

# 內政部指定地政類非公務機關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。」鑑於內政部業管地政類非公務機關，基於經營業務需要，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，訂定內政部指定地政類非公務機關個人資料檔案安全維護管理辦法（以下簡稱本辦法），計二十四條，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、非公務機關之定義。（第三條）
- 四、非公務機關應訂定個人資料檔案安全維護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）、訂定內容及報備查期限。（第四條）
- 五、非公務機關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、個人資料範圍之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、非公務機關所屬人員為執行業務蒐集、處理及利用個人資料之規範、非公務機關應遵守告知義務等事項。（第九條及第十條）
- 八、依不動產經紀業及租賃住宅服務業行業特性，除應尊重當事人拒絕接受行銷之權利，應有將拒絕情形通知總公司、加盟店及有參與聯賣服務者作統一處理之機制。（第十一條）
- 九、非公務機關國際傳輸個人資料時應遵循事項。（第十二條）
- 十、非公務機關對於當事人行使本法第三條規定之權利時採取之措施。

(第十三條)

- 十一、非公務機關對所保管之個人資料檔案應採取必要適當之防護措施，並應對所屬人員有適度之管理措施。(第十四條及第十五條)
- 十二、非公務機關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。(第十六條)
- 十三、非公務機關應定期或不定期對所屬人員進行教育宣導。(第十七條)
- 十四、本計畫及處理方法之稽核、使用紀錄留存、檢討改善等事項。(第十八條至第二十條)
- 十五、非公務機關委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。(第二十一條)
- 十六、非公務機關業務終止後所保有個人資料之處理方式。(第二十二條)
- 十七、本辦法施行前之非公務機關，應訂定或修正本計畫及處理方法，並於一定期間內報備查。(第二十三條)
- 十八、本辦法施行日期。(第二十四條)

# 內政部指定地政類非公務機關個人資料檔案安全維護管理辦法

條文	說明
<p>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。</p>	<p>本辦法訂定依據。</p>
<p>第二條 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。</p>	<p>本辦法主管機關。</p>
<p>第三條 本辦法所稱非公務機關，包括下列各款：</p> <p>一、不動產經紀業。</p> <p>二、租賃住宅服務業。</p> <p>三、不動產估價師事務所。</p> <p>四、地政士事務所</p> <p>五、其他經中央主管機關公告指定者。</p> <p>前項第三款所稱不動產估價師事務所，指依不動產估價師法規定開業設立之事務所。</p> <p>第一項第四款所稱地政士事務所，指依地政士法規定開業設立之事務所。</p>	<p>定明本辦法之適用對象為：依不動產經紀業管理條例規定許可設立之公司或商號、依租賃住宅市場發展及管理條例規定許可設立之公司、依不動產估價師法及依地政士法規定開業設立之事務所；另為因應日後可能納入管理之非公務機關需求，第一項除前四款之非公務機關外，於第五款規定其他經中央主管機關公告指定者。</p>
<p>第四條 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。</p> <p>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，參酌第五條至第二十二條規定，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：</p> <p>一、非公務機關之組織規模及特性。</p> <p>二、個人資料檔案之安全管理措施：</p>	<p>一、第一項定明非公務機關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之義務及訂定內容。</p> <p>二、由於非公務機關大小規模不一，經營型態不盡相同，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。爰第二項規定非公務機關得參酌其規模、特性、保有個人資料之性質及數量等事項，參考第五條至第二十二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。</p> <p>三、考量國內非公務機關為數眾多，倘未予訂定統一規範，業者於訂</p>

