

內政部指定政黨及全國性民政財團法人個人資料檔案安全維護管理辦法總說明

個人資料保護法（以下簡稱本法）第二十七條規定：「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。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」鑑於政黨及全國性民政財團法人屬內政部業管之非公務機關，為事務運作需要，經手管理相關個人資料，為防止個人資料被竊取、竄改、毀損、滅失或洩漏，其對所保有之個人資料檔案應採行適當之安全措施，爰依本法第二十七條第三項規定授權，並參酌本法施行細則第十二條規定，訂定「內政部指定政黨及全國性民政財團法人個人資料檔案安全維護管理辦法」（以下簡稱本辦法），以資上開政黨及法人遵循，其要點如下：

- 一、本辦法之訂定依據。（第一條）
- 二、本辦法之主管機關。（第二條）
- 三、本辦法之適用對象。（第三條）
- 四、政黨及全國性民政財團法人應訂定個人資料檔案安全維護計畫及解散或被廢止備案後之個人資料處理方法（以下簡稱本計畫及處理方法）、訂定內容及訂定時限。（第四條）
- 五、政黨及全國性民政財團法人應配置適當管理人員及提供相當資源，以執行本計畫及處理方法，及公告個人資料保護管理政策等事項。（第五條）
- 六、個人資料之範圍界定及個人資料檔案現況之盤點、業務流程之風險分析與管控，及相關侵害事故之應變等事項。（第六條至第八條）
- 七、政黨及全國性民政財團法人之成員蒐集、處理及利用個人資料之規範、政黨及全國性民政財團法人所蒐集持有及應遵守告知義務等事項。（第九條及第十條）
- 八、政黨及全國性民政財團法人國際傳輸個人資料時應遵循事項。（第十一條）

- 九、政黨及全國性民政財團法人對於當事人行使本法第三條規定之權利時採取之措施。(第十二條)
- 十、政黨及全國性民政財團法人對所保管之個人資料檔案應採取必要適當之防護設施，並應對其成員有適度之管理措施。(第十三條及第十四條)
- 十一、政黨及全國性民政財團法人使用資通訊系統蒐集、處理或利用個人資料時應採取之資訊安全措施。(第十五條)
- 十二、政黨及全國性民政財團法人應定期或不定期對其成員進行教育宣導。(第十六條)
- 十三、本計畫及處理方法之稽核、使用紀錄留存、檢討改善等事項。(第十七條至第十九條)
- 十四、政黨及全國性民政財團法人委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。(第二十條)
- 十五、政黨及全國性民政財團法人解散或被廢止備案後所保有個人資料之處理方式。(第二十一條)
- 十六、本辦法施行前之政黨及全國性民政財團法人，應訂定本計畫及處理方法，並於一定期間報備查。(第二十二條)
- 十七、本辦法施行日期。(第二十三條)

內政部指定政黨及全國性民政財團法人個人資料檔案安全維護管理辦法

條文	說明
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。	本辦法訂定依據。
第二條 本辦法所稱主管機關為內政部。	本辦法主管機關。
第三條 本辦法所稱全國性民政財團法人，包括下列各款全國性財團法人： 一、依財團法人法或其他法令規定許可設立，其捐助章程所定法人名稱、目的及業務項目，以民政業務為主，並以內政部為主管機關者。 二、於財團法人法施行前，以推動內政相關業務為目的，從事民政業務服務，經內政部許可設立者。 三、依二二八事件處理及賠償條例設立者。 財團法人祭祀公業及宗教財團法人，不適用本辦法有關全國性民政財團法人之規定。	一、第一項定明本辦法有關全國性民政財團法人規定適用範圍。 二、符合第一項第二款規定之全國性民政財團法人，計有財團法人凱達格蘭基金會、財團法人李登輝基金會、財團法人民族基金會、財團法人民權基金會、財團法人國家發展基金會及財團法人中華民族發展基金會；至於財團法人二二八事件紀念基金會，則為第一項第三款指涉對象。 三、財團法人祭祀公業及宗教財團法人之個人資料檔案安全維護管理相關辦法另定之，爰於第二項定明上開財團法人不適用本辦法。
第四條 政黨及全國性民政財團法人應訂定個人資料檔案安全維護計畫及解散或被廢止備案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。 政黨及全國性民政財團法人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，參酌第五條至第二十一條規定，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、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。	一、第一項定明政黨及全國性民政財團法人訂定個人資料檔案安全維護計畫及解散或被廢止備案後個人資料處理方法之義務。 二、由於政黨及全國性民政財團法人大小規模不一，尚難作統一規範，爰參照本法施行細則第十二條第二項規定意旨，所採行之安全措施與所欲達成之個人資料保護目的間，具有適當比例為原則。爰第二項規定得參酌其規模、特性、保有個人資料之性質及數量等事項，參考第五條至第二十一條及本法施行細則第十二條第二項規定，訂定適宜並符合比例原則之安全措施，據以執行。 三、考量政黨及全國性民政財團法人組織成立初期對個人資料保護之執行與行政機關規定熟悉度較低，爰第二項明定訂定計畫時應

