大陸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。	本辦法訂定之依據。
第二條 大陸委員會（以下簡稱本會）所管非公務機關應依本辦法規定，規劃、訂定、修正與執行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）。但保有個人資料未達五千筆之非公務機關，不在此限。 保有個人資料筆數達五千筆以上之非公務機關，應於本辦法施行之日起六個月內完成前項計畫之訂定；保有個人資料筆數雖未達五千筆之非公務機關，於本辦法施行後，因直接或間接蒐集而達五千筆以上時，應於保有筆數達五千筆之日起六個月內完成之。 依第一項規定完成本計畫及處理方法之訂定者，若因刪除、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之非公務機關，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而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。 第一項至第三項中個人資料筆數之計算，以非公務機關單日所保有之個人資料為認定基準。	一、考量本會所管非公務機關之業務規模及特性不同，爰依分級管制原則訂定保有個人資料筆數五千筆以上之門檻，惟非公務機關應負舉證責任。 二、考量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需一定時間，爰於第二項明定非公務機關應完成本計畫及處理方法之期限，使非公務機關於因應本辦法時有所緩衝。 三、考量非公務機關可能因業務規模之改變等因素，致所保有之個人資料筆數減少，爰於第三項明定已依本條第一項規定完成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非公務機關，因刪除、銷毀或其他方式致所保有之個人資料筆數未達五千筆時，且連續二年期間所保有之個人資料筆數皆未達五千筆時，得不執行本計畫及處理方法之全部或一部。考量非公務機關於日後仍有可能所保有之個人資料筆數達五千筆以上之情形，爰於第三項但書明定應於保有筆數達到五千筆以上之當日時起三十日內恢復本計畫及處理方法全部之執行。 四、於第四項明定本條所稱五千筆之認定基準。
第三條 非公務機關為符合本法、本辦法及其他相關法令規定，應依其業務規模及特性，衡酌營運資源之合理分配，配置管理人員及相當資源，負責規劃、訂定、修正與執行本計畫及處理方法。 本計畫及處理方法之訂定或修正，應經非公務機關負責人、法定代理人或內部權責單位核定或簽署。	一、配合本法第二十七條及其施行細則第十二條第二項第一款之規定，非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，應考量業務規模及特性，依比例原則採取技術上及組織上之措施，規劃、訂定、修正與執行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。 二、明定相關計畫及處理方法之訂定或修正，應經非公務機關負責人、法定代理人或內部權責單位(如董、監事會議)核定或簽署。
第四條 非公務機關應定期清查所保有之個人資料檔案與筆數，界定本計畫及處理方法	一、配合本法施行細則第十二條第二項第二款之規定，應定期清查所保有之個人資料檔

之適用範圍。	案與筆數，界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適用範圍，並作為後續個人資料風險評估及管理作業之依據。 二、非公務機關清查個人資料檔案時，應依其執行業務所應適用之各種法令辦理，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，定期評估可能產生之風險，並依據風險評估結果，採取適當安全管理措施。	配合本法施行細則第十二條第二項第三款之規定，非公務機關應以前條所界定之範圍及其相關業務流程為依據，評估個人資料可能面臨之風險及其發生可能性，並根據風險評估結果，採取適當之安全管理措施。
第六條 非公務機關為因應個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定下列應變、通報及預防機制： 一、事故發生後應採取之應變措施，包括降低、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。 二、事故發生後應受通報之對象及其通報方式。 三、事故發生後研議其矯正預防措施之機制。 非公務機關遇有個人資料安全事故，將危及大量當事人權益者，應於發現事故後七十二小時內填具「個人資料侵害事故通報與紀錄表」(如附表 1)通報本會下列事項，未於時限內通報者應附遲延理由： 一、非公務機關名稱、通報人及聯絡方式。 二、通報機關、通報時間、事件發生時間、擬通知當事人時間。 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、擬採通知當事人之方式。 本會接受非公務機關依第二項通報後，得依本法第二十二條至第二十五條等規定，為適當之監督管理措施。	一、配合本法施行細則第十二條第二項第四款，為降低或控制因個人資料被竊取、竄改、毀損、滅失或洩漏等事故造成主體財產及非財產之損害，非公務機關應訂定個人資料安全事故應變、通報及預防機制。 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。爰於第一項第一款規定應變措施應包括控制當事人之損害之方式、查明事故後通知當事人之適當方式及內容。 三、次按非公務機關如發生個人資料遭竊、外洩等安全事故，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中，爰為第一項第二款之規定。 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，應明定事故發生後矯正預防措施之研議機制。 五、末按非公務機關遭遇個人資料安全事故而危及大量當事人權益，應採取較一般事故更嚴密之應變措施，爰於第二項明定相關因應機制及其必要作為，並應於發現事故後七十二小時內填具「個人資料侵害事故通報與紀錄表」通報本會。 六、於第三項明定本會接受非公務機關通報重大個人資料外洩事故後，得依本法第二十二條至第二十五條等規定，為適當之監督管理措施，如派員檢查、沒入或命銷毀違

