

**法規名稱：**大陸委員會指定非公務機關個人資料檔案安全維護辦法

**發布日期：**民國 110 年 12 月 28 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**

- 1 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。
- 2 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。
- 3 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。
- 4 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。

## **第 3 條**

- 1 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。
- 2 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。

## **第 4 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之適用範圍。

## **第 5 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。

## **第 6 條**

- 1 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。

- 2 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。

- 3 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。

## 第 7 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 8 條

1 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。

2 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。

## 第 9 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。

## 第 10 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。

## 第 11 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。

## 第 12 條

- 1 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。
- 2 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。

## 第 13 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。

## 第 14 條

- 1 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。
- 2 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。

## 第 15 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。

## 第 16 條

本辦法自發布日施行。