<p>(一) 配置管理之人員及相當資源。</p> <p>(二) 界定蒐集、處理及利用個人資料之範圍。</p> <p>(三) 個人資料之風險評估及管理機制。</p> <p>(四) 事故之預防、通報及應變機制。</p> <p>(五) 個人資料蒐集、處理及利用之內部管理程序。</p> <p>(六) 設備安全管理、資料安全管理及人員管理措施。</p> <p>(七) 認知宣導及教育訓練。</p> <p>(八) 個人資料安全維護稽核機制。</p> <p>(九) 使用紀錄、軌跡資料及證據保存。</p> <p>(十) 個人資料安全維護之整體持續改善。</p> <p>(十一) 業務終止後之個人資料處理方法。</p> <p>第一項之本計畫及處理方法，不動產經紀業應於申請開業備查時，租賃住宅服務業應於申請租賃住宅服務業登記時，其餘非公務機關應於申請開業時，一併報請所在地直轄市、縣（市）主管機關備查；中央主管機關依前條第一項第五款公告指定前，已完成開業或營業項目登記者，應於公告指定之日起六個月內報請所在地直轄市、縣（市）主管機關備查。</p>	<p>定本計畫及處理方法時恐無所適從，爰第二項定明非公務機關訂定本計畫及處理方法時應包括之事項，並保留彈性空間，非公務機關得依個別情況，於必要時整併第二項第二款各目之相關事項。</p> <p>四、第三項定明非公務機關訂定本計畫及處理方法報請所在地直轄市、縣（市）主管機關備查之期限。</p>
<p>第五條 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。</p> <p>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。</p>	<p>一、第一項規定非公務機關應指派配置適當管理人員，負責本計畫及處理方法之規劃、訂定、修正及執行等事宜，並提供適當之資源協助，以為確保個人資料維護安全措施發揮效能。另本法第四十八條第四款及第五十條規定，對違反本法第二十七條第一項或未依同條第二項訂定計畫或業務終止後個人資料處理方法之非公務機關之代表人得併同處罰，爰規定負責本計畫及處理方法之管理</p>

	<p>人員須定期向負責人提出報告，促使負責人能據以監督本計畫及處理方法之執行，落實對個人資料保護之工作。</p> <p>二、為能讓全體員工明瞭個人資料保護之重要性，第二項規定非公務機關應將個人資料保護管理政策及蒐集、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，公告於營業處所適當之處，以供所屬人員遵循，更可使當事人知曉業者保護個人資料之相關事項，俾保護自身權益。</p>
<p>第六條 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。</p>	<p>非公務機關蒐集個人資料應符合個人資料保護相關法令之規定，並定期查核確認所蒐集、處理及利用個人資料之類別及範圍，界定其是否納入本計畫及處理方法之範圍。</p>
<p>第七條 非公務機關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。</p>	<p>定明非公務機關應就已界定個人資料之範圍與蒐集、處理及利用個人資料流程，分析評估可能發生之風險，並針對該可能發生之風險，採取必要之防範與管控措施，避免個人資料被竊取、竄改、洩漏、毀損、滅失或濫用。</p>
<p>第八條 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（以下簡稱個人資料事故），應訂定下列應變、通報及預防機制：</p> <p>一、個人資料事故發生後應採取之各類措施，包括：</p> <p>（一）控制當事人損害之方式。</p> <p>（二）查明個人資料事故後通知當事人之適當方式。</p> <p>（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。</p> <p>二、個人資料事故發生後應受通報之對象及其通報方式。</p> <p>三、個人資料事故發生後，其矯正預防措施之研議機制。</p> <p>非公務機關遇有達一千筆以上之個人資料事故時，應於發現後七</p>	<p>一、本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事故者，應查明後以適當方式通知當事人。爰第一項定明非公務機關訂定個人資料安全事故之應變、通報及預防機制之義務。</p> <p>二、考量各非公務機關大小規模、經營型態及掌握之個人資料數量不一，爰以個人執業之中小型事務所所能掌握之個人資料數量一千筆為基準，於第二項定明非公務機關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八月十一日訂定之「行政院及所屬各機關落實個人資料保護聯繫作業要點」第四點第一項第三款規</p>