(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)解散或被廢止備案後之個人資料處理方法。 第一項之本計畫及處理方法，政黨應於主管機關同意備案日起六個月內、全國性民政財團法人應於主管機關許可設立日起六個月內，報請主管機關備查。	包括之事項，並保留彈性空間，政黨及全國性民政財團法人得依個別情況，於必要時整併第二項第二款各目之相關事項。 四、第三項明定政黨及全國性民政財團法人應於主管機關同意備案或許可設立後六個月內訂定計畫及處理方法，並應報請主管機關備查。
第五條 政黨及全國性民政財團法人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。 政黨及全國性民政財團法人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，公告於主事務所及分支機構等適當之處；如有網站者，並揭露於網站首頁，使其成員及個人資料當事人均能知悉。	第一項定明政黨及全國性民政財團法人規劃、訂定、修正、執行本計畫及處理方法之具體方式，另於第二項規定其應訂定個人資料保護管理政策與揭露蒐集、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之義務。
第六條 政黨及全國性民政財團法人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。	定明政黨及全國性民政財團法人應定期查核確認所保有之個人資料現況，並界定其納入本計畫及處理方法之範圍之義務。
第七條 政黨及全國性民政財團法人應依前條界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管控機制。	定明政黨及全國性民政財團法人評估個人資料風險，並根據風險評估之結果訂定適當管控機制之義務。
第八條 政黨及全國性民政財團法人為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），應訂定下列應變、通報及預防機制：	一、第一項定明政黨及全國性民政財團法人訂定個人資料安全事故之應變、通報及預防機制之義務。 二、第二項考量現行政黨及全國性民政財團法人組織規模，定明政黨

一、個人資料事故發生後應採取之各類措施，包括： (一)控制當事人損害之方式。 (二)查明個人資料事故後通知當事人之適當方式。 (三)應通知當事人個人資料事故事實、所為因應措施及諮詢服務專線等內容。 二、個人資料事故發生後應受通報之對象及其通報方式。 三、個人資料事故發生後，其矯正預防措施之研議機制。 政黨及全國性民政財團法人遇有達一千筆以上之個人資料事故時，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、是否於發現個人資料外洩後立即通報等事項，以書面通報主管機關（書面通報格式如附件）。 主管機關對於重大個人資料事故，得依本法第二十二條規定對政黨及全國性民政財團法人之應變、通報及預防機制進行實地檢查，並視檢查結果為後續處置。	及全國性民政財團法人遇有達一千筆以上之個人資料被竊取、洩漏、竄改或其他侵害之重大個人資料事故時，負通報義務。並依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，定明事故通報時點及應通報事項。 三、為調查事故發生後，是否係政黨及全國性民政財團法人所採取保護安全措施不足導致，第三項定明主管機關對於重大個人資料事故得採取之措施及後續行政檢查規定。
第九條 政黨及全國性民政財團法人之成員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。	定明政黨及全國性民政財團法人成員執行業務蒐集一般個人資料時，應遵守相關法定要件及程序。
第十條 政黨及全國性民政財團法人蒐集個人資料，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，要求其成員確實辦理。	定明政黨及全國性民政財團法人蒐集、處理及利用個人資料時應遵循之程序；並要求政黨及全國性民政財團法人應區分個人資料蒐集方式為直接蒐集或間接蒐集，分別訂定告知之方法、內容及相關注意事項，以便其成員在辦理業務時能據以執行。
第十一條 主管機關依本法第二十一條規定，對政黨及全國性民政財團法人為限制國際傳輸個人資料之命令或處分時，	一、第一項定明主管機關依本法第二十一條規定所為之命令或處分，政黨及全國性民政財團法人應通知團體成員知曉並遵照辦理。

政黨及全國性民政財團法人應通知其成員遵循辦理。 政黨及全國性民政財團法人將個人資料作國際傳輸者，應檢視是否受主管機關限制，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。	二、第二項定明政黨及全國性民政財團法人將個人資料作國際傳輸者，應檢視是否受主管機關依本法第二十一條規定之命令或處分限制，並且告知個人資料所欲國際傳輸之區域，同時對資料接收方為相關之監督。
第十二條 政黨及全國性民政財團法人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，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規定。	定明政黨及全國性民政財團法人於個人資料當事人行使本法第三條所定權利時應辦理之事項。
第十三條 政黨及全國性民政財團法人對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。 前項安全設備或防護措施，應包含下列事項： 一、紙本資料檔案之安全保護設施。 二、電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。 三、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，其對受託者之監督依第二十條規定辦理。	第一項定明政黨及全國性民政財團法人對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施，並於第二項規定該等設備或措施應包含事項。

