法規名稱：保全業個人資料檔案安全維護管理辦法
訂定時間：中華民國 105 年 7 月 8 日

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。

〔立法理由〕

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。

〔立法理由〕

本辦法主管機關。

第三條

保全業應訂定個人資料檔案安全維護計畫（以下簡稱計畫），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。

前項所稱保全業，指依保全業法規定許可，並經依法設立經營保全業務之股份有限公司。

〔立法理由〕

一、依個人資料保護法（以下簡稱本法）第二十七條第二項規定，於第一項指定保全業應訂定個人資料檔案安全維護計畫（以下簡稱計畫）。

二、第二項明定本辦法適用對象。

第四條

保全業依前條第一項規定訂定計畫時，得視其規模、特性、保有個人資料之性質及數量等事項，參酌第六條至第二十二條規定，訂定適當之安全維護管理措施。

前項計畫內容應包括下列事項，第二款相關事項必要時得整併之：

一、保全業之組織規模。

二、個人資料檔案之安全管理措施：

（一）配置管理之人員及相當資源。

（二）界定蒐集、處理及利用個人資料之範圍。

（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）個人資料蒐集、處理及利用之內部管理程序。

（六）設備安全管理、資料安全管理及人員管理措施。

（七）認知宣導及教育訓練。
（八）個人資料安全維護稽核機制。
（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。
（十一）業務終止後之個人資料處理方法。
〔立法理由〕
一、本辦法規定之相關組織及程序要求，業者應明定於計畫內，並定期檢視及配合相關法令修正。
二、由於保全業大小規模不一，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。爰第一項規定保全業得參酌其規模、特性、保有個人資料之性質及數量等事項，參考第六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。
三、考量國內保全業為數眾多，倘未予訂定統一規範，業者於訂定計畫時恐無所適從，爰第二項明定保全業訂定計畫時應包括之事項，並保留彈性空間，保全業得依個別情況，於必要時整併第二項第二款各目之相關事項。

第五條
保全業應於申請開業備查時，一併將計畫報請當地直轄市或縣（市）主管機關備查。
保全業於本辦法發布施行前已完成開業備查者，應於本辦法發布施行日起六個月內，將計畫報請當地直轄市或縣（市）主管機關備查。已經許可經營保全業務而尚未完成開業備查者，亦同。
〔立法理由〕
一、為使保全業落實訂定計畫，爰第一項規定保全業應將訂定之計畫，報請當地主管機關備查。
二、依保全業法第四條之二第一項規定，保全業應自開業之日起七日內報請當地主管機關備查。爰第二項明定保全業所定計畫應配合報請備查之時間，以利業者遵循，並供當地主管機關輔導管理之依據。

第六條
保全業應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。
保全業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。
〔立法理由〕
一、第一項規定保全業應指派配置適當管理人員，負責該計畫或業務終止後個人資料處理方法之規劃、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，爰規定負責計畫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計畫之執行，落實對個人資料保護之工作。
二、為能讓全體員工明瞭個人資料保護之重要性，保全業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事項（包括保全業依第三條第一項規定訂定之計畫及依第二十條規定修正之計畫），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。

第七條
保全業應確認蒐集個人資料之特定目的，於達成特定目的之必要範圍內，界定所蒐集、處理及利用個人資料之類別及範圍，並定期清查所保有個人資料檔案之現況。
保全業依前項清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。
〔立法理由〕
一、第一項規定保全業蒐集個人資料（包括所屬人員個人資料）應明確界定其蒐集之特定目的為何，界定所蒐集、處理及利用個人資料之類別及範圍是否屬於必要，並應定期清查所蒐集保有之個人資料是否符合所界定之範圍。
二、第二項規定保全業在清查所蒐集之個人資料類別及範圍時，如發現有逾越特定目的必要範圍之個人資料或特定目的消失、期限屆滿而無保存必要者，應依本法第十一條第三項及第四項規定予以刪除或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。

第八條
保全業應依已界定蒐集、處理與利用個人資料之類別、範圍及流程，分析評估可能發生之風險，訂定適當之管控措施。
〔立法理由〕

本條規定保全業應參酌整體業務運作狀況，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。

第九條

保全業應訂定應變機制，於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，迅速處理以保護當事人之權益。

前項應變機制，應包括下列事項：

一、採取適當之措施控制事故對當事人造成損害。

二、查明事故發生原因及損害狀況，並以適當方式通知當事人事故事實、因應措施及諮詢服務專線等。

三、研議改進措施，避免類似事故再度發生。

四、發生重大個人資料事故者，應即以書面通報當地直轄市或縣（市）主管機關。

前項第四款所稱重大個人資料事故，指個人資料被竊取、洩漏、竄改或其他侵害事故，致危及大量當事人權益之情形。

〔立法理由〕

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。爰本條規定保全業在計畫中應訂定應變機制及其必要作為之相關事項，在發生個人資料被竊取等侵害事故時，得迅速遵循處理，以保護當事人之權益。

