**附錄4：資服業者落實個人資料安全維護計畫自我檢查表範例**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **資服業者落實個人資料安全維護計畫自我檢查表** | | | | |
| **業者名稱：** | | | **檢查時間：** | **檢查人：** |
| **編號** | | **檢查項目** | **適用情形** | **檢查情形說明** |
| **1.** **配置管理之人員及相當資源** | | | | |
| **1.1配置個資保護總負責人** | | | | |
| 1.1.1 | | 由高階管理者擔任個資安全總負責人  可由總經理、代表人擔任、副總經理級或資安長級擔任 | □適用  □不適用  說明： | □由 (職位)擔任個資安全總負責人  □業者之代表人或其授權人員核定業者安全維護計畫、個資保護政策  □確保有關個資安全角色與職權之分配與傳達  □統籌各部門、協調與推動個資安全相關事宜及所需之資源  □檢驗所有資訊保護的防護措施的正確完成執行  □其他： |
| **1.2建立個資小組及配置個資管理專員** | | | | |
| 1.2.1 | | 建立個資小組 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第5條  □不適用  說明： | □建立個資小組  □訂定及修正安全維護計畫、個資保護政策  □由高階管理者擔任個資小組總召集人  □配置聯絡窗口、安全維護計畫檢核人員、資訊人員、執行人員等  □其他： |
| 1.2.2 | | 配置管理人員（一位或以上） | □適用  □不適用  說明： | □有配置管理人員辦理個資安全維護事項之落實  □（建議）業者之總管理人員為專責/職人員  □各部門配置管理人員  □其他： |
| **2.界定及盤點個人資料之範圍** | | | | |
| **2.1蒐集處理利用個人資料之告知** | | | | |
| 2.1.1 | | 「蒐集處理利用個人資料」告知義務  除有免告知事由，應對資料當事人踐行告知「當事人得行使權利」之義務 | □適用  個人資料保護法第8條 | □蒐集、處理、利用個人資料時有皆盡告知義務 |
| **2.2界定個人資料之範圍** | | | | |
| 2.2.1 | | 蒐集、處理、利用個資之對象 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第6條  □不適用  說明： | □員工  □客戶承辦人  □上下游供應商承辦人  □受委託處理個資  □維修時接觸個資  □其他： |
| 2.2.2 | | 界定個人資料範圍 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第6條  □不適用  說明： | □定期界定頻率：  □確實盤點公司保有或可控制之所有個資  □敘明個資蒐集之特定目的、個資類別、處理或利用方式、處理或利用期間  □其他： |
| **2.3個人資料盤點（清查）** | | | | |
| 2.3.1 | | 清查確認所蒐集、處理或利用之個人資料現況  建議可使用「分析個資流程」方式 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第6條  □不適用  說明： | □定期清查頻率：  □清查各作業流程表單及紀錄，辨識、歸納、整理成個人資料檔案  □使用個人資料盤點表檢視個資檔案，確認檔案名稱、保有依據、特定目的、個資種類  □使用個人資料盤點表檢視個資檔案之生命週期過程內容及是否合法  □其他方式： |
| **3.風險評估與管理機制** | | | | |
| **3.1風險評估** | | | | |
| 3.1.1 | | 營運風險評估 | □適用  □不適用  說明： | □識別委託者業別  □識別應遵循法令及評估法遵成本風險  □識別應遵守契約條款及評估遵守契約成本風險  □其他： |
| 3.1.2 | | 系統或設備之風險評估 | □適用  □不適用  說明： | □評估業者內部電腦及資訊系統  □評估儲存客戶之消費者個資之系統或設備  □其他： |
| 3.1.3 | | 蒐集、處理、利用作業之風險評估  蒐集、處理與利用可能產生的各種作業情境及內容 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第7條  □不適用  說明： | □定期評估頻率：  □加工（例如輸入、編輯、輸出、掃描等）  □內部傳輸（例如E-mail、網路伺服器）  □外部傳輸（例如E-mail、網路伺服器）  □保管儲存（載體包含個人電腦、資料庫、主機伺服器）（不當存取、個人電腦遭外部攻擊）  □廢棄（例如刪除、資料銷毀不夠落實致外洩）  □其他： |
| **3.2風險管理** | | | | |
| 3.2.1 | | 風險管理  針對風險評估結果提出預定或已採取之具體風險管理措施或風險處理對策 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第8條  □不適用  說明： | □加工管理方式：  □內部傳輸管理方式：  □外部傳輸管理方式：  □保管儲存管理方式：  □廢棄管理方式：  □其他： |
| **4.事故之預防、通報及應變機制** | | | | |
| **4.1事故應變** | | | | |
