數位經濟相關產業個人資料檔案安全維護管理辦法總說明

個人資料保護法第二十七條第二項、第三項規定，中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法；其相關事項之辦法，亦由中央目的事業主管機關定之。

數位發展部（以下簡稱本部）為數位經濟相關產業之中央目的事業主管機關，為使相關業者自行或受委託蒐集、處理或利用個人資料檔案，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰依上開規定之授權訂定數位經濟相關產業個人資料檔案安全維護管理辦法（以下簡稱本辦法），要求該等業者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（以下簡稱安全維護計畫），以加強管理、確保個人資料之安全維護，其要點如下：

一、本辦法之授權依據及適用對象。（第一條及第二條）

二、業者應訂定安全維護計畫及公開個人資料保護管理政策，並指定專人負責訂定、修正及執行。（第三條至第五條）

三、業者應界定個人資料之範圍，進行個人資料之風險評估及管理，規劃事故之預防、通報及應變機制。（第六條至第八條）

四、業者應實施個人資料蒐集、處理或利用之內部管理程序、國際傳輸應辦理事項。（第九條及第十條）

五、業者應實施各項個人資料安全維護措施，包含資料安全管理、人員管理、認知宣導及教育訓練、設備安全管理等措施。（第十一條至第十四條）

六、業者應檢查及持續改善個人資料安全維護措施。（第十五條至第十七條）

七、達一定登記資本額以上或保有個人資料一定筆數以上之業者，分級管理強化部分措施執行頻率。（第十八條）

八、受委託業者與委託業者應遵循個人資料保護之原則（第十九條）

九、本辦法之施行日期。（第二十條）

數位經濟相關產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　本辦法所稱數位經濟相關產業（以下簡稱業者),指從事附表一所列行業之自然人、私法人或其他團體。	參酌行政院主計總處行業統計分類，於本條及附表一明定本辦法之適用對象。
第三條　業者應於本辦法施行之日起三個月內完成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（以下簡稱安全維護計畫）之規劃及訂定。 安全維護計畫應納入符合第五條至第十七條規定之具體內容。 業者應依其所訂定之安全維護計畫執行之。數位發展部（以下簡稱本部）得要求業者提出安全維護計畫之實施情形，業者應於指定期限內，以書面方式提出。	一、依本法第二十七條第二項規定，本部得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。考量業者訂定安全維護計畫需一定時間，爰於第一項明定業者應規劃及訂定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，使所屬人員知悉計畫並據以為執行，方可謂完成計畫之訂定。安全維護計畫訂定後，應依第十七條第二款規定定期檢視或修正。 二、第二項明定安全維護計畫之具體內容。 三、業者依第一項規定訂定安全維護計畫後，應據以執行。依本法第二十二條規定，主管機關為執行檢查，得要求業者提出安全維護計畫實施情形，爰於第三項規定業者提出實施情形之期限及方式。
第四條　業者應對內公開周知個人資料保護管理政策，使所屬人員明確瞭解及遵循，其內容應包括下列事項之說明： 一、遵守我國個人資料保護相關法令規定。 二、以合理安全之方式，於特定目的	參考中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項（以下簡稱訂定辦法之參考事項）第二點第一款第二目，為使業者全體所屬人員對於個人資料之保護能有所體認並落實，業者應對內公開周知個人資料保護管理政策。

範圍內，蒐集、處理或利用個人資料。 三、以可期待之合理安全水準技術保護其所蒐集、處理或利用之個人資料檔案。 四、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。 五、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。 六、如委託蒐集、處理或利用個人資料者，應妥善監督受託者。 七、持續維運安全維護計畫之義務，以確保個人資料檔案之安全。	
第五條　業者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，負責下列事項： 一、個人資料保護管理政策之訂定及修正。 二、安全維護計畫之訂定、修正及執行。 個人資料保護管理政策、安全維護計畫之訂定或修正，應經業者之代表人或其授權人員核定。	一、參考本法施行細則第十二條第二項第一款，及訂定辦法之參考事項第二點第一款，為落實個人資料保護之目的，第一項規定業者應考量其業務規模及特性，衡酌經營資源之合理分配，配置管理人員及相當資源，負責訂定個人資料保護管理政策及安全維護計畫。 二、個人資料保護管理政策及安全維護計畫，須有高階管理者之支持，以確保業者能確實推動及執行，第二項規定個人資料保護管理政策及安全維護計畫之訂定或修正，應經作為高階管理者之業者代表人或其授權人員核定。
第六條　業者應定期清查確認所蒐集、處理或利用之個人資料現況，界定納入安全維護計畫之範圍。	參考本法施行細則第十二條第二項第二款及訂定辦法之參考事項第二點第二款第一目，業者訂定安全維護計畫，應先界定個人資料範圍，定期清查蒐集、處理或利用之個人資料現況。
第七條　業者應依已界定之個人資料範圍及其業務涉及個人資料蒐集、處理或利用之流程，定期評估可能產生之	參考本法施行細則第十二條第二項第三款及訂定辦法之參考事項第二點第三款，業者訂定安全維護計畫，應先就個

