 制：<br>一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。<br>二、事故發生後應受通報之對象及其通報方式。<br>三、事故發生後，其矯正預防措施之研議機制。<br>非公務機關遇有重大個人資料安全事故者，應即通報本會；其所研議之矯正預防措施，並應經公正、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。<br>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，將危及非公務機關正常營運或大量當事人權益之情形。 | 機制。<br>二、按事故應變之首要目標，係根據事故之類型，採取應變措施降低或控制當事人損害之範圍，並儘速依本法第十二條、本法施行細則第二十二條等規定通知當事人。爰於第一款規定本計畫及處理方法之應變措施，應包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。<br>三、次按非公務機關如發生個人資料遭竊、外洩等事故，為使有關機關、單位及時掌握情況，自應以適當方式通報。為利執行，宜將此等通報對象及通報方式，一併明定於本計畫及處理辦法中，爰為第二款之規定。<br>四、再按避免類似事故重複發生，亦為應變措施之重點，爰於第一項第三款規定本計畫及處理方法，應明定事故發生後矯正預防措施之研議機制。<br>五、末按非公務機關如遭遇重大個人資料安全事故而危及其正常營運或多數當事人權益，應採取較一般事故更嚴密之應變及預防措施，爰於第四項明定應通報本會；其依第一項第三款所研議之矯正預防措施，亦須視事故發生原因、規模等，由公正、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，儘速研議完成。另參酌「銀行業通報重大偶發事件之範圍與適用對象」及「保險業通報重大偶發事件之範圍與適用對象」相關規定，於第三項明定重大個人資料事故之定義。 |
| 第七條　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。 | 一、配合本法施行細則第十二條第二項第七款之規定，非公務機關應透過認知宣導及教育訓練，使所屬人員均能明瞭個人資料保護相關法令之要求、所應負擔之責任範圍及相關機制、程序及措施，俾本計畫及處理方法得以落實。 |

| | |
|---|---|
| | 二、又本辦法所規定應列入本計畫及處理方法者，包括第二章至第四章之各類「機制」、「程序」、「措施」等，均應透過認知宣導及教育訓練使非公務機關所屬人員明瞭。為求其範圍明確及用語一致，爰將機制、程序、措施等明定於本條，併此敘明。 |
| 第三章　個人資料之管理程序及措施 | 章名 |
| 第八條　非公務機關應就下列事項，訂定個人資料之管理程序：<br>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。<br>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。<br>三、檢視個人資料之蒐集、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；其經當事人書面同意者，並應確保符合本法第七條第一項之規定。<br>四、檢視個人資料之利用，是否符合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，經當事人書面同意者，並應確保符合本法第七條第二項之規定。<br>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。<br>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。 | 一、配合本法施行細則第十二條第二項第五款之規定，明定非公務機關應依本辦法將其個人資料蒐集、處理及利用之內部管理程序，明定於本計畫及處理方法中，包括：檢視一般或特種個人資料之蒐集、處理或利用是否符合法定要件；當事人拒絕行銷之處置；對受託人之監督事項；遵守本會所為國際傳輸之限制；當事人行使權利之處理；個人資料正確性之維護；個人資料之刪除等事項。<br>二、另本條第七款所謂國際傳輸受本會限制之情形，依本法第二條第六款之規定，係指本會針對非公務機關將個人資料作跨國(境)處理或利用之各種限制，例如現行金融機構作業委託他人處理內部作業制度及程序辦法第十八條第四項、第五項，及保險業作業委託他人處理應注意事項第三點等規定，尚不限於依本法第二十一條各款所為之命令或處分。 |

| | |
|---|---|
| 七、進行個人資料國際傳輸前，檢視是否受本會限制並遵循之。<br>八、當事人行使本法第三條所定權利之相關事項：<br>(一)當事人身分之確認。<br>(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。<br>(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。<br>(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。<br>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。<br>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。 | |
| 第九條　非公務機關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：<br>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。<br>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。<br>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。 | 一、依本法第二十七條第一項之規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。爰配合本法施行細則第十二條第二項第六款，明定非公務機關應於本計畫及處理方法中，訂定資料安全管理之相關措施。<br>二、非公務機關使用各類設備或儲存媒體，蒐集、處理或利用個人資料，應訂定相關使用規範，以確保資料安全，其報廢或轉作他用時亦同，爰為第一款之規定。<br>三、針對本法第二條第四款所定個人資料處理行為之各種態樣，如非公務機關評估有加密之必要，應採取適當之加密措 |