	法蒐集之個人資料、公布非公務機關之違法情形及其名稱與負責人姓名等。
第七條 非公務機關為確保個人資料之蒐集、處理或利用，符合個人資料保護相關法令之規定，應訂定下列內部管理程序： 一、蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料者，檢視是否符合本法第六條第一項但書所定情形。 二、檢視個人資料蒐集或處理，是否符合本法第十九條第一項所定之法定情形及特定目的；經當事人同意而為蒐集或處理者，並應確保符合本法第七條第一項之規定。 三、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，檢視是否符合本法第二十條第一項但書所定情形；經當事人同意而為特定目的外之利用者，並應確保符合本法第七條第二項之規定。 四、檢視個人資料之蒐集是否符合本法第八條第二項或第九條第二項得免為告知之事由；無得免為告知之事由者，並應確保符合本法第八條第一項或第九條第一項之規定。 五、利用個人資料行銷而當事人表示拒絕接受行銷者，確保符合本法第二十條第二項及第三項之規定。 六、委託他人蒐集、處理或利用個人資料者，確保符合本法施行細則第八條之規定，並於委託契約或相關文件明確約定其內容。 七、當事人行使本法第三條所定權利之相關事項： （一）提供當事人行使權利之方式。 （二）確認當事人或其代理人之身分。 （三）檢視是否符合本法第十條但書、第十一條第二項但書及第十一條第三項但書所定得拒絕其請求之事由。 （四）依據前目規定拒絕當事人行使權利者，應附理由通知當事人。 （五）就當事人請求為准駁決定及延長決定期間之程序，並應確保符合	配合本法施行細則第十二條第二項第五款之規定，非公務機關應於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中，訂定個人資料蒐集、處理及利用之內部管理程序，以確保個人資料之蒐集、處理或利用，符合個人資料保護相關法令之規定。

本法第十三條之規定。 （六）當事人請求更正或補充其個人資料者，其應為釋明之事項。 （七）就當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準。 八、維護個人資料正確性之機制；個人資料正確性有爭議者，並應確保符合本法第十一條第一項、第二項及第五項之規定。 九、定期檢視個人資料蒐集之特定目的是否已消失或期限是否已屆滿；其特定目的消失或期限屆滿者，並應確保符合本法第十一條第三項之規定。	
第八條 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： 一、個人資料有加密之必要者，應於蒐集、處理或利用時，採取適當之加密措施。 二、個人資料有備份之必要者，應對備份資料採取適當之保護措施。 三、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。 非公務機關為維護所保有個人資料之安全，應對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、電腦、自動化機器設備及其他媒介物（以下簡稱儲存媒介物），採取下列設備安全管理措施： 一、依儲存媒介物之特性及使用方式，建置適當之保護設備或技術。 二、依所屬人員業務特性、內容及需求，訂定適當之管理規範。 三、針對存放儲存媒介物之環境，施以適當之進出管制措施。	一、配合本法施行細則第十二條第二項第六款之規定，非公務機關保有個人資料檔案者，應依據個人資料風險評估之結果，於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中，訂定相關資料安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏： （一）個人資料檔案經風險評估有加密之必要時，非公務機關應依蒐集、處理或利用等各種行為態樣，採取適當之加密措施，爰為第一項第一款之規定。 （二）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，個人資料檔案經風險評估有備份之必要時，非公務機關亦應針對複製、備份之個人資料檔案，採取適當之保護措施，爰為第一項第二款之規定。 （三）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，應訂定相關使用範圍，以確保資料安全，其報廢或轉作他用時亦同，爰為第一項第三款之規定。 二、配合本法施行細則第十二條第二項第八款之規定，非公務機關保有個人資料檔案者，應依據個人資料風險評估之結果，於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中，訂定相關設備安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，包括非公務機關用以