風險，並根據風險評估結果，採行適當之安全措施。	人資料進行風險評估，爰明定業者應定期評估其已界定之個人資料範圍，及因蒐集、處理或利用個人資料流程中，可能面臨之相關風險，並採行適當之安全措施。
第八條　業者為因應當事人個人資料被竊取、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、適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之電話專線或其他適當管道。 三、事故發生後研議其矯正預防措施之機制。 業者遇有個人資料安全事故，將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內依附表二格式通報本部，或通報直轄市、縣（市）政府時副知本部。 無法於時限內通報或無法於當次提供前項所述事項之全部資訊者，應檢附延遲理由或分階段提供。 本部或直轄市、縣（市）政府接獲第二項通報後，得依本法第二十二條至第二十五條規定為適當之處理。	一、參考本法施行細則第十二條第二項第四款及訂定辦法之參考事項第二點第四款，為降低或控制因個人資料被竊取、竄改、損毀、滅失或洩漏等事故造成資料當事人財產及非財產上之損害，第一項規定業者應訂定相關因應機制及其必要作為。又參考本法第十二條及本法施行細則第二十二條業者對當事人之通知義務，第二款規定事故發生時，業者應適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之電話專線或其他適當管道。 二、為期業者可藉由對主管機關之事故通報，充分掌握個人資料事故發生原因，並予以妥善處理，進而控制個人資料事故造成之損害並防止復發，參考行政院及所屬各機關落實個人資料保護聯繫作業要點第五點第一項第三款，於第二項規定業者遇有將危及正常營運或大量當事人權益之個人資料安全事故時，須詳實就所掌握事故相關事項，於知悉事故後七十二小時內依附表二格式向本部通報，倘通報對象為直轄市、縣（市）政府，應同時副知本部。 三、考量通報時效性，參考歐盟個人資料保護規則（GDPR）關於資料侵害發生時須向主管機關通報等規定，第三項規定未於時限內通報者應附具延遲理由、未能於當次提供通報

	事項全部資訊者應分階段提供。 四、第四項規定主管機關得視實際需求依本法第二十二條至第二十五條規定採取相關行政作為。
第九條　業者應訂定下列事項之內部管理程序： 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規定。 六、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	參考本法施行細則第十二條第二項第五款及訂定辦法之參考事項第三點，規定業者應於安全維護計畫中，訂定個人資料蒐集、處理或利用之內部管理程序，以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，包括檢視是否為特種個人資料、檢視個人資料之蒐集、處理或利用是否符合法定要件、當事人拒絕行銷之處置、當事人行使權利之處理、個人資料正確性之維護、個人資料之刪除等事項。

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。 七、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、第二項及第五項規定。 八、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規定。	
第十條　業者將個人資料作國際傳輸者，應檢視是否受本部依本法第二十一條所為之限制，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。	業者將個人資料作跨國或跨境之處理或利用時，對於我國人民隱私影響甚鉅，甚至有危及國家安全之疑慮，爰參考本法第二十一條，規定業者將當事人個人資料作國際傳輸者，應遵守本部所為之限制，並同時告知當事人相關個人資料傳輸之區域,及業者應對資料接收方(包括受業者委託或複委託者）為適當之監督。
第十一條　業者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	一、參考本法施行細則第十二條第二項第六款及訂定辦法之參考事項第四點第一款，第一項規定業者蒐集、處理或利用個人資料檔案者，應依據個人資料風險評估之結果，於安全維護計畫中訂定相關資料安全管

