法規名稱：內政部指定營建類非公務機關個人資料檔案安全維護管理辦法

發布日期：民國 110 年 11 月 30 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

本辦法所稱主管機關，在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第 3 條

1 本辦法所稱非公務機關，包括下列各款：

一、營造業。

二、不動產開發業。

三、建築師事務所。

四、公寓大廈管理維護公司。

五、都市更新業務財團法人。

六、其他經中央主管機關公告指定者。

2 前項第二款不動產開發業，指以銷售為目的，從事土地、建物等不動產投資興建之行業。

第 4 條

1 非公務機關應訂定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），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

2 非公務機關依前項規定訂定本計畫及處理方法時，應視其業務規模、特性、保有個人資料之性質及數量等事項，參酌第五條至第二十三條規定，訂定包含下列各款事項之適當安全維護管理措施；必要時，第二款各目事項得整併之：

一、非公務機關之組織規模及特性。

二、個人資料檔案之安全管理措施：

（一）配置管理之人員及相當資源。

（二）界定蒐集、處理及利用個人資料之範圍。

（三）個人資料之風險評估及管理機制。

（四）事故之預防、通報及應變機制。

（五）個人資料蒐集、處理及利用之內部管理程序。

（六）設備安全管理、資料安全管理及人員管理措施。

（七）認知宣導及教育訓練。

（八）個人資料安全維護稽核機制。

（九）使用紀錄、軌跡資料及證據保存。

（十）個人資料安全維護之整體持續改善。

（十一）業務終止後之個人資料處理方法。

3 第一項之本計畫及處理方法，都市更新業務財團法人應於主管機關許可設立之日起六個月內報請其主管機關備查，其餘非公務機關應於開業或完成營業項目登記之日起六個月內，報請主事務所所在地之直轄市、縣（市）主管機關備查。

4 中央主管機關依前條第一項第六款公告指定前，已完成開業、營業項目登記或財團法人許可設立者，應於公告指定之日起六個月內，將第一項之本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

第 5 條

1 非公務機關應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並定期向負責人提出報告。

2 非公務機關應訂定個人資料保護管理政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於營業處所或主事務所適當之處；如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉。

第 6 條

非公務機關應界定納入本計畫及處理方法之個人資料範圍，辦理下列事項：

一、定期清查保有之個人資料現況。

二、確認保有之個人資料所應遵循適用之個人資料保護相關法令現況。

第 7 條

非公務機關應依前條已界定之個人資料範圍及蒐集、處理、利用個人資料之流程，評估可能產生之風險，並根據風險評估之結果，依風險等級訂定適當之管控措施。

第 8 條

非公務機關為因應保有之個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），應採取下列應變、通報及預防機制：

一、採取適當之應變措施，以控制個人資料事故對當事人之損害，並通報內部有關單位。

二、查明個人資料事故之狀況並以適當方式通知當事人有關個人資料事故事實、所為因應措施及諮詢服務專線等內容。

三、研議預防機制，避免類似個人資料事故再次發生。

第 9 條

1 非公務機關依前條第一款通報者為重大個人資料事故，應於發現後七十二小時內，將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現事故後立即通報等事項，以書面通報主事務所所在

地之直轄市、縣（市）主管機關或財團法人主管機關；如為直轄市、縣（市）主管機關接獲通報，並應副知中央主管機關（書面通報格式如附件）。

2 前項所稱重大個人資料事故，指個人資料被竊取、竄改、毀損、滅失或洩漏達一千筆以上，將危及非公務機關正常營運或大量當事人權益之情形。

3 主管機關接獲通報或主動知悉事故，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。

第 10 條

非公務機關所屬人員對於個人資料蒐集、處理及利用，應注意下列事項：

一、屬本法第六條所定特種個人資料者，應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，應符合本法第七條第一項、第二項及第四項規定。

二、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要件。其經當事人同意者，應符合本法第七條第一項、第三項及第四項規定。

三、檢視一般個人資料之利用，是否符合本法第二十條規定，於蒐集之特定目的必要範圍內為之；特定目的外之利用，是否符合本法第二十條第一項但書規定。其經當事人同意者，應符合本法第七條第二項及第四項規定。

四、利用個人資料為行銷，當事人表示拒絕行銷後，立即停止利用其個人資料行銷，且周知所屬人員，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。

五、於蒐集、處理或利用過程中，檢視個人資料是否正確，有不正確時，應主動更正或補充。其正確性有爭議者，應依本法第十一條第二項規定辦理。

第 11 條

非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第 12 條

1 中央主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。

2 非公務機關將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：

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。

第 13 條

非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

一、提供聯絡窗口及聯絡方式。

二、確認為個人資料當事人本人，或經其委託者。

三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。

四、有收取必要成本費用者，應告知當事人收費基準。

五、遵守本法第十三條有關處理期限之規定。

第 14 條

非公務機關為維護所保有個人資料之安全，使用存有個人資料之各類設備或儲存媒體，應採取下列資料安全管理措施：

一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定各類設備或儲存媒體之使用規範。

二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

三、作業過程有備份個人資料之需要時，該備份資料比照原件，依本法規定予以保護之。

四、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，於報廢、汰換或轉作其他用途時，應採適當防範措施，以避免由該媒介物洩漏個人資料；委託他人執行者，非公務機關對受託人之監督依第二十二條規定辦理。

第 15 條

1 非公務機關使用資通訊系統蒐集、處理或利用個人資料，且其資料庫保有個人資料數量達五千筆以上者，應採取下列措施：

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、個人資料檔案與資料庫之存取控制及保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行為之監控及因應機制。

2 前項第五款及第六款所定措施，應定期演練及檢討改善。

第 16 條

1 非公務機關對保有個人資料之環境及實體設備安全，應採取下列措施：

一、依據作業內容之不同，實施適宜之進出管制方式。

二、訂定媒介物之管制方式，並檢視其保管情形。

三、針對不同媒介物存在之環境，建置適度之保護設備或技術。

2 前項所稱環境，指第十四條所定各類設備、儲存媒體或媒介物之存放區域。

第 17 條

1 非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。

2 前項管理措施，應包括下列事項：

一、依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

三、要求所屬人員妥善保管存有個人資料之媒介物，並約定保管及保密義務。

四、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

第 18 條

非公務機關應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍、各種個人資料保護事項之作業程序及應遵守之相關管理措施。

第 19 條

1 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，訂定個人資料安全維護稽核機制，並指定適當人員每半年至少進行一次本計畫及處理方法執行情形之檢查。

2 前項檢查結果應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。

3 非公務機關依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。

第 20 條

1 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 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、時間或地點。

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、地點，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 21 條

非公務機關應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必要時予以修正；修正時，應於十五日內將修正後之本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

第 22 條

1 非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第

八條規定為適當之監督。

2 非公務機關為執行前項監督，應與受託人明確約定相關監督事項及方式。

第 23 條

非公務機關業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年：

一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

第 24 條

本辦法發布施行前，未訂定本計畫及處理方法之非公務機關，應依本辦法規定訂定，並於本辦法發布施行日起六個月內，將本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

第 25 條

本辦法自發布日施行。