| 4.1.1 | | 事故發生時應變  列舉發生時、發生後之可能做法或執行流程，包含降低、控制當事人損害之方式 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第8條  □不適用  說明： | □建立做法或執行流程機制  □立即通報主管機關機制  □立即通知客戶機制  □協助客戶通知消費者機制  □調查事件成因機制  □立即採取補救措施（尋找惡意程式等）機制  □重新評估與客戶間資安責任  □至少一年一次事故演練並檢討  □其他： |
| **4.2事故通報** | | | | |
| 4.2.1 | | 通報主管機關  敘明以下內容  通報時點：知悉發生事故72小時內  通報條件：資服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。  通報對象：資服業者應通報數位發展部，或通報地方政府時副知數位發展部。  通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。  延遲通報：無法於時限內通報或無法於當次提供通報內容中的全部資訊時，應附延遲理由或分階段提供。 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第8條 | □通報時點：  □通報條件：  □通報對象：  □通報內容：  □延遲通報：  □其他： |
| 4.2.2 | | 資服業者通知客戶及其消費者  敘明以下內容  通知時點：盡速。  通知事由：資服業者遇有客戶之消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。  通知內容：使客戶知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。  通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。 | □適用  □不適用  說明： | □通知客戶  □協助通知消費者  □通知時點：  □通知條件：  □通知內容：  □其他： |
| 4.2.3 | | 業者通知消費者  敘明以下內容  通知時點：盡速。  通知事由：業者遇有消費者個資被竊取、洩漏(個資外洩)或竄改、損毀、滅失之事故。  通知內容：使消費者知悉個資遭竊取、已採取的因應措施、通知當事人的時間和方法。  通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。 | □適用  □不適用  說明： | □通知消費者  □通知時點：  □通知條件：  □通知內容：  □其他： |
| **4.3事故修補改善及預防措施** | | | | |
| 4.3.1 | | 事故發生後矯正  研議矯正改善措施之機制 | □適用  □不適用  說明： | □建立做法或執行流程  □改善資安措施（必須採取）  □改變個資蒐集處理利用方式（選擇採取）  □重新評估與客戶間資安責任  □其他： |
| **5.內部管理程序** | | | | |
| **5.1個人資料之蒐集、處理或利用程序** | | | | |
| 5.1.1 | | 特種個資 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第1款  □不適用  說明 | □蒐集、處理或利用特種個資  □檢視是否符合個資法第6條第1項但書所定情形  □其他： |
| 5.1.2 | | 一般個資蒐集或處理 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第2、4款  □不適用  說明 | 每筆個資檔案皆有紀錄：  □以何種方式蒐集之個人資料  □如何向當事人告知蒐集之目的，或變更使用之目的  □蒐集符合個資法第19條第1項之何項法定依據  □以符合法規要求方式取得當事人同意  □以最小化原則蒐集  □以何種方式處理  □其他： |
| 5.1.3 | | 一般個資利用 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第3款  □不適用  說明 | □敘明以何種方式利用及行銷  □敘明拒絶行銷時的後續處理機制為何  □其他： |
| **5.2受理當事人行使權利之程序** | | | | |
| 5.2.1 | | 受理程序  於個人資料安全維護計畫中敘明受理當事人行使權利之程序 | □適用  □不適用  說明： | □建立受理當事人行使權利之程序  □使當事人知悉受理程序流程  　□以文字使當事人知悉  　□以流程圖使當事人知悉 |
| 5.2.2 | | 拒絕行銷  利用個資行銷而當事人表示拒絕接受行銷者，確保符合個資法第20條第2、3項規定 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第5款  □不適用  說明： | □當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷  □首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用  □提供當事人免費、快速、容易表達之簡便方式 |
| 5.2.3 | | 當事人行使個資法第3條權利  當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。  除有免告知事由，應對資料當事人踐行告知「當事人得行使權利」之義務 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第6款  □不適用  說明 | □告知當事人得依個資法第3條規定得行使之權利及方式  □至少與蒐集當事人個資相同之方式、管道、難易度相同。  □受理後處理方式是否包含：  □確認當事人或其代理人之身分  □檢視是否符合個資法第10條但書、第11條第2項但書及第11條第3項但書得拒絕其請求之事由  □拒絕當事人行使權利者，應附理由通知當事人  □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13條之規定  □當事人請求更正或補充其個人資料者，其應釋明之事項  □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 |