第十條

保全業所屬人員為執行業務蒐集個人資料時，應檢視符合蒐集要件及特定目的之必要範圍，並接受該保全業監督。

〔立法理由〕

明定保全業所屬人員執行業務蒐集個人資料時，應遵守相關法定要件及程序，並應受保全業監督。

第十一條

保全業蒐集個人資料，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。

〔立法理由〕

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。爰本條規定保全業，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。

第十二條
中央主管機關依本法第二十一條規定，對保全業為限制國際傳輸個人資料之命令或處分時，保全業應通知所屬人員遵循辦理。
〔立法理由〕
本條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，保全業應通知所屬人員知曉並遵照辦理。

第十三條
保全業所蒐集之個人資料需作特定目的外利用者，應檢視有無本法第二十條第一項但書規定得為利用之情形。
〔立法理由〕
依本法第二十條第一項規定，個人資料應於蒐集之特定目的必要範圍內利用，但具備一定法定情形者，得為特定目的外之利用，爰本條規定保全業如需作特定目的外利用時，應先行檢視是否符合規定。

第十四條
保全業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：
一、提供聯絡窗口及聯絡方式。
二、確認為個人資料當事人之本人，或經其委託者。
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，應附理由通知當事人。
四、收取必要成本費用者，應告知當事人收費基準。
五、遵守本法第十三條有關處理期限規定。
〔立法理由〕
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，爰本條明定保全業應辦理事項，以利資料當事人行使權利。

第十五條
保全業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。
前項安全設備或防護措施，應包含下列事項：
一、紙本資料檔案之安全保護設施。

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。
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，保全業對受託者之監督依第二十二條規定辦理

〔立法理由〕

為確保保全業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。

第十六條

保全業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。

前項管理措施，應包含下列事項：

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。
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。
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。
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，並應簽訂保密切結書。

〔立法理由〕

一、保全業與所屬人員，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。
二、第二項規定保全業應根據業務性質，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。

第十七條

保全業對於個人資料蒐集、處理及利用，應符合本法第十九條及第二十條相關規定，並定期或不定期對於所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

〔立法理由〕

本條規定保全業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。

第十八條

保全業應訂定個人資料檔案安全維護稽核機制，每半年定期或不定期檢查計畫執行情形，檢查結果並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。

保全業依前項檢查結果發現計畫不符法令或不符法令之虞者，應即改善。

〔立法理由〕

一、第一項規定保全業訂定之計畫應包含安全稽核機制，由適當管理人員檢查該計畫是否落實執行，並應將檢查結果報告負責人。

二、第二項規定檢查結果發現計畫不符法令者，保全業應作必要之改善。

第十九條

保全業應採行適當措施，留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，其保存期限至少五年。

〔立法理由〕

保全業為證明確實執行計畫，已盡防止個人資料遭侵害之義務，爰本條規定，應視其規模及業務性質採行適當措施，留存相關證據，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。

第二十條

保全業應隨時參酌業務及計畫執行狀況，社會輿情、技術發展及相關法規訂修等因素，檢討所定計畫，必要時應予修正；修正後，應於十五日內將修正計畫報請當地直轄市或縣（市）主管機關備查。

〔立法理由〕

由於科技發展不斷進步，社會活動型態亦隨時改變，爰本條規定保全業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。如有不合時宜之處，應立即修正計畫，以落實保護個人資料。

第二十一條

保全業業務終止後，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：

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保有該項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。

〔立法理由〕

一、保全業因解散、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。爰本條規定終止業務之保全業，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。

二、保全業在銷毀、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，以便日後得以提出舉證。

第二十二條

保全業委託他人蒐集、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。

保全業為執行前項監督，應與受託者明確約定相關監督事項及方式。

〔立法理由〕

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。是以，保全業自應依該規定辦理委託案件，並與受託者約定相關監督事項與方式，以期明確。

第二十三條

本辦法自發布日施行。

〔立法理由〕

本辦法施行日期。