個人資料檔案安全維護管理辦法草案總說明

因應個人資料保護委員會成立，為落實資訊隱私權保障，兼顧個人資料檔案安全維護並促進合理利用，依據個人資料保護法(以下簡稱本法)第十八條第二項、第二十條之一第二項授權，就個人資料檔案安全維護事項、管理機制、應採取之措施及其他相關事項之辦法，由主管機關定之。

建立並實施個人資料檔案管理機制及安全維護措施為保障個人資料安全必要作為，為促進相關規範事項具有一致性，並確保對於個人資料之保護與管理，均能達到一定水準，爰訂定共通性規範，提供公務機關或非公務機關據以制定內部管理制度及安全維護控制措施，作為實施個人資料保護相關作業之基本準則，亦作為個人資料檔案安全維護最低限度之要求。

參考本法與施行細則、各機關所定個人資料檔案安全維護辦法、國際隱私保護法規、原則要項及個人資料管理趨勢，機關應衡酌持有之個人資料檔案類別、數量、機關特性、業務需求等，配置合理資源，實施個人資料安全維護作為；為協助公務機關或非公務機關針對個人資料檔案採取適當之安全維護措施，並持續精進及優化個人資料檔案安全維護事項，透由制定及落實組織上與程序上必要之管理，降低個人資料蒐集、處理及利用活動之安全風險，爰擬具「個人資料檔案安全維護管理辦法」(以下簡稱本辦法）草案，其要點如下：

一、本辦法訂定依據、目的、名詞定義與個人資料檔案筆數計算方式及增減適用。(草案第一條至第四條)

二、界定個人資料之管理範圍。(草案第五條)

三、建立事故之預防、通報及應變機制。(草案第六條)

四、對蒐集、處理及利用個人資料業務流程之人員採取安全管理措施。（草案第七條）

五、定期實施個人資料保護認知宣導及教育訓練。(草案第八條)

六、對保有電子個人資料檔案之設備採取安全管理措施。(草案第九條)

七、採取適當之實體安全措施以保護存放個人資料之場域。(草案第十條)