第十四條 政黨及全國性民政財團法人為確實保護個人資料之安全，應對其成員採取適度管理措施。 前項管理措施，應包含下列事項： 一、依據業務需求，適度設定成員不同之權限，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、要求成員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。 四、成員異動或離職時，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。	第一項定明政黨及全國性民政財團法人為確實保護個人資料之安全，應對其成員採取之適度管理措施，並於第二項規定該等措施應包含事項。
第十五條 政黨及全國性民政財團法人使用資通訊系統蒐集、處理或利用個人資料達一萬筆以上者，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、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。 前項第五款及第六款所定措施，應定期演練及檢討改善。	一、第一項定明保有個人資料筆數達一萬筆以上之政黨及全國性民政財團法人應訂定個人資料安全事故之應變、通報及預防機制之義務。另參照行政院資通安全處建議，至少應採取下列資訊安全措施，以落實保護個人資料： (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及(六)非法或異常使用行為之監控與因應機制等六項資料安全管理措施，以落實保護個人資料。參考資通安全責任等級分級辦法附表十資通系統防護基準，針對六項資訊安全措施之實作說明如下： (一)系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除程序，並執行身分驗證管理，如身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。

	(二) 系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考 CNS 二九一九一「資訊技術—安全技術—部分匿名及部分去連結鑑別之要求事項」國家標準。 (三) 個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗證且未遭破解之演算法。 (四) 儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身分管理，並採用最小權限原則進行存取控制管理。 (五) 針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統，及應用程式防火牆等。 (六) 針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。 二、隨網路科技進步，個人資料遭外部網路入侵或非法或異常使用行為損害情形層出不窮，爰第二項規定針對第一項第五款及第六款所定措施，政黨及全國性民政財團法人應定期進行演練及檢討改善。
第十六條 政黨及全國性民政財團法人應定期或不定期對於成員施以基礎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、成員之責任範圍與各種個人資料保護事項之機制、程序及措	定明政黨及全國性民政財團法人應定期或不定期對其成員施以認知宣導或教育訓練，以使成員能充分認知個人資料保護相關法令及責任範圍，避免發生違法情事。

施。	
第十七條 政黨及全國性民政財團法人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。 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。 政黨及全國性民政財團法人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。	第一項定明政黨及全國性民政財團法人執行個人資料安全維護稽核機制之方法，並於第二項及第三項規範相關配套措施。
第十八條 政黨及全國性民政財團法人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。 政黨及全國性民政財團法人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。 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定者，不在此限。	第一項定明政黨及全國性民政財團法人應記錄其個人資料使用情況，並留存軌跡資料或相關證據；另於第二項規定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時，亦應留存相關紀錄；且於第三項規範上述軌跡資料、相關證據及紀錄，除法令另有規定者外，應至少留存五年。
第十九條 政黨及全國性民政財團法人應隨時參酌業務及本計畫及處理方法執行狀況、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管機關備查。	由於科技發展不斷進步，社會活動型態亦隨時改變，爰規定政黨及全國性民政財團法人應注意媒體對個人資料侵害或保護事件相關報導，並配合個人資料保護法令之訂修，隨時檢討所訂計畫。如有不合時宜之處，應立即修正計畫，以落實保護個人資料。
第二十條 政黨及全國性民政財團法人委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定為適當監督。 政黨及全國性民政財團法人為執行	依本法施行細則第八條之規定，委託他人蒐集、處理或利用個人資料時，委託者應為適當之監督，避免受託者有違反本法情事發生。是以政黨及全國性民政財團法人自應依該規定辦理

前項監督，應與受託者明確約定相關監督事項及方式。	委託案件，爰為第一項規定，並於第二項規範其應與受託者約定相關監督事項與方式，以期明確。
第二十一條 政黨因解散或經主管機關廢止備案、全國性民政財團法人解散後，其保有之個人資料不得繼續使用，應依下列方式處理，並將相關紀錄報送主管機關保存至少五年： 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。	一、政黨因解散或經主管機關廢止備案、全國性民政財團法人解散後，自不得再繼續持有使用個人資料，應作妥善處置。爰規定此類政黨及全國性民政財團法人，應將所保有之個人資料予以銷毀、移轉或其他刪除、停止處理或利用等方式處理，並將相關紀錄報送主管機關保存一定時間。 二、政黨及全國性民政財團法人在銷毀、移轉或其他刪除、停止處理或利用個人資料過程中，亦宜保存執行方法、時間、地點、執行人員、接受移轉個人資料之對象及合法移轉個人資料之法規依據等資料，以便日後舉證。
第二十二條 本辦法發布施行前，未訂定本計畫及處理方法之政黨及全國性民政財團法人，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管機關備查。	規範本辦法施行前之政黨及全國性民政財團法人，應依本辦法訂定本計畫及處理方法，並於一定期間內報請備查。
第二十三條 本辦法自發布日施行。	本辦法施行日期。

附件

個人資料事故通報及紀錄表		
政黨/財團法人名稱 通報機關	通報時間： 年 月 日 時 分 通報人： 簽名(蓋章) 職稱： 電話： Email： 地址：	
發生時間		
發生種類	☐ 竊取 ☐ 竄改 ☐ 毀損 ☐ 滅失 ☐ 洩漏 ☐ 其他侵害情形	個人資料侵害之總筆數(大約)
		☐ 一般個人資料____筆 ☐ 特種個人資料____筆
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		
是否於發現個人資料外洩後七十二小時內通報	☐ 是 ☐ 否，理由：	

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。

說明：依據第八條第二項規定，定明政黨及全國性民政財團法人遇個人資料侵害事故發生後，應依本表格式通報主管機關。