# 內政部指定警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 |
| --- | --- |
| 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：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。 | 本辦法主管機關。 |
| 第三條　本辦法所稱非公務機關，包括下列各款：<br>一、保全業。<br>二、當舖業。<br>三、槍砲彈藥刀械業。<br>四、其他經中央主管機關公告指定者。<br>前項第三款槍砲彈藥刀械業，指依槍砲彈藥刀械許可及管理辦法第十三條、第二十八條或模擬槍許可及管理辦法第三條規定許可之廠商。 | 定明本辦法之適用對象為：依保全業法許可設立之保全業、依當舖業法許可設立之當舖業、依槍砲彈藥刀械許可及管理辦法或模擬槍許可及管理辦法規定許可之廠商；另為因應日後可能納入管理之非公務機關需求，除前三款之非公務機關外，於第四款規定其他經中央主管機關公告指定者。 |
| 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。<br>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：<br>一、非公務機關之組織規模及特性。<br>二、個人資料檔案之安全管理措施：<br>（一）配置管理之人員及相當資源。<br>（二）界定蒐集、處理及利用個人資料之範圍。<br>（三）個人資料之風險評估及管理 | 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、訂定內容及報備查期限。 |

| | |
|---|---|
| 機制。<br>（四）事故之預防、通報及應變機制。<br>（五）個人資料蒐集、處理及利用之內部管理程序。<br>（六）設備安全管理、資料安全管理及人員管理措施。<br>（七）認知宣導及教育訓練。<br>（八）個人資料安全維護稽核機制。<br>（九）使用紀錄、軌跡資料及證據保存。<br>（十）個人資料安全維護之整體持續改善。<br>（十一）業務終止後之個人資料處理方法。<br>第一項之本計畫及處理方法，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；中央主管機關依前條第一項第四款公告指定前，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主事務所所在地之直轄市、縣(市)主管機關備查。 | |
| 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。<br>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。 | 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。<br>二、為能讓全體員工明瞭個人資料保護之重要性，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。 |
| 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。 | 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。 |
| 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。 | 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。 |
| 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：<br>一、個人資料事故發生後應採取之各類措施，包括：<br>（一）控制當事人損害之方式。<br>（二）查明個人資料事故後通知當事人之適當方式。<br>（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。<br>二、個人資料事故發生後應受通報之對象及其通報方式。<br>三、個人資料事故發生後，其矯正預防措施之研議機制。<br>非公務機關遇有達五千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，以書面通報主事務所所在地之直轄市、縣(市)主管機關，並副知中央主管機關(書面通報格式如附件)。<br>直轄市、縣(市)主管機關對於重 | 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、竄改、毀損、滅失或洩漏等個人資料事故者，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。<br>二、第二項參考製造業及技術服務業個人資料檔案安全維護管理辦法第二條規定，係以保有消費者個人資料筆數達五千筆以上之業者應負個人資料檔案安全維護義務，爰定明非公務機關遇有達五千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。<br>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，定明第三項中央及直轄市、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。 |

| | |
|---|---|
| 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。 | |
| 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。 | 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。 |
| 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。 | 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。 |
| 第十一條　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。<br>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：<br>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。<br>二、當事人行使本法第三條所定權利之相關事項。 | 一、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。<br>二、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　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：<br>一、提供聯絡窗口及聯絡方式。<br>二、確認為個人資料當事人本人，或經其委託者。<br>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 | 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 |

| | |
|---|---|
| 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。<br>四、有收取必要成本費用者，應告知當事人收費基準。<br>五、遵守本法第十三條有關處理期限之規定。 | 條定明非公務機關應辦理事項，以利資料當事人行使權利。 |
| 第十三條　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。<br>前項安全設備或防護措施，應包含下列事項：<br>一、紙本資料檔案之安全保護設施。<br>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。<br>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之監督依第二十條規定辦理。 | 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，爰本條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，於所訂計畫中採取必要且適當之安全設備或防護措施。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。 |
| 第十四條　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。<br>前項管理措施，應包含下列事項：<br>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。<br>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。<br>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。<br>四、所屬人員離職時，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 | 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訂計畫中，對所屬人員採取必要且適當之管理措施。<br>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離職時，所持有之個人資料如何交接與保密切結等事項。 |

| | |
|---|---|
| 簽訂保密切結書。 | |
| 第十五條　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五千筆以上者，應採取下列資訊安全措施：<br>一、使用者身分確認及保護機制。<br>二、個人資料顯示之隱碼機制。<br>三、網際網路傳輸之安全加密機制。<br>四、個人資料檔案及資料庫之存取控制與保護監控措施。<br>五、防止外部網路入侵對策。<br>六、非法或異常使用行為之監控與因應機制。<br>前項第五款及第六款所定措施，應定期演練及檢討改善。 | 一、依據行政院一百十年二月三日會議決議事項，非公務機關使用資通訊系統蒐集、處理或利用個人資料，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，並參酌製造業及技術服務業個人資料檔案安全維護管理辦法第二條規定，保有消費者個人資料筆數達五千筆以上之業者應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。參照行政院資安處建議，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。另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：<br>（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。<br>（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。<br>（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。<br>（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。<br>（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。<br>（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。<br>二、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。 |
| 第十六條　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。 | 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。 |
| 第十七條　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。<br>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。<br>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。 | 定明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配套措施。 |
| 第十八條　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 | 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；另於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 |

| | |
|---|---|
| 證據。<br>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：<br>一、刪除、停止處理或利用之方法、時間或地點。<br>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。<br>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。 | 應留存相關紀錄；且上述軌跡資料、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。 |
| 第十九條　非公務機關應隨時參酌業務及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)主管機關備查。 | 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，隨時檢討所訂計畫及處理方法。如有不合時宜之處，應立即修正，以落實保護個人資料。 |
| 第二十條　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。<br>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。 | 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，爰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，並與受託者約定相關監督事項與方式。 |
| 第二十一條　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：<br>一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。<br>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。<br>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、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。爰定明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。<br>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。 |

| | |
|---|---|
| 第二十二條　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主事務所所在地之直轄市、縣(市)主管機關備查。 | 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。 |
| 第二十三條　本辦法自發布日施行。 | 本辦法施行日期。 |

# 附件、個人資料事故通報與紀錄表

<table>
<tr><td colspan="3">個人資料事故通報與紀錄表</td></tr>
<tr><td>非公務機關名稱<br>_____<br><br>通報機關<br>_____</td><td colspan="2">通報時間：　年　月　日　時　分<br>通報人：　　簽名(蓋章)<br>職稱：<br>電話：<br>Email：<br>地址：</td></tr>
<tr><td>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取<br>□竄改<br>□毀損<br>□滅失<br>□洩漏<br>□其他侵害情形</td><td>個人資料侵害之總筆數(大約)<br>_____</td></tr>
<tr><td>□一般個人資料 _____筆<br>□特種個人資料 _____筆</td></tr>
<tr><td>發生原因及摘要</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七十二小時內通報</td><td colspan="2">□ 是　　□否，理由：</td></tr>
</table>

備註：特種個人資料，係指有關病歷、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，係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，定明內政部指定警政類非公務機關遇個人資料侵害

事故發生後，應依本表格式通報主事務所所在地之直轄市、縣(市)主管機關。