八、特種個人資料檔案安全管理。（草案第十一條）

九、機關自行或委外設置、開發之資通系統存取安全控制措施。（草案第十二條）

十、機關自行或委外設置、開發之資通系統事件日誌記錄及保存。（草案第十三條）

十一、機關自行或委外設置、開發之資通系統儲存之個人資料定期備份及保護措施。（草案第十四條）

十二、個人資料刪除及業務終止後個人資料處理方法。（草案第十五條）

十三、訂定個人資料檔案安全維護計畫。（草案第十六條）

十四、配置個人資料保護管理人員。（草案第十七條）

十五、定期清查作業流程與個人資料現況並文件化。（草案第十八條）

十六、個人資料之風險評估及管理機制。（草案第十九條）

十七、事故之通知、通報及應變機制之演練。（草案第二十條）

十八、定期實施管理制度及差異化教育訓練。（草案第二十一條）

十九、個人資料檔案安全管理。（草案第二十二條）

二十、機關維運自行或委外設置、開發之資通系統之資訊安全措施。（草案第二十三條）

二十一、內部個人資料安全稽核及受託者稽核。（草案第二十四條）

二十二、個人資料使用紀錄及證據保存。（草案第二十五條）

二十三、個人資料安全維護之整體持續改善機制。（草案第二十六條）

二十四、非公務機關於過渡期間個人資料檔案安全維護管理辦法適用情形。（草案第二十七條）

二十五、本辦法之施行日期。（草案第二十八條）

個人資料檔案安全維護管理辦法草案

條文	說明
第一章　總則	章名。
第一條　本辦法依個人資料保護法（以下簡稱本法）第十八條第二項及第二十條之一第二項規定訂定之。	明定本辦法訂定之依據。
第二條　公務機關或非公務機關應按其機關規模、特性與其保有之個人資料檔案，衡酌資源之合理分配，規劃、訂定、檢討及修正內部管理機制，落實安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。	本辦法適用於公務機關或非公務機關，其所具資源、規模與保有之個人資料檔案相異。機關應審酌其組織規模、業務屬性、經營模式、保有之個人資料檔案類型或數量等具體情狀，基於比例原則採取適當管理機制及安全維護措施並落實之。
第三條　本辦法用詞，定義如下： 一、大型非公務機關：指依法辦理公司、有限合夥或商業登記，而非屬中小企業認定標準第二條所稱中小企業，且保有當事人個人資料檔案筆數達一萬筆以上之非公務機關。 二、風險評估：包括風險識別、風險分析及風險評量之過程。 三、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。	一、參考經濟部「中小企業認定標準」第二條所定之標準，排除中小企業，明定具一定經濟規模之大型企業保有大量個人資料檔案者為大型非公務機關，其執行法令遵循之資源及能力相對充足，採行加強管理機制，為第一款規定。 二、參考行政院及所屬各機關風險管理及危機處理作業原則及行政院及所屬各機關風險管理及危機處理作業手冊之規範，為第二款規定。 三、參照資通安全管理法第三條第一款之定義，為第三款規定。
第四條　非公務機關保有個人資料檔案筆數，以非公務機關單日所保有每一自然人之每一蒐集特定目的加總計算。 非公務機關保有個人資料檔案筆數未達一萬筆，於本辦法施行後，因直接或間接蒐集而達一萬筆者，應於保有筆數達一萬筆之日起算六個月內採行本辦法所定大型非公務機關安全維護事項及管理機制。 大型非公務機關因刪除、銷毀或其他方法致保有個人資料檔案筆數減少，且連續二年期間保有個人資料檔案筆數未達一萬筆之業者，得不適用第十六條至第二十六條之規定。但嗣後因直接或間接蒐集而致保有個人資料檔案筆數達一萬筆以上者，應於保有筆數達一萬筆之日起算六個月內，恢復適用本條規定。	一、本條第一項非公務機關保有個人資料檔案筆數之計算方式，所稱「單日」係指機關盤點當日，筆數依個人資料蒐集之不同目的而個別累加計算。舉例同一自然人之個人資料檔案蒐集為「網站會員資料」及「內部員工資料」之蒐集特定目的不同，則加總其個人資料檔案筆數。 二、非公務機關因組織或業務規模擴大等因素，致個人資料檔案筆數增加，應重新盤點個人資料檔案筆數，並應於保有筆數達一萬筆之日起算六個月內一併採行本辦法所定大型非公務機關安全維護事項及管理機制。 三、考量大型非公務機關依法令主動或依當事人之請求刪除個人資料、或可能因為業務規模或經營之改變等因素，致保有個人資料檔案筆數有所增

	減，爰於第二項及第三項明定非公務機關適用、不再適用及重新適用本辦法對於大型非公務機關之相關規範。
第二章　公務機關或非公務機關共通安全維護措施	一、章名。 二、本章明定公務機關或非公務機關必須採行之共通安全維護措施規定。
第五條　公務機關或非公務機關應依個人資料保護相關法令，定期清查確認所保有之個人資料現況，界定個人資料管理範圍。	個人資料之蒐集、處理或利用係屬連續且變動之過程，透過定期盤點與現況清查，可釐清保有之個人資料之種類、數量及法律依據等，並據此確認資料之正確性與保存必要性。爰明定公務機關或非公務機關應建立定期清查確認機制，以界定並調整應納入管理之範圍，避免因範圍界定不明或管理疏漏致生事故風險，並落實個人資料保護相關法令規範。
第六條　公務機關或非公務機關應依個人資料事故通知通報及應變辦法規定，建立個人資料事故之通報、通知及應變機制。	一、公務機關或非公務機關發生個人資料事故，應採行通知、通報及應變措施，並負保存事故紀錄之義務。 二、為確保公務機關或非公務機關運作事故之處置，應建立通知、通報、應變及檢討改善之機制。
第七條　公務機關或非公務機關應對蒐集、處理或利用個人資料業務流程之人員，採取下列人員安全管理措施，並定期檢視措施之適當性及必要性： 一、識別業務內容涉及個人資料蒐集、處理或利用之人員。 二、依組織業務特性、內容與需求，建立人員之保密義務、身分識別與鑑別及權限管控措施。 三、機關業務或職務異動時，異動人員於載有個人資料媒介物之交接、返還或資料刪除措施。	一、為使公務機關或非公務機關建立人員管理之體系，應識別業務涉及個人資料蒐集、處理或利用之人員，以達到權責分明，並有效追蹤及管理，為第一款規定。 二、公務機關或非公務機關辦理個人資料之蒐集、處理或利用，所屬人員直接或間接有取得個人資料可能性，應與其約定個人資料保密義務，以降低未經授權的人員濫用個人資料之風險。針對接觸個人資料之人員建立身分驗證機制，確保已識別為合法授權人員，並經鑑別其身分真確性方可存取個人資料，應依循最小權限原則配發必要權限，為第二款規定。 三、為避免人員業務異動或離職仍繼續保有機關內部個人資料致生風險，並確保機關對個人資料之控制，應落實存有個人資料之載體返還以及資料之刪除，為第三款規定。
第八條　公務機關或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。	公務機關或非公務機關應教育所屬人員其所負之法律責任，確保其瞭解內部管理程序與要求，並因應內、外部環境變化之