| 5.2.4 | | 個資更正  維護個資正確性之機制 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第7款  □不適用  說明 | □維護個人資料之正確，並主動或依當事人之請求更正或補充之。  □提供當事人免費、快速、容易表達之簡便方式請求更正或補充之。  □個資正確性有爭議時，以個資法第十一條第一項、第二項及第五項規定處理。 |
| **5.3國際／境外傳輸** | | | | |
| 5.3.1 | | 是否有國際／境外傳輸  業者之伺服器或資料庫位在我國以外之國家地區，則有個人資料為國際／境外傳輸之情形 | □適用  □不適用  說明： | □有國際／境外傳輸  □傳輸地區：  □傳輸方式：  □無國際／境外傳輸 |
| 5.3.2 | | 檢視是否受主管機關數位發展部限制 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第10條  □不適用  說明： | □有檢視限制  □未檢視限制  □限制內容： |
| 5.3.3 | | 告知「個資有國際／境外傳輸」義務 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第10條  □不適用  說明： | □告知客戶，其消費者之個人資料會傳輸至我國以外區域處理、利用  □告知個資當事人，其個人資料會傳輸至我國以外區域處理、利用 |
| **5.4委託他人蒐集、處理或利用個人資料之管理程序** | | | | |
| 5.4.1 | | 委託他人蒐集、處理或利用個人資料之管理程序 | □適用  個人資料保護法施行細則第8條  □不適用  說明： | □無委託他人蒐集個人資料之情形  □有委託他人蒐集、處理或利用個人資料，受託者進行個資安全維護之監督管理  □預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間  □於契約中敘明個資安全維護責任之事項  □對受託者1年檢查 次受託者採取措施  □受託者複委託時有監督複受託者  □受託者或其受僱人違反個資相關法規時，向本公司通知事項及採行補救措施  □本公司對受託者有保留指示者，其保留指示之事項  □委託關係終止或解除時，個資載體之返還，及受託者履行委託契約以儲存方式而持有之個資料刪除 |
| **5.5業務終止後有關於個人資料之處理方式** | | | | |
| 5.5.1 | | 特定業務減少或終止 | □適用  □不適用  說明： | □建立業務項目終止時個資處理方式  □個資刪除或移轉之程序及佐證  □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據  □使資料當事人知悉其個資被移轉至他業者  □使當事人能行使個資法第3條之權利 |
| 5.5.2 | | 法人格消滅 | □適用  □不適用  說明： | □建立法人格消滅時個資處理方式  □個資刪除或移轉之程序及佐證  □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。  □使資料當事人知悉其個資被移轉至他業者  □使當事人能行使個資法第3條之權利 |
| 5.5.3 | | 個資移轉予其他法人 | □適用  □不適用  說明： | □建立移轉個資處理方式  □個資刪除或移轉之程序及佐證  □個資移轉之原因、對象、方法、時間、地點、受移轉對象得保有該個人資料之合法依據。  □使資料當事人知悉其個資被移轉至他業者  □使當事人能行使個資法第3條之權利 |
| 5.6**定期檢視特定目的是否已消失或期限已屆滿** | | | | |
| 5.6.1 | | 特定目的已消失或期限已屆滿 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第9條第8款  □不適用  說明 | □定期檢視頻率：  □敘明以何種方式檢視特定目的已消失或期限已屆滿：  □敘明已消失或已屆滿後主動刪除  □其他： |
| **6.** **資料安全管理及人員管理** | | | | |
| **6.1基本資料安全管理措施** | | | | |
| 6.1.1 | 基本資料安全管理措施 | | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第11條第1項  □不適用  說明： | □資料加密機制：  □對備份資料採取適當保護措施  □傳輸資料時採取適當保護措施：  □其他： |
| **6.2以資通系統處理個資之資料安全管理措施** | | | | |
| 6.2.1 | 以資通系統蒐集、處理或利用以公司自己名義保有之個資  以公司自己名義保有個資，係指員工個資、企業客戶聯繫個資、供應商聯繫個資、消費者個資等 | | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第11條第2項  □不適用  說明： | □外部網路入侵對策  □定期執行頻率：  □防火牆更新頻率：  □應用程式防火牆更新頻率：  □電子郵件過濾機制更新頻率：  □端點防護更新頻率：  □入侵偵測設備：  □異常存取資料行為之監控及因應演練  □定期執行頻率：  □檢測系統漏洞及修補  □定期執行頻率：  □檢測工具：  □檢測時間及頻率：  □修補情形：  □防毒軟體及惡意程式檢測  □防毒軟體隨時更新及執行  □惡意程式檢測執行頻率：  □密碼及認證機制  □密碼符合一定複雜度：  □其他認證機制  □避免利用真實個資測試  □資訊系統變更時確保其安全性未降低  □定期檢查資通系統使用情況及個資存取情形  □定期執行頻率：  □個資（傳輸時）隱碼  □傳輸時  □提供電子商務時  □其他使用情境：  □其他： |
