製造業及技術服務業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。	明定本辦法訂定之依據。
第二條　保有消費者個人資料之製造業及技術服務業業者（以下簡稱業者），應依本辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫(以下簡稱本計畫)。但保有消費者個人資料未達五千筆之業者，不在此限。 保有消費者個人資料筆數達五千筆以上之業者，應於本辦法施行之日起六個月內完成前項計畫之訂定；保有消費者個人資料筆數雖未達五千筆之業者，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之訂定者，若因刪除、銷毀或其他方式致所保有之消費者個人資料筆數減少，且連續二年期間所保有之筆數未達五千筆之業者，得停止本計畫全部或一部之執行。但嗣後因直接或間接蒐集而致所保有之消費者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全部之執行。 第一項所稱製造業及技術服務	一、　參酌「個人資料保護法非公務機關之中央目的事業主管機關」及「經濟部主管個人資料保護法非公務機關之分工表」，於本條第一項明定本辦法之適用對象。惟考量業者之業務規模及特性相差甚遠，為避免保有消費者個人資料筆數較少且規模較小之業者負擔過高的法令遵循成本，遂參考日本個人資訊保護法施行令（個人情報の保護に関する法律施行令）第二條規定，於第一項但書明文保有之消費者個人資料未達五千筆者不適用本辦法，惟企業應負舉證責任。又，業者為證明不適用本辦法，應確實清查消費者個人資料並為詳實之記錄，於此併同敘明。 二、　考量業者訂定消費者個人資料檔案安全維護計畫需一定時間，爰於第二項明定業者應完成消費者個人資料檔案安全維護計畫之期限，使業者於因應本辦法時有所緩衝。又，業者於完成計畫之研擬後，應有一定之程序，使所屬人員知悉本計畫並據以為執行，方可謂完成本計畫之訂定。另，本條稱以上者俱連本

業，指附表所列之行業。 第一項至第三項中消費者個人資料筆數之計算，以業者單日所保有之消費者個人資料為認定基準。 本辦法所稱消費者，指以消費為目的而為交易、使用商品或接受服務者。	數計算。 三、 考量業者可能因為業務規模或經營之改變等因素，致所保有之消費者個人資料數筆減少，且考量業者法令遵循之成本，爰建立退場條款，於第三項明定已依本條第一項規定完成訂定消費者個人資料檔案安全維護計畫之業者，因刪除、銷毀或其他方式致所保有之消費者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，得不執行本計畫之全部或一部。然而，考量業者於日後仍有可能所持有之消費者個人資料筆數達五千筆以上之情形，爰於第三項但書明定因第三項本文之規定得不執行本計畫之全部或一部之業者，日後因直接或間接蒐集而致消費者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當日時起三十日內恢復本計畫全部之執行。 四、 依行政院所定之分工，於第四項明定本辦法所稱之製造業及技術服務業之範圍。 五、 於第五項明定本條所稱五千筆之認定基準。又，本辦法所稱「個人資料」，依本法第二條第一款規定，指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或

	間接方式識別該個人之資料，而本法所稱「得以間接方式識別」，依本法施行細則第三條規定，則係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。因此，於認定個人資料筆數時，應以業者所保有之資料得以直接或間接方式識別特定個人方屬之，若業者所保有之資料，尚不足以直接或間接方式識別特定個人，則不計入個人資料筆數。又依個人資料保護法第二條第四款之規定，處理指「為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送」，故有關於單日保有處理消費者個人資料達五千筆以上者，係含單日儲存消費者個人資料達五千筆以上者，實質概念為累計概念，於此敘明。 六、 本辦法所稱之消費者係指終端消費者。參考消費者保護法第二條第一款於本條第六項明定消費者之定義，避免實務運作之困擾。
第三條　業者為符合本法、本辦法及其他相關法令規定，應依其業務規模及特性，衡酌經營資源之合理分配，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。	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，業者為防止消費者個人資料被竊取、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、修正與執行消費者個人資料檔案安全維護計畫。
第四條　業者應定期清查所保有之消	一、配合本法施行細則第十二條第二項第

費者個人資料檔案與筆數，界定本計畫之適用範圍。	二款之規定，應定期清查所保有之消費者個人資料檔案與筆數，界定消費者個人資料檔案安全維護計畫之適用範圍，並作為後續消費者個人資料風險評估及管理作業之依據。 二、業者清查個人資料檔案時，應依業者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　業者應依前條界定之消費者個人資料範圍，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，業者應以前條所界定之範圍及其相關業務流程為依據，評估消費者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，依本辦法第八條、第十條及第十二條之規定，採取適當之安全管理措施。
第六條　業者為因應消費者個人資料被竊取、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。 業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益者，應立即通報經濟部（以下	為降低或控制因消費者個人資料被竊取、竄改、損毀、滅失或洩漏等事故造成資料主體財產及非財產上之損害，業者得訂定相關因應機制及其必要作為。

簡稱本部）或直轄市、縣（市）政府。	
第七條　業者為確保消費者個人資料之蒐集、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消費者個人資料者，檢視是否符合本法第六條第一項但書所定情形。 二、 檢視消費者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、 檢視消費者個人資料之利用，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、 檢視消費者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、 利用消費者個人資料行銷而當事人表示拒絕接受行銷者，確保	配合本法施行細則第十二條第二項第五款之規定，業者應於消費者個人資料檔案安全維護計畫中，訂定消費者個人資料蒐集、處理及利用之內部管理程序，以確保消費者個人資料之蒐集、處理或利用，符合消費者個人資料保護相關法令之規定。