	可能性，應定期辦理個人資料保護認知宣導及教育訓練。
第九條　公務機關或非公務機關保有電子個人資料檔案，應採取下列設備安全管理措施： 一、妥善保管並實施適宜之存取管制。 二、資通訊軟、硬體應適時進行必要更新或升級，並修補漏洞。 三、電腦應安裝防毒軟體或採用其他防護設備;防毒軟體應設定自動更新至最新版本病毒碼,且應啟動即時病毒防範機制,定期執行完整掃描作業，並針對惡意程式執行刪除。	公務機關或非公務機關使用資通訊軟、硬體，進行個人資料之蒐集、處理或利用，應妥善保管資訊資產與實施存取管制，並執行必要之資通訊軟、硬體升級更新與漏洞修補，建置與啟動即時病毒防範及惡意程式處理機制。
第十條　公務機關或非公務機關應採取適當之實體安全措施以保護存放個人資料之場域，其安全措施包括但不限於下列項目： 一、場域進出:建立對於資訊機房及檔案庫房等管制區域之人員進出管理，僅允許經授權之人員進入。 二、監控系統:於資訊機房與檔案庫房等管制區域安裝監控系統,監控並記錄人員及個人資料之進出。 三、實體障礙:使用安全鎖、門禁系統等實體安全措施。	個人資料檔案為紙本或電子檔案形式，均須確保儲存媒介物之實體場域安全防護，實施如管制場域進出、設置監控系統及建立實體障礙等，以防止個人資料遭不當存取，並應考量風災、水災等環境威脅之防範措施,以降低發生個人資料事故之風險。
第十一條　公務機關或非公務機關保有本法第六條第一項有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料者，應針對載有前述個人資料之紙本或電子檔案採取下列資料安全管理措施： 一、訂定紙本及使用可攜式設備或儲存媒體之管制規範。 二、保有個人資料檔案之媒介物於銷毀、報廢或轉作其他用途時，應採取適當防範措施。 三、處理過程有備份個人資料之需要時，應比照原件，依本辦法規定予以保護。 四、檔案安全加密措施。 五、資料安全傳輸措施。 六、安全銷毀機制。	一、特種個人資料如發生竊取、竄改、毀損、滅失或洩漏之事故其對當事人權益影響將更為嚴重，爰本條明定資料安全管理措施。 二、公務機關或非公務機關保有特種個人資料，應確保資料生命週期之安全,檔案資料儲存之媒介物之管制與安全防範措施。 三、依本法施行細則第五條之意旨，檔案備份資料應比照原件予以保護，另檔案資料儲存應加密及採取安全傳輸措施，並應於個人資料蒐集之特定目的消失或期限屆滿須刪除時,確保資料已安全銷毀且不可回復。