	保存個人資料之各類儲存媒介物，應具有一定保護程度之要求，如一定程度之技術、設備、管制措施及安全環境等。
第九條 非公務機關使用資通訊系統蒐集、處理或利用個人資料者，為維護所保有個人資料之安全，除前條要求外，應採取下列資料安全管理措施(如附表 2)： 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機制。 五、防止外部網路入侵對策。 六、非法或異常使用行為之監控與因應機制。	處理個人資料之資通訊系統遭受內部異常使用或外部攻擊者入侵時，往往導致大量個人資料外洩，為維護所保有個人資料之安全，爰為第一款至第六款之規定。
第十條 非公務機關將個人資料作國際傳輸者，應檢視是否受個人資料保護相關法令之限制，並且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。	非公務機關將個人資料作跨國（境）之處理或利用時，對於人民隱私影響甚鉅，甚至有危及國家安全之疑慮，爰配合本法第二十一條之規定，要求非公務機關將個人資料作國際傳輸者，應遵守個人資料保護相關法令之限制，同時必須告知當事人相關個人資料傳輸之區域，並配合本法施行細則第十二條第二項第六款之規定，要求非公務機關應對資料接收方為下列適當之監督： 一、非公務機關國際傳輸個人資料前，宜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，爰為第一款之規定。 二、為有效處理當事人就其個人資料行使個人資料保護法第三條所定權利，爰於第二款規定。
第十一條 非公務機關為維護所保有個人資料之安全，應採取下列人員管理措施： 一、與所屬人員約定保密義務。 二、識別業務內容涉及個人資料蒐集、處理或利用之人員。 三、依其業務特性、內容及需求，設定所屬人員接觸個人資料之權限，並定期檢視其適當性及必要性。 四、人員離職時，要求人員返還個人資料之載體，並刪除因執行業務而持有之個人資料。	配合本法施行細則第十二條第二項第六款之規定，非公務機關保有個人資料檔案者，應依據個人資料風險評估之結果，於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中，訂定下列相關人員管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏： 一、為確保所屬人員履行人員管理相關措施，約定其保密義務，爰為第一款之規定。 二、為控管所屬人員接觸個人資料之權限，並定期檢視其適當性及必要性，非公務機關應識別業務內容涉及個人資料蒐集、處理或利用之人員，考量其業務之特性、內容