備份資料採取適當之保護措施。 三、傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。 業者以資通系統直接或間接蒐集、處理或利用個人資料時，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、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。 二、資通系統存有個人資料者，應設定異常存取資料行為之監控及定期演練因應機制。 三、確認蒐集、處理或利用個人資料之電腦、相關設備或系統具備必要之安全性，採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅。 四、與網路相聯之資通系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。 五、資通系統存有個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。 六、處理個人資料之資通系統進行測試時，應避免使用真實個人資料；使用真實個人資料者，應訂定使用規範。 七、處理個人資料之資通系統有變更時，應確保其安全性未降低。 八、定期檢視處理個人資料之資通系統，檢查其使用狀況及存取個人資料之情形。 九、評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。 十、其他本部公告之資料安全管理措施。	理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，說明如下： （一）第一款規定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。 （二）依本法施行細則第五條規定，本法第二條第二款所定個人資料檔案，包括備份檔案。準此，第二款規定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、備份之個人資料檔案，採取適當之保護措施。 （三）第三款規定業者傳輸個人資料時，應依不同傳輸方式及其風險評估結果，採取適當之安全措施。 二、透過資通系統蒐集、處理或利用個人資料時，若個人資料不慎外洩，將對當事人造成較大損害。為維護上開資通系統所蒐集、處理或利用個人資料之安全，並配合行政院及所屬各機關落實個人資料保護聯繫作業要點第五點第一項第二款，爰為第二項第一款至第十款規定。其中第九款隱碼機制，業者評估使用情境以決定是否以及如何採取適當之隱碼措施，例如供企業內部使用之通訊錄，於已採取其他安全維護措施情形下，或可評估不採行隱碼；另第十款授權本部公告其他資料安全管理措施，以即時符合最新技術之適當安全維護措施要求。

第十二條　業者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。	參考本法施行細則第十二條第二項第六款及訂定辦法之參考事項第四點第二款，規定業者蒐集、處理或利用個人資料檔案者，應依據個人資料風險評估之結果，於安全維護計畫中，訂定相關人員管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
第十三條　業者應定期對所屬人員，實施下列個人資料保護認知宣導及教育訓練： 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、安全維護計畫各項管理程序、機制及措施之要求。 業者對代表人、負責人或第五條所稱管理人員，另應依其於安全維護計畫所擔負之任務及角色，定期實施必要之教育訓練。 從事以網際網路方式供他人零售商品之平台業者，其安全維護計畫，應加入下列事項： 一、對其平台使用者，進行適當之個人資料保護及管理之認知宣導或教育訓練。 二、訂定個人資料保護守則，要求平台使用者遵守。	一、參考本法施行細則第十二條第二項第七款及訂定辦法之參考事項第二點第五款，第一項規定業者應定期透過認知宣導及教育訓練，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安全維護計畫中各項管理程序、機制及措施之要求。 二、為使代表人、負責人或第五條所稱管理人員，更應使其明瞭其於安全維護計畫中所擔負之任務及角色，第二項規定業者應定期實施認知宣導及教育訓練之規定。 三、有鑑於從事以網際網路方式供他人零售商品之平台業者，熟悉其提供服務所採取之個人資料安全維護措施，為使較無個人資料處理能力之平台使用者遵守個人資料保護規範及加強管理認知，並配合平台業者之個人資料安全維護措施，共同維護個人資料安全，爰參考網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法第二十條，第三項規定其安全維護計畫應加入事項。

第十四條　業者應對存有個人資料之儲存媒介物，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、針對所屬人員保管個人資料之儲存媒介物，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。	參考本法施行細則第十二條第二項第八款及訂定辦法之參考事項第四點第三款，規定業者蒐集、處理或利用個人資料檔案者，應依據個人資料風險評估之結果，於安全維護計畫中，訂定相關設備安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，包括業者用以保存個人資料之各類儲存媒介物，應具有一定保護程度之要求，例如一定程度之技術、設備、管制措施及安全環境等。
第十五條　業者應訂定個人資料安全稽核機制，定期檢查安全維護計畫執行狀況，並作成評估報告；如有缺失，應予改善。	參考本法施行細則第十二條第二項第九款及訂定辦法之參考事項第五點第一款，業者應於安全維護計畫中，訂定個人資料安全稽核機制，並定期進行內部稽核；該稽核之結果，應用以檢討修正個人資料保護管理政策、安全維護計畫及規劃相關改善措施。爰規定業者依其業務規模及特性，訂定適當之個人資料安全稽核機制，檢查執行狀況，作成評估報告及改善，並依第十六條第一項第三款規定保留處理紀錄。另為確保稽核品質，該稽核人員宜由具備管理、法制及資訊安全之人員擔任之。
第十六條　業者執行安全維護計畫時，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、處理或利用紀錄。 二、自動化機器設備之軌跡資料。 三、落實執行安全維護計畫之證據。 業者於業務終止後，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蒐集	一、參考本法施行細則第十二條第二項第十款及訂定辦法之參考事項第五點第二款，第一項規定業者應於安全維護計畫中，訂定相關使用紀錄、軌跡資料及證據保存機制，妥善保存個人資料之蒐集、處理或利用紀錄、自動化機器設備之軌跡資料及落實個人資料檔案安全維護計畫之證據等。上開落實個人資料檔案安全維護計畫之證據，係指：(一)個人資料提供或移轉第三人之紀錄，該紀錄應包括提供或移轉之對象、依據、原因、方法、時間及地點等資訊。(二)確認個人資料正確性及