第十二條　公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，其帳號管理及存取安全控制措施應規範之範圍包括但不限於下列項目： 一、使用者存取應採最小權限原則。 二、帳號安全管理及定期清查。 三、設置密碼並符合複雜性需求。	一、公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料者，明定資通系統存取控制至少應採取之安全控制措施，以降低資料遭未經授權存取並濫用之風險。 二、使用者存取個人資料應僅限於其執行業務所需最低限度之最小權限原則、建立完善之帳號生命週期管理機制，包含帳號之申請、審核、啟用、停用及註銷等流程。 三、應定期對現有帳號進行清查，以有效識別並移除不再使用或異常之帳號、以及強制使用者設置符合一定複雜性要求之密碼，並定期更換。
第十三條　公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應執行下列事項： 一、訂定日誌之記錄時間週期及留存政策，並保存適當期間。 二、確保資通系統具備記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。	一、公務機關或非公務機關如有維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料者，為確保可有效進行個人資料事故之追查與鑑識，明定資通系統事件日誌與可歸責性至少應採取之安全控制措施。 二、機關應明確訂定資通系統日誌的記錄時間、週期及留存政策，確保資通系統具備記錄特定重要事件的功能。 三、機關應明定應記錄的特定資通系統事件（如使用者登入、登出、權限變更、資料存取、修改或刪除等敏感操作行為）、以及記錄並監控系統特權帳號所執行的各項操作。
第十四條　公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應就資通系統儲存之個人資料定期備份，並應對備份資料採取適當之保護措施及確保其可用性。	公務機關或非公務機關維運自行或委外設置、開發之資通系統蒐集、處理及利用個人資料者，明定資通系統營運持續計畫應就儲存之個人資料定期備份、對備份檔案採取等同原件之保護，並確保實施備份資料取代或回復後之檔案可用性。
第十五條　公務機關或非公務機關依本法第十一條第三項規定刪除個人資料，應採取適當刪除措施使資料不可回復，並留存刪除紀錄。 前項機關於職務或業務終止後，其所蒐集、處理或利用之個人資料應依下列方式處理，並留存下列紀錄： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。	一、公務機關或非公務機關應確保個人資料之銷毀程序，使其無法還原或重建，並留存可供查核之紀錄。 二、機關於職務或業務終止後其所蒐集、處理及利用之個人資料，應採取銷毀、移轉或其他刪除、停止處理或利用之方法，均應予記錄。 三、所有刪除與職務或業務終止後處理的紀錄，均應留存至少五年，以供於

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。 前二項紀錄應留存至少五年。	當事人權利主張時進行追溯或供主管或上級機關進行監督查核。
第三章　公務機關或大型非公務機關強化安全維護措施	一、章名。 二、本章明定公務機關或大型非公務機關必須採行之強化安全維護措施規定。非公務機關依其個人資料保護需要及目的性，亦可採行本章措施。
第十六條　為實施第二條內部管理機制，公務機關或大型非公務機關應訂定個人資料檔案安全維護計畫(以下簡稱本計畫)，包括但不限於下列項目： 一、配置管理之人員及相當資源。 二、界定個人資料之範圍。 三、個人資料之風險評估及管理機制。 四、事故之預防、通報及應變機制。 五、人員管理、認知宣導及教育訓練。 六、設備及場域安全管理。 七、資料安全、資訊安全。 八、資料安全稽核機制。 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。 前項計畫之訂定或修正，應經公務機關個人資料保護長、非公務機關代表人、管理人、其他代表人或其指派之適當人員核定。	一、公務機關或大型非公務機關應制定個人資料檔案安全維護計畫，以系統性與文件化作法達成個人資料檔案管理目的，具體建構內部管理機制及安全維護事項等規劃俾據以實施。 二、個人資料檔案安全維護計畫內容應包含本辦法第五條至第二十六條規定之具體實踐內容。 三、為強化組織治理及領導階層責任，個人資料檔案安全維護計畫之訂定或修正，應由機關之個人資料保護最高管理者或其指派之適當人員審查、確認及核定。
第十七條　大型非公務機關應指定個人資料保護管理專責人員，並設置個人資料保護管理執行小組與查核人員，以辦理本辦法所定安全維護事項及管理機制之經常性工作。 大型非公務機關應確保管理專責人員及查核人員具備適當專業能力，且兩者不得兼任。	一、本條為本辦法第七條之強化規定。 二、大型非公務機關應指定專責人員辦理個人資料檔案安全維護事項，以防止個人資料事故，並應設置個人資料保護管理執行小組，任務包括機關內個人資料保護政策研議、執行、稽核、改善等事項，並應訂定成員組成及小組運作相關事項，為第一項規定。 三、辦理個人資料安全稽核，為確保稽核之獨立性，應要求查核人員與執行個人資料管理之管理人員不得互相兼任；並為強化人員專業性，應規範管理人員、查核人員具備適當專業能