| 6.2.2 | 受委託以資通系統蒐集、處理或利用以客戶名義保有之個資  例如代管伺服器、代維運系統、提供雲端服務等 | | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第11條第2項  □不適用  說明： | □外部網路入侵對策  □定期執行頻率：  □防火牆更新頻率：  □應用程式防火牆更新頻率：  □電子郵件過濾機制更新頻率：  □端點防護更新頻率：  □入侵偵測設備：  □異常存取資料行為之監控及因應演練  □定期執行頻率：  □檢測系統漏洞及修補  □定期執行頻率：  □檢測工具：  □檢測時間及頻率：  □修補情形：  □防毒軟體及惡意程式檢測  □防毒軟體隨時更新及執行  □惡意程式檢測執行頻率：  □密碼及認證機制  □密碼符合一定複雜度：  □其他認證機制  □避免利用真實個資測試  □資訊系統變更時確保其安全性未降低  □定期檢查資通系統使用情況及個資存取情形  □定期執行頻率：  □個資（傳輸時）隱碼  □傳輸時  □提供電子商務時  □其他使用情境：  □其他： |
| **6.3人員安全管理措施** | | | | |
| 6.2.1 | | 基本人員安全管理措施 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第12條  □不適用  說明： | □人員保密義務約定  □識別業務內容涉及個資蒐集、處理或利用之人員  □人員存取權限之控制  □人員離退時之資料返還  □其他： |
| 6.2.2 | | 分散式管理或沒有固定辦公場所之人員安全管理措施  例如制定自帶裝置（BYOD）安全政策、遠距辦公設備安全政策 | □適用  □不適用  說明： | □有訂定相關安全管理機制：  □人員存取紀錄  □資料返還紀錄  □其他： |
| **7. 認知宣導及教育訓練** | | | | |
| **7.1內部員工教育訓練** | | | | |
| 7.1.1 | | 內部員工教育訓練  訓練內容：個人資料保護相關法令之規定；所屬人員之責任範圍；本計畫各項管理程序、機制及措施之要求  頻率：敘明實施頻率，規模較小業者至少於業者資安或個資政策更新時實施。  程序；訂定實施頻率；每次宣導或訓練時訂定主題、議程，且實施簽到、製作會議紀錄、課後評量機制 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第13條  □不適用  說明： | □訓練內容：  □訓練頻率：＿＿＿至少1次  □訓練紀錄：  □其他： |
| 7.1.2 | | 個資小組人員（代表人、負責人及管理人員）特殊教育訓練 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第13條  □不適用  說明： | □訓練內容：於安全維護計畫所擔負之任務及角色  □訓練頻率：＿＿＿至少1次  □訓練紀錄：  □其他： |
| **7.2外部客戶認知宣導** | | | | |
| 7.2.1 | | 外部客戶認知宣導 | □適用  □不適用  說明： | □契約簽訂前向該客戶揭露其個人資料安全維護措施  □使客戶認知使用系統時所需安全環境  □其他認知宣導措施： |
| **8.設備安全管理措施** | | | | |
| 8.1 | | 儲存媒介物設備安全管理措施  儲存媒介物：紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或其他自動化設備等 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第14條  □不適用  說明： | □設備維護安全管理措施  □儲放環境安全管理措施  □人員保管規範  □人員進出管制規範  □過期資料及軟硬體的處理方式  □其他： |
| **9.使用紀錄、軌跡資料及證據保存** | | | | |
| 9.1 | | 使用紀錄及軌跡資料證據保存  至少五年：a.個人資料使用紀錄；b.自動化機器設備之軌跡資料；c.落實執行個人資料檔案安全維護計畫之證據  自動化機器設備之軌跡資料：例如網頁日誌（web LOG）、伺服器或系統登入日誌（Logon LOG）、防火牆 IP LOG、資料庫存取LOG、作業系統事件日誌（OS event LOG）等 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第16條第1項  □不適用  說明： | □個資之蒐集、處理或利用紀錄  □保存方法：  □保存地點：  □保存\_\_\_\_年  □自動化機器設備之軌跡資料  □保存方法：  □保存地點：  □保存\_\_\_\_年  □落實執行個人資料檔案安全維護計畫之證據  □保存方法：  □保存地點：  □保存\_\_\_\_年  □其他： |
| 9.2 | | 因業務終止而銷毀證據保存 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第16條第2項  □不適用  說明： | □有紀錄銷毀方法、時間、地點及證明銷毀之方式  □有