<p>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，以書面通報所在地直轄市、縣（市）主管機關，並副知中央主管機關（書面通報格式如附件）。</p> <p>直轄市、縣（市）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非公務機關之應變、通報及預防機制進行實地檢查，並視檢查結果為後續處置。中央主管機關認有必要時，得督導直轄市、縣（市）主管機關對於非公務機關之相關機制改善情形。</p>	<p>定，定明事故通報之對象、時點及應通報事項。</p> <p>三、為調查事故發生後，是否係非公務機關所採取保護安全措施不足導致，於第三項定明中央及直轄市、縣（市）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。</p>
<p>第九條 非公務機關所屬人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。</p>	<p>定明非公務機關所屬人員執行業務蒐集、處理、利用一般個人資料時，應遵守相關法定要件及程序。</p>
<p>第十條 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。</p>	<p>為尊重當事人能知曉其個人資料被蒐集、處理及利用之狀況，本法第八條及第九條規定資料蒐集者有告知義務。爰規定非公務機關，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，以便所屬人員在辦理業務時能據以執行。</p>
<p>第十一條 不動產經紀業或租賃住宅服務業所屬人員利用個人資料行銷時，應明確告知當事人其所屬公司或商號名稱；其屬加盟經營者，應告知加盟品牌名稱及公司或商業登記之名稱。</p> <p>不動產經紀業或租賃住宅服務業利用個人資料行銷時，應提供當事人免費表示拒絕接受行銷之方式。</p> <p>不動產經紀業或租賃住宅服務業利用個人資料進行行銷者，當事</p>	<p>一、本條依不動產經紀業及租賃住宅服務業行業特性另定之。</p> <p>二、為讓當事人知曉對其進行行銷之不動產經紀業者或租賃住宅服務業為何，第一項規定不動產經紀業或租賃住宅服務業應規定所屬人員於行銷時，須確實表明業者名稱，其屬加盟經營之業者，並須告知公司或商業登記名稱，以便讓當事人在行使拒絕接受行銷之權利時，知悉拒絕之對象為何，以免在日後追究其違法行銷</p>

<p>人表示拒絕接受行銷時，應即停止利用其個人資料行銷。</p> <p>前項當事人表示拒絕接受行銷之情形，直營店應通知總公司彙整後再周知所屬各部門；加盟店應通知內部其他業務人員，其有上傳加盟總部者，亦應併同通知加盟總部；不動產經紀業涉有參與聯賣服務者，應通知其他聯賣業者。</p> <p>不動產經紀業或租賃住宅服務業，應於當事人表示拒絕接受行銷之日起七日內完成前項通知。</p>	<p>責任時，發生爭議。</p> <p>三、依本法第二十條第三項規定，首次行銷當事人表示拒絕接受時，其意思表示如需費用，應由行銷者負擔，第二項爰規定不動產經紀業或租賃住宅服務業應提供當事人免費表示拒絕接受行銷之方式。</p> <p>四、本法第二十條第二項定明當事人有拒絕接受行銷之權利，第三項爰規定不動產經紀業或租賃住宅服務業利用個人資料進行行銷時，應確實遵循上開規定辦理。</p> <p>五、第四項規定當事人明確表示拒絕接受行銷時，不動產經紀業或租賃住宅服務業之直營店應將該拒絕情形通知總公司作統一處理，並應有機制通知其他各直營店知悉。採取加盟經營之業者，因彼此法人人格獨立，除經當事人同意外，資源無法共享，因此無法要求將拒絕接受行銷之資訊通知其他加盟業者。惟至少要做到將該拒絕接受行銷之情形，通知店內其他業務人員，如有上傳加盟總部者，亦應盡到通知加盟總部之義務，以避免發生再度行銷之情事。不動產經紀業之加盟或直營業者，涉有參與聯賣服務者，應通知其他聯賣業者，所稱聯賣服務，係泛指經紀業經委託人同意將受託交易之不動產，利用資訊網路或其他方式與他經紀業組成共同銷售資訊網，由經紀業與他經紀業依約定使用交易資訊並藉以尋找交易相對人之服務。</p> <p>六、為避免業者怠於通知，致當事人權益受損，爰於第五項定明通知期限。</p>
<p>第十二條 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。</p>	<p>一、第一項規定中央主管機關依本法第二十一條規定所為之命令或處分，非公務機關應通知所屬人員知曉並遵照辦理。</p> <p>二、第二項規定非公務機關將個人資</p>