	力，為第二項規定。
第十八條　公務機關或大型非公務機關於界定個人資料管理範圍時，應定期清查其個人資料蒐集、處理或利用之流程，與其所保有之個人資料現況，並建立個人資料檔案盤點清冊及個人資料蒐集、處理或利用流程之說明文件。 前項盤點清冊應包括但不限於下列項目： 一、保有單位。 二、個人資料之項目、類別、型態、數量。 三、蒐集之特定目的、方式、來源。 四、依本法第八條或第九條向當事人告知之方式，或得免為告知之情形。 五、蒐集、處理及利用相關業務或程序。 六、依本法第六條第一項、第十六條或第二十條第一項為目的外利用之情形。 七、保存方式、期限及銷毀方式。	一、本條為本辦法第五條之強化規定。 二、公務機關或大型非公務機關應每年清查盤點個人資料蒐集、處理及利用所涉之業務流程，及所保有個人資料之現況，以界定個人資料檔案之管理範圍，並建立個人資料盤點清冊及流程說明文件等文件化資訊，為第一項規定。 三、公務機關或大型非公務機關應建立個人資料檔案盤點清冊，並明定盤點清冊至少應包含項目，為第二項及各款規定。
第十九條　公務機關或大型非公務機關，應依據前條所界定之個人資料管理範圍，針對其保有之個人資料現況與其業務涉及個人資料蒐集、處理或利用之流程，每年定期識別、分析及評估可能面臨之風險，並根據風險評估結果，採行適當安全維護措施。 前項風險評估應包括但不限於下列事項： 一、個人資料之項目、類別、型態、數量。 二、處理個人資料之方法、技術。 三、內部及外部之潛在威脅。	一、公務機關或大型非公務機關完成個人資料檔案盤點及管理範圍界定，於製作個人資料檔案盤點清冊後，應每年定期識別、分析及評估可能面臨之風險。 二、依風險評估結果列出可行的風險處理對策，評估接受、規避、抑減或移轉風險，採取對應適當安全維護管理機制及措施，並擬定及實施風險處理計畫。
第二十條　公務機關或大型非公務機關應依據前條風險評估結果，定期辦理個人資料事故之通報、通知及應變機制演練，以確保機制運行之有效性。	一、本條為本辦法第六條之強化規定。 二、公務機關或大型非公務機關應落實個人資料事故應變處理流程，提升回應效能、強化面對個人資料事故之韌性，機關應依據風險評估結果，每年定期辦理個人資料事故通知、通報與應變機制演練。

第二十一條　公務機關或大型非公務機關應根據職務或業務規模、個人資料檔案保有量、業務性質等差異，定期辦理必要之教育訓練，確保本法第十八條第二項指定之專人或第十七條第一項指定之專責人員明瞭內部與外部規定之要求、責任範圍與個人資料保護機制、程序及措施。	一、本條為本辦法第八條之強化規定。 二、公務機關或大型非公務機關應評估有關條件，明定妥適頻率定期辦理管理制度及差異化(如通識及專業課程)之個人資料保護教育訓練，確保個人資料檔案保護專人或專責人員具備工作對應之責任、意識及能力。 三、訓練內容包含內、外部相關法令遵循權責任務及相關規範、機制、程序及措施之要求，並應進行訓練成效評估，俾利正確實施個人資料檔案安全維護事項，長期並建立機關個人資料保護文化。
第二十二條　公務機關或大型非公務機關保有紙本或電子個人資料檔案，應採取下列資料安全管理措施： 一、訂定紙本及使用可攜式設備或儲存媒體之管制規範。 二、保有個人資料檔案之媒介物於銷毀、報廢或轉作其他用途時，應採取適當防範措施。 三、處理過程具備份個人資料之需要時，應比照原件，依本辦法規定予以保護之。 保有個人資料檔案屬於本法第六條以外之個人資料，經第十九條風險評估結果，屬優先處理項目且為執行業務所必要者，得採取第十一條第四款、第五款及第六款之安全管理措施。	一、公務機關或大型非公務機關應落實個人資料保護之課責性、公平性及可執行性，評估機關規模、資源及保有一定數量個人資料檔案之影響。 二、第一項明定機關就所保有之本法第六條以外之個人資料，採行本辦法第十一條第一款至第三款之資料安全管理措施；惟個人資料檔案如經本辦法第十九條風險評估結果，認有必要優先處理安全風險且為執行業務所必要者，得評估併採取本辦法第十一條第四款至第六款之資料安全管理措施。
第二十三條　公務機關或大型非公務機關，維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應採取下列資訊安全措施： 一、使用者帳號管理、身分鑑別及保護機制。 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。 七、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	一、本條為本辦法第十二條、第十三條及第十四條之強化規定。 二、公務機關或大型非公務機關維運自行或委外設置、開發之資通系統蒐集、處理或利用個人資料，應採行資訊安全措施，以防止個人資料事故發生。 三、提供對外服務之資通系統潛在風險高，個人資料外洩之影響層面鉅大，系統上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點、漏洞修補作業；另考量資通訊科技發展日新月異，資訊安全亦與時俱進，爰系統上線後仍應持續辦理前述安全性掃描檢測及弱點、漏洞修補作業。