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。	補充、更正之紀錄。(三)當事人行使本法第三條之權利及處理過程之紀錄。(四)個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。(五)存取個人資料系統之紀錄。(六)資料備份及確認其有效性之紀錄。(七)人員權限新增、變動及刪除之紀錄。(八)因應事故發生所採取行為之紀錄。(九)定期檢查處理個人資料之資訊系統之紀錄。(十)認知宣導及教育訓練之紀錄。(十一)稽核及改善安全維護計畫之紀錄。(十二)其他必要紀錄或證據。 二、業者業務終止後，亦即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其所蒐集、處理或利用之個人資料者，應留存相關紀錄；因業務終止而將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個人資料之合法依據。本項所稱業務終止，係指業者因結束業務經營、交易完成、特定目的消失、契約或法令規定期限屆滿等情況。 三、另本法第二十九條針對業者之損害賠償責任設有推定過失之規定，本部作為其中央目的事業主管機關，亦得依同法第二十二條規定為行政檢查，或依第四十七條至第五十條等規定為行政裁罰。為督促業者留存相關文件紀錄，俾利舉證及備供本部檢查，爰參酌本法第三十條之

	時效期間，規定相關證明文件紀錄應至少留存五年。
第十七條　業者應訂定下列整體持續改善機制： 一、安全維護計畫未落實執行時應採取矯正預防措施。 二、參酌安全維護計畫執行狀況、技術發展、業務調整及法令變化等因素，定期檢視或修正。	參考本法施行細則第十二條第二項第十一款及訂定辦法之參考事項第二點第二款第二目及第五點第三款，規定業者應於安全維護計畫中，訂定安全維護計畫之整體持續改善機制。
第十八條　業者之資本額為新臺幣一千萬元以上或保有個人資料筆數達五千筆以上者，於安全維護計畫訂定後，第六條、第七條、第九條第八款、第十一條第二項第一款至第四款、第八款、第十二條第三款、第十三條第一項、第二項、第十五條及前條第二款之措施，應每十二個月至少實施及檢討改善一次。 業者之資本額於本辦法施行後始增資達新臺幣一千萬元以上，或因直接或間接蒐集而保有個人資料達五千筆以上者，應自符合條件之日起六個月後，每十二個月至少實施及檢討改善前項措施一次。 前二項所定資本額，於股份有限公司為實收資本額，於有限公司、無限公司及兩合公司為登記之資本總額，於獨資或合夥方式經營之事業，為登記之資本額。 因刪除、銷毀或其他方法致保有個人資料筆數減少，且連續二年期間保有個人資料筆數未達五千筆之業者，得不適用第一項規定。但嗣後因直接或間接蒐集而致保有個人資料筆數達五千筆以上者，應於保有筆數達五千筆以上之日起三十日內，恢復適用第一項規定。保有個人資料筆數之計算，以業者單日所保有之個人資料	一、參考網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法對於適用範圍規定為資本額一千萬元以上，以及檢視歷年調查有疑似個人資料外洩之電腦系統設計服務業、入口網站經營、資料處理、網站代管及相關服務業，及其他資訊供應服務業，其資本額多在一千萬元以上。為避免業務規模較小之業者負擔過多成本訂定及執行安全維護計畫，第一項規定一定資本額以上之業者，就部分安全維護措施採取執行頻率分級管理，應於安全維護計畫訂定後，每十二個月至少實施及檢討改善一次相關措施。另鑒於部分中小型企業可能保有可觀個人資料筆數，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，除資本額一千萬元以上之業者外，將保有五千筆以上個人資料筆數之業者亦納入第一項義務。 二、考量業者落實相關安全維護措施需一定時間，爰於第二項規定業者應實施及檢討改善第一項措施之期限，使業者於因應本辦法時有所緩衝。另，本辦法稱以上者俱連本數計算。