<p>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：</p> <ol style="list-style-type: none"> <li>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。</li> <li>二、當事人行使本法第三條所定權利之相關事項。</li> </ol>	<p>料作國際傳輸者，應檢視是否受中央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。</p>
<p>第十三條 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：</p> <ol style="list-style-type: none"> <li>一、提供聯絡窗口及聯絡方式。</li> <li>二、確認為個人資料當事人本人，或經其委託者。</li> <li>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。</li> <li>四、有收取必要成本費用者，應告知當事人收費基準。</li> <li>五、遵守本法第十三條有關處理期限之規定。</li> </ol>	<p>依本法第三條規定，當事人就其個人資料得行使查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除其個人資料等權利，且非公務機關除有本法第十條但書、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情形外，應於本法第十三條規定期間內准駁當事人之請求，爰本條定明非公務機關應辦理事項，以利資料當事人行使權利。</p>
<p>第十四條 非公務機關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。</p> <p>前項安全設備或防護措施，應包含下列事項：</p> <ol style="list-style-type: none"> <li>一、紙本資料檔案之安全保護設施。</li> <li>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。</li> <li>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，非公務機關對受託者</li> </ol>	<p>為確保非公務機關所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰第一項規定業者得視其規模、業務性質、資料儲存之媒介物及其數量等，於所定本計畫及處理方法中採取必要且適當之安全設備或防護措施。第二項並規定安全設備或防護措施應包括事項，例如：對紙本資料之保護應採用堅固之保險箱或櫥櫃、電腦設備應設置防火牆及防毒程式、對複製或上傳檔案行為予以管控、制定紙本資料之銷毀程序、磁碟、磁帶、光碟片、微縮片、積體電路晶片及其他存放個人資料之媒介物需報廢汰換或轉作其他用途時，應確實刪除所存放之個人資料檔案或防範洩漏個人資料等。</p>



<p>之監督依第二十一條規定辦理。</p>	
<p>第十五條 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。</p> <p>前項管理措施，應包含下列事項：</p> <ol style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>三、要求所屬人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。</li> <li>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。</li> </ol>	<ol style="list-style-type: none"> <li>一、非公務機關與所屬人員，不論是何種法律關係，業者都必須避免個人資料之保管及處理發生弊端，導致侵害當事人權益情事，爰第一項規定應於所定本計畫及處理方法中，對所屬人員採取必要且適當之管理措施。</li> <li>二、第二項規定非公務機關應根據業務性質，檢視容易發生問題之處，預先予以防範。例如：與業務無關人員不得任意接觸資料、授予必要利用個人資料人員不同等級之權限、所屬人員在個人資料蒐集、處理及利用流程中有無漏洞、約束規範嚴密保管個人資料檔案及所屬人員異動或離職時，所持有之個人資料如何交接與保密切結等事項。</li> </ol>
<p>第十六條 非公務機關使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者，應採取下列資訊安全措施：</p> <ol style="list-style-type: none"> <li>一、使用者身分確認及保護機制。</li> <li>二、個人資料顯示之隱碼機制。</li> <li>三、網際網路傳輸之安全加密機制。</li> <li>四、個人資料檔案與資料庫之存取控制及保護監控措施。</li> <li>五、防止外部網路入侵對策。</li> <li>六、非法或異常使用行為之監控及因應機制。</li> </ol> <p>前項第五款及第六款所定措施，應定期演練及檢討改善。</p>	<ol style="list-style-type: none"> <li>一、依非公務機關行業特性，鑑於個人執業之小型事務所、商號，或新開業之業者，如納入分級加強管理對象之範疇，將造成其於營運上負擔不符比例原則之行政及法令遵循成本，爰參考實務執行情形，以營業約五年之不動產經紀業者掌握之個人資料數量一萬筆，作為分級加強管理之標準。考量該等業者於營業上已具有相當之規模及穩定性，納入需分級加強管理對象之範疇應無疑義，爰於第一項明定一萬筆以上為應加強管理之條件，以兼顧比例原則及政策目標。</li> <li>二、非公務機關使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上者，為避免使用者個人資料於使用資通訊服務時被竊取、洩漏、竄改或其他侵害事故發生，依行政院一百十年八月十一日訂定之「行政院及所屬各機關落實個人資料保護聯繫作業</li> </ol>