八、儲存之個人資料定期備份。 九、資通系統如提供對外服務，系統上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點、漏洞修補作業；系統上線後應持續辦理。 前項各款所定措施，應定期評估其有效性及檢討改善。	四、第二項明定機關應定期演練前項各款所定措施，以熟悉整體作業流程，及時發現問題並檢討改善，俾周全資訊安全防護作業。
第二十四條　公務機關或大型非公務機關應訂定內部個人資料安全稽核機制，每年應至少辦理一次稽核機關實施個人資料安全維護事項與管理機制之情形及成效。 前項內部稽核機制應包括但不限於下列項目： 一、稽核項目及內容。 二、執行稽核之合理頻率。 三、稽核結果之紀錄。 公務機關或大型非公務機關具委外辦理蒐集、處理或利用個人資料之情形者，委託機關與受託機關應於委託契約或相關文件中，明確約定其內容，並每年至少辦理一次稽核受託者執行情形及記錄稽核結果備查。 第一項及第三項稽核結果應向公務機關首長、非公務機關代表人、管理人或其他有代表權人報告，並落實改善；稽核結果之紀錄應保存五年。	一、為確認安全維護管理機制及措施之落實情形及有效性，並強化機關內、外部相關控制機制，明定公務機關或大型非公務機關應由查核人員每年定期辦理內部稽核；若稽核發現缺失，應立即進行改善，為第一項規定。 二、明定內部稽核機制至少應包含之項目，為第二項規定。 三、委託他人蒐集、處理或利用個人資料之行為，將使個人資料置於可控制範圍以外之區域，委託方應善盡對受託者之監督管理責任，有必要與受託方就委託管理為妥善約定。公務機關或大型非公務機關應就前述約定內容，每年定期對受託者進行稽核作業，為第三項規定。 四、公務機關或大型非公務機關內部稽核或對受託者稽核之結果應向機關首長或代表人等報告並落實改善，並明定每次稽核結果紀錄應至少保存五年，以對應提供法令遵循及相關規範等之內、外部查核，為第四項規定。
第二十五條　公務機關或大型非公務機關執行本計畫所定各種個人資料保護機制、程序及措施，應保存下列紀錄： 一、個人資料之蒐集、處理或利用紀錄。 二、落實安全維護措施之證據。 三、當事人權利行使之紀錄。 前項紀錄之保存期間，除本辦法另有規定者外，應留存至少五年。	一、公務機關或大型非公務機關應佐證個人資料檔案安全保護制度之落實，並為保護當事人權利及避免訴訟爭議，明定機關應就個人資料之流向及處理過程之完整紀錄、安全維護措施之執行紀錄、當事人權利行使紀錄等妥為保存。 二、相關紀錄之保存期限，參考對應本法第三十條規定，明定業者應保存至少五年。
第二十六條　公務機關或大型非公務機關應訂定包含下列措施之整體持續改善機制： 一、安全維護計畫未落實執行時之矯正預防措施。	公務機關或大型非公務機關應持續改善、有效執行個人資料檔案之安全保護事項，明定應追蹤並持續關注計畫未落實執行之矯正預防措施，並配合法令訂定或修正及參酌內、外部因素，定期檢討所定之計畫

二、應配合法令訂定或修正，參酌執行業務狀況、技術發展等因素，定期檢視所定之規定、計畫合宜性，必要時應予修正。	是否合宜，並進行必要修正，俾利個人資料檔案安全維護事項得持續滾動檢討改善。
第四章　附則	章名。
第二十七條　本法第五十一條之一第一項及第二項公告範圍內之非公務機關，應適用中央目的事業主管機關依同條第四項授權訂定之辦法。但中央目的事業主管機關未訂定相關辦法，或本辦法規定較為嚴格者，適用本辦法之規定。	本法第五十一條之一訂有六年過渡期規定，部分非公務機關於過渡期間仍由中央目的事業主管機關或直轄市、縣（市）政府管轄，為使前述非公務機關明確理解本辦法與其他中央目的事業主管機關所定辦法間之適用關係，為本條規定。
第二十八條　本辦法施行日期，由主管機關定之。	配合本法修正期程，明定施行日期由主管機關定之。