為認定基準。	三、第三項規定第一項及第二項「資本額」之規定，不適用於財團法人，其適用第一項及第二項規定，僅以保有個人資料筆數計算。所稱「資本額」，指於經濟部商業司商工登記公示資料可得查詢之內容，股份有限公司為「實收資本額」，有限公司、無限公司與兩合公司為「資本總額」，獨資或合夥為登記之「資本額」。 四、考量業者可能因為業務規模或經營之改變等因素，致保有個人資料筆數有所增減，考量業者法令遵循之成本，爰於第四項規定不再適用第一項及重新適用第一項之情形。所稱保有個人資料，係指蒐集、處理或利用個人資料。
第十九條　業者受委託蒐集、處理或利用個人資料者，應遵循委託者之中央目的事業主管機關所定之個人資料相關法規。 業者委託他人蒐集、處理或利用個人資料者，應對受託者依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。	一、鑑於數位經濟相關產業業者商業模式多元，可能是委託他人蒐集、處理或利用資料，也可能是受託者，為再次明確本法關於委託與受託之義務，故於本條明定於受託或委託而蒐用資料時應遵循之義務。 二、依本法第四條及本法施行細則第七條規定，非公務機關受委託蒐集、處理或利用個人資料時，視同委託機關之行為。因此業者應確認委託者之業別，並遵守委託者應適用之相關法令規範，例如依本法第二十七條第三項授權中央目的事業主管機關訂定之個人資料檔案安全維護計畫或業務終止後個人資料處理方法標準等相關事項之辦法，或其他個人資料相關法規命令。爰於第一項重申本法第四條意旨，提醒業者受委託蒐集、處理或利用個人資料時，應檢視及遵守委託者之個人資料安全維護措施標準。此外，業者

	受委託蒐集、處理或利用個人資料後，又複委託給其他非公務機關蒐集、處理或利用個人資料，該其他非公務機關（即複受託者）除應遵守複委託業者（如資訊服務業）之中央目的事業主管機關所定之相關法令規範外，亦應遵循原委託者(如食藥批發零售、旅宿業、社福團體等非公務機關）之中央目的事業主管機關所定之相關法令規範。 三、參考本法第四條及本法施行細則第八條規定之意旨，及法務部一百零一年十一月二十一日法律字第一〇一〇三一〇七八〇〇號函釋:「受託為個人資料之蒐集、處理或利用者，仍以委託機關為權責歸屬機關。為釐清責任歸屬，委託機關應對受託者為適當之監督，以確保委託處理個人資料之安全管理。」爰於第二項重申，業者委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督，並於委託契約或相關文件中，明確約定其內容。
第二十條　本辦法自發布日施行。	本辦法之施行日期。

附表一

行政院主計總處行業統計分類 分類編號及行業名稱		適用本辦法之行業
4871	電子購物及郵購業	從事以網際網路方式零售商品之行業（不含電視、廣播、電話等其他電子媒介及郵購方式）
582	軟體出版業	軟體出版業
620	電腦程式設計、諮詢及相關服務業	電腦程式設計、諮詢及相關服務業
6312	資料處理、主機及網站代管服務業	從事代客處理資料、主機及網站代管以及相關服務之行業（不含線上影音串流服務）
639	其他資訊服務業	其他資訊服務業
6699	未分類其他金融輔助業	第三方支付服務業（不含其他金融輔助業）

附表二　業者個人資料外洩通報表

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>業者名稱

通報機關</td><td colspan="2">通報時間:　年　月　日　時　分
通報人:　　簽名(蓋章)
職稱:
電話:
Email:
地址:</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個人資料侵害之總筆數(大約)
_____筆</td></tr>
<tr><td>□一般個人資料_____筆
□特種個人資料_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於知悉個人資料外洩後 72 小時通報</td><td colspan="2">□是　　□否，理由：</td></tr>
</table>