	及需求，設定所屬人員接觸個人資料之權限，爰為第二款及第三款之規定。 三、為防止因所屬人員離職而導致個人資料被竊取、竄改、毀損、滅失或洩漏，非公務機關應要求該人員返還個人資料之載體，並刪除因執行業務而持有之個人資料，爰為第四款之規定。
第十二條 非公務機關應對所屬人員定期施以個人資料保護認知宣導及教育訓練。 前項認知宣導及教育訓練，至少應包括下列事項： 一、個人資料保護相關法令之規定。 二、所屬人員之責任範圍。 三、本計畫及處理方法各項管理程序、機制及措施之要求。	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、其所負擔之責任範圍，以及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中各項管理程序、機制及措施之要求。
第十三條 非公務機關為確保本計畫及處理方法之落實，應訂定個人資料安全稽核機制，定期或不定期檢查本計畫及處理方法執行狀況，提出評估報告，並採取第十五條第一款之改善機制。	配合本法施行細則第十二條第二項第九款之規定，非公務機關應於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中，訂定個人資料安全稽核機制。
第十四條 非公務機關執行本計畫及處理方法時，應評估其必要性，保存下列紀錄至少五年： 一、個人資料之蒐集、處理及利用紀錄。 二、自動化機器設備之軌跡資料。 三、落實執行本計畫及處理方法之證據。 非公務機關於業務終止後，其保有之個人資料應依下列方式處理及記錄： 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蒐集該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、配合本法施行細則第十二條第二項第十款之規定，非公務機關應於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中，訂定相關使用紀錄、軌跡資料及證據保存機制，妥善保存個人資料之蒐集、處理及利用紀錄、自動化機器設備之軌跡資料，以及落實本計畫及處理方法之證據等。 二、非公務機關業務終止後，亦即個人資料蒐集之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、銷毀、停止處理或利用，惟當事人往往無從知悉，為避免不必要之糾紛，爰於第二項規定非公務機關因業務終止而刪除個人資料者，應留存相關紀錄；因業務終止而將個人資料移轉予他人者，應記錄其原因、對象、方法、時間、地點及受移轉對象得蒐集該個人資料之合法依據。 三、本條所稱之業務終止為非公務機關因結束業務經營、特定目的消失、契約或法令規定期限屆滿之情況。
第十五條 非公務機關為持續改善本計畫及處理方法，應訂定下列整體持續改善機制： 一、本計畫及處理方法未落實執行時應採	配合本法施行細則第十二條第二項第十一款之規定，非公務機關應於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中，訂定

取矯正預防措施。 二、參酌本計畫及處理方法執行狀況、技術發展及法令變化等因素，定期檢視或修正本計畫及處理方法。	個人資料安全維護之整體持續改善機制。
第十六條 本辦法自發布日施行。	本辦法之施行日期。

附表 1

<table>
<tr><th colspan="3">個人資料侵害事故通報與紀錄表</th></tr>
<tr><td>非公務機關名稱

通報機關

</td><td colspan="2">通報時間：　　年　月　日　時　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個人資料侵害之總筆數(大約)

</td></tr>
<tr><td>□一般個人資料＿＿＿＿筆
□特種個人資料＿＿＿＿筆</td></tr>
<tr><td>發生原因及事故摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後 72 小時通報</td><td colspan="2">□是　　□否，理由</td></tr>
</table>

附表 2

資料安全管理措施說明表	
管制措施	說明
一、 使用者身分確認及保護機制	針對資通系統或個人資料檔案存取，提供使用者識別、鑑別及身分驗證管理機制，如帳密管制、多重認證技術、帳戶鎖定機制、密碼具一定複雜程度等。
二、 個人資料顯示之隱碼機制	系統呈現介面上，如有個人資料資訊，應評估使用情境，於以適當且一致性之遮蔽，以為個人資料保護。
三、 網際網路傳輸之安全加密機制	當個人資料進行網路傳輸時，應採用加密機制，包含使用加密傳輸管道、資料加密傳輸等。
四、 個人資料檔案及資料庫之存取控制與保護監控措施	針對個人資料檔案及資料庫之儲存，應適當加密；存取時，應提供使用者識別、鑑別及身分驗證管理機制；留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。
五、 防止外部網路入侵對策	針對可能來自於網路的入侵，採取相關的偵測或防護作為，如個人電腦安裝防毒軟體、使用電子郵件過濾機制、設定網路防火牆、架構應用程式防火牆、採用入侵偵測及防禦機制或進階持續性威脅攻擊防禦措施等。
六、 非法或異常使用行為之監控與因應機制	針對資通系統或個人資料檔案之存取，留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。