| | |
|---|---|
| | 施，爰為第二款之規定。<br>四、依本法施行細則第五條之規定，本法第二條第二款所定個人資料檔案，包括備份檔案。準此，非公務機關針對複製、備份之個人資料檔案，亦應有適當之保護措施，爰為第三款之規定。 |
| 第十條　非公務機關提供電子商務服務系統，應採取下列資訊安全措施：<br>一、使用者身分確認及保護機制。<br>二、個人資料顯示之隱碼機制。<br>三、網際網路傳輸之安全加密機制。<br>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。<br>五、個人資料檔案及資料庫之存取控制與保護監控措施。<br>六、防止外部網路入侵對策。<br>七、非法或異常使用行為之監控與因應機制。<br>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。<br>第一項第六款、第七款所定措施，應定期演練及檢討改善。 | 一、目前各類非公務機關，經常提供電子商務服務系統，以促進交易效率。考量網際網路對於個人資料安全之潛在風險，其提供此等系統，不論目的為營利（例如網路銀行、網路下單）或非營利（例如證券櫃檯買賣中心建置交易系統、訓練機構販售學習點數或收取報名費用），均須採行相關個人資料安全保護措施，包括：系統使用者之身分確認、個人資料顯示之隱碼去識別化機制、網際網路傳輸之安全加密、系統正常運作之驗證與確認、系統中個人資料檔案及資料庫之存取控制與保護監控、防範外部網路入侵及其他非法或異常使用等，並將相關內容明定於本計畫及處理方法中，爰為本條第一項規定。另參酌行政院發布之「電子商務消費者保護綱領」，明定電子商務之定義於第二項。<br>二、非公務機關提供之電子商務系統因外部網路入侵、非法或異常使用等人為因素，往往導致大量個人資料外洩、毀損，及當事人其他權益損害。為使系統遭遇各類資安事故時，能儘速恢復正常並控制損害，非公務機關除依本條第一項規定採取相關措施，並依本辦法第十五條進行自我評估外，亦宜針對其中防範非法入侵或異常使用等應變措施定期進行演練，爰為第三項之規定。 |
| 第十一條　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 | 非公務機關用以保存個人資料之各類媒介物，其接近使用及安全維護與個人資料保護息息相關，爰配合本法施行細則第十二條第 |

| | |
|---|---|
| 器設備或其他媒介物者，應採取下列設備安全管理措施：<br>一、實施適宜之存取管制。<br>二、訂定妥善保管媒介物之方式。<br>三、依媒介物之特性及其環境，建置適當之保護設備或技術。 | 二項第八款，明定非公務機關應於本計畫及處理方法中，訂定設備安全管理之相關措施。 |
| 第十二條　非公務機關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，並與所屬人員約定保密義務。 | 配合本法施行細則第十二條第二項第六款，明定非公務機關應於本計畫及處理方法中，訂定人員管理之相關措施，亦即依所屬人員負責業務之內容、性質等，設定其接觸個人資料之適當權限，就實際接觸情形予以控管，並與其約定保密義務以確保履行。 |
| 第四章　　個人資料之安全稽核、紀錄保存及持續改善機制 | 章名 |
| 第十三條　非公務機關為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。 | 非公務機關為落實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，應依其業務規模及特性，依比例原則建置內部個人資料安全稽核機制，定期查察執行情況，以符合相關法令規定。爰配合本法施行細則第十二條第二項第九款，規定非公務機關應於本計畫及處理方法中，訂定個人資料安全稽核機制，並將之列入內部控制及稽核項目。惟其他法令並未要求非公務機關制定內部控制及稽核制度者，自不在此限。 |
| 第十四條　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。<br>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：<br>一、刪除、停止處理或利用之方法、時間。<br>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。<br>前二項之軌跡資料、相關證據及紀 | 一、非公務機關為證明已落實本計畫及處理方法所定之機制、程序及措施，並釐清個人資料於蒐集、處理或利用過程之相關權責，應就個人資料使用情況、軌跡資料等建立保存機制。爰配合本法施行細則第十二條第二項第十款，於第一項規定非公務機關應於本計畫及處理方法中，訂定相關紀錄、證據保存機制。<br>二、非公務機關業務終止後，亦即特定目的消失或期限屆滿後，原則上應依本法第十一條第三項之規定刪除、停止處理或利用相關個人資料，惟其是否實際刪除、停止處理或利用，當事人往往無從得知。為預防不必要之紛爭，爰於第二 |

| | |
|---|---|
| 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。 | 項明定非公務機關刪除、停止處理或利用所保有之個人資料後，應留存相關紀錄。又非公務機關雖將所保有之個人資料刪除，仍可能於刪除前將其備份資料移轉他人，爰於本項第二款併予規定，以求周延。<br>三、按本法第二十九條針對非公務機關之損害賠償責任，設有推定過失之規定；本會作為其目的事業主管機關，亦得依同法二十二條為行政檢查，或依第四十七條至第五十條等規定為行政裁罰。為督促非公務機關留存相關文件紀錄，俾利舉證及備供本會檢查，爰參酌本法第三十條之時效期間，規定相關證明文件紀錄應至少留存五年。惟如有其他法令規定或契約約定之保存期間，不論是否較本辦法所定期間為短，均從其規定或約定，併此敘明。 |
| 第十五條　非公務機關為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，並訂定下列機制：<br>一、檢視、修訂本計畫及處理方法等相關個人資料保護事項。<br>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。<br>前項自我評估報告，應經非公務機關董(理)事會、常務董(理)事會決議或經其授權之經理部門核定。但非公務機關為外國在臺分行、分公司，或未設董(理)事會者，應經其負責人簽署。 | 一、非公務機關應定期自我評估個人資料安全維護之執行情形，提出相關報告，並參酌法令增修、業務需求等客觀因素，俾持續改善其個人資料安全維護運作。爰配合本法施行細則第十二條第二項第十一款，於第一項規定非公務機關應於本計畫及處理方法中，訂定持續改善相關機制。<br>二、為使非公務機關之經營管理階層定期瞭解、掌握其個人資料安全維護情形，並配合修訂本計畫及處理方法，爰於第二項規定自我評估報告應經董(理)事會等決議或核定。另考量本辦法適用範圍甚廣，如非公務機關係未設董(理)事會之自然人、非法人團體、外國金融服務業在臺分行、分公司，其自我評估報告之審查，自毋庸依前開方式辦理，惟仍應依前項規定定期執行自我評估並留存相關文件紀錄，併此敘明。 |
| 第五章　　附則 | 章名 |

| | |
|---|---|
| 第十六條　本辦法自發布日施行。 | 明定本辦法之施行日期。 |