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、處理或利用消費者個人資料者，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、維護消費者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、定期檢視消費者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　業者為維護所保有消費者個人資料之安全，應採取下列資料安全管理措施： 一、消費者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、消費者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、傳輸消費者個人資料時，應依不同傳輸方式，採取適當之安全措施。 業者使用資訊系統處理消費者個人資料者，為維護所保有消費者個人資料之安全，除前項要求外，應採取下列資料安全管理措施： 一、建置防火牆或其他入侵偵測設備。 二、與網際網路相聯之資訊系統存	一、配合本法施行細則第十二條第二項第六款之規定，業者保有消費者個人資料檔案者，應依據消費者個人資料風險評估之結果，於消費者個人資料檔案安全維護計畫中，訂定相關資料安全管理措施，防止消費者個人資料被竊取、竄改、毀損、滅失或洩漏： (一) 消費者個人資料檔案經風險評估有加密之必要時，業者應依蒐集、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，消費者個人資料檔案經風險評估有備份之必要時，業者亦應針對複製、備份之消費者個人資料檔案，採取適當之保護措施，爰為第一項第二款之規定。 (三)業者傳輸消費者個人資料時，應

有消費者個人資料者，應安裝防毒軟體，定期更新病毒碼，並執行掃毒作業。 三、針對電腦作業系統及應用程式之漏洞，定期安裝修補程式。 四、資訊系統存有消費者個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。 五、資訊系統存有消費者個人資料者，應設定異常存取資料行為之監控機制。 六、處理消費者個人資料之資訊系統進行測試時，應避免使用消費者真實個人資料；使用消費者真實個人資料者，應訂定使用規範。 七、處理消費者個人資料之資訊系統有變更時，應確保其安全性未降低。 八、定期檢視處理消費者個人資料之資訊系統，檢查其使用狀況及存取個人資料之情形。	依不同傳輸方式及其風險評估結果，採取適當之安全措施，爰為第一項第三款之規定。 二、處理消費者個人資料之資訊系統遭受內部異常使用或外部攻擊者入侵時，往往導致大量消費者個人資料外洩，為維護所保有個人資料之安全，爰為第二項第一款至第八款之規定。
第九條　業者將消費者個人資料作國際傳輸者，應檢視是否受經濟部限制，並且告知消費者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。	業者將消費者個人資料作跨國（境）之處理或利用時，對於我國人民隱私影響甚鉅，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，要求業者將消費者個人資料作國際傳輸者，應遵守經濟部所為之限制，同時必須告知消費者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，要求業者應對資料接收方為下列適當之監督：

二、當事人行使本法第三條所定權利之相關事項。	一、業者國際傳輸消費者個人資料前，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。
第十條　業者為維護所保有消費者個人資料之安全，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，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性。 四、人員離職時，要求人員返還消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料。	配合本法施行細則第十二條第二項第六款之規定，業者保有消費者個人資料檔案者，應依據消費者個人資料風險評估之結果，於消費者個人資料檔案安全維護計畫中，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消費者個人資料之權限，並定期檢視其適當性及必要性，業者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，設定所屬人員接觸消費者個人資料之權限，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消費者個人資料被竊取、竄改、毀損、滅失或洩漏，業者應要求該人員返還消費者個人資料之載體，並刪除因執行業務而持有之消費者個人資料，爰為第四款之規定。
第十一條 業者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。	配合本法施行細則第十二條第二項第七款之規定，業者應透過認知宣導及教育訓

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、本計畫各項管理程序、機制及措施之要求。	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及消費者個人資料檔案安全維護計畫中各項管理程序、機制及措施之要求。
第十二條 業者為維護所保有消費者個人資料之安全，應對存有消費者個人資料之紙本、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。	配合本法施行細則第十二條第二項第八款之規定，業者保有消費者個人資料檔案者，應依據消費者個人資料風險評估之結果，於消費者個人資料檔案安全維護計畫中，訂定相關設備安全管理措施，防止消費者個人資料被竊取、竄改、毀損、滅失或洩漏，包括業者用以保存消費者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。
第十三條 業者為確保本計畫之落實，應訂定消費者個人資料安全稽核機制，定期或不定期檢查本計畫執行狀況，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，業者應於消費者個人資料檔案安全維護計畫中，訂定消費者個人資料安全稽核機制。
第十四條 業者執行本計畫時，應評估其必要性，保存下列紀錄至少五年： 一、消費者個人資料之蒐集、處理及利用紀錄。	一、配合本法施行細則第十二條第二項第十款之規定，業者應於消費者個人資料檔案安全維護計畫中，訂定相關使用紀錄、軌跡資料及證據保存機制，妥善保存消費者個人資料之蒐集、處

二、自動化機器設備之軌跡資料。 三、落實執行本計畫之證據。 業者於業務終止後，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。	理及利用紀錄、自動化機器設備之軌跡資料及落實消費者個人資料檔案安全維護計畫之證據等。 二、業者業務終止後，亦即消費者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，爰於第二項規定業者因業務終止而刪除消費者個人資料者，應留存相關紀錄；因業務終止而將消費者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消費者個人資料之合法依據。 三、本條所稱之業務終止為公司因結束業務經營、交易完成、特定目的消失、契約或法令規定期限屆滿之情況。
第十五條 業者為持續改善本計畫，應訂定下列整體持續改善機制： 一、本計畫未落實執行時應採取矯正預防措施。 二、參酌本計畫執行狀況、技術發展及法令變化等因素，定期檢視或修正本計畫。	配合本法施行細則第十二條第二項第十一款之規定，業者應於個人資料檔案安全維護計畫中，訂定消費者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。