要點」第四點第一項第一款及第二款規定，應加強管理，並至少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。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 29191「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

	<p>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。</p> <p>三、隨網路科技之進步，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，爰第二項定明針對第一項第五款及第六款所定措施，非公務機關應定期進行演練及檢討改善。</p>
<p>第十七條 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。</p>	<p>定明非公務機關應定期或不定期對所屬人員施以認知宣導或教育訓練，以使所屬人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。</p>
<p>第十八條 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。</p> <p>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。</p> <p>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。</p>	<p>一、第一項規定非公務機關執行個人資料安全維護稽核機制之方法及相關檢查措施。</p> <p>二、第二項規定檢查結果應向負責人提出報告及保存。</p> <p>三、第三項規定檢查結果發現本計畫及處理方法不符法令者，非公務機關應作必要之改善。</p>
<p>第十九條 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。</p> <p>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：</p> <p>一、刪除、停止處理或利用之方法、時間或地點。</p> <p>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</p>	<p>一、為非公務機關證明確實執行本計畫及處理方法，已盡防止個人資料遭侵害之義務，第一項定明非公務機關應記錄其個人資料使用情況，並留存軌跡資料或相關證據，供日後發生法律爭議時提供說明佐證，以免除或減輕其法律責任。</p> <p>二、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。</p> <p>三、另依本法第三十條規定，損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不</p>

<p>間、地點，及該對象蒐集、處理或利用之合法依據。</p> <p>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。</p>	<p>行使而消滅；自損害發生時起，逾五年者，亦同。爰第三項規定上述軌跡資料、相關證據及紀錄，除法令另有規定或契約另有約定者外，應至少留存五年。</p>
<p>第二十條 非公務機關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所在地直轄市、縣（市）主管機關備查。</p>	<p>由於科技發展不斷進步，社會活動型態亦隨時改變，爰定明非公務機關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，隨時檢討所定本計畫及處理方法，如有不合時宜之處，應立即修正本計畫及處理方法，以落實保護個人資料。</p>
<p>第二十一條 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，應依本法施行細則第八條規定為適當監督。</p> <p>非公務機關為執行前項監督，應與受託者明確約定相關監督事項及方式。</p>	<p>依本法施行細則第八條規定，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，爰第一項定明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，應為適當之監督，並於第二項規定與受託者約定相關監督事項與方式。</p>
<p>第二十二條 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：</p> <ol style="list-style-type: none"> <li>一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。</li> <li>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。</li> <li>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。</li> </ol>	<ol style="list-style-type: none"> <li>一、非公務機關因解散、歇業、公司合併或其他原因終止業務後，自不得再繼續持有使用個人資料，應作妥善處置。爰規定終止業務之非公務機關，應視其終止業務之原因，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。另依本法第三十條規定，損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。爰定明相關紀錄至少應留存五年。</li> <li>二、非公務機關在銷毀、移轉或其他刪除、停止處理或利用個人資料過程中，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。</li> </ol>

<p>第二十三條 本辦法發布施行前，未訂定或已訂有本計畫及處理方法之非公務機關，應依本辦法規定訂定或修正，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所在地直轄市、縣（市）主管機關備查。</p>	<p>規範本辦法施行前之非公務機關，應依本辦法訂定或修正本計畫及處理方法，並於一定期間內報備查。</p>
<p>第二十四條 本辦法自發布日施行。</p>	<p>本辦法施行日期。</p>

附件

個人資料事故通報及紀錄表	
非公務機關名稱 _____  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	<input type="checkbox"/> 竊取 <input type="checkbox"/> 竄改 <input type="checkbox"/> 毀損 <input type="checkbox"/> 滅失 <input type="checkbox"/> 洩漏 <input type="checkbox"/> 其他侵害情形
	個人資料侵害之總筆數(大約) _____ <input type="checkbox"/> 一般個人資料_____筆 <input type="checkbox"/> 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	<input type="checkbox"/> 是 <input type="checkbox"/> 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：配合第八條規定，擬訂「個人資料事故通報及紀錄表」之統一格式，俾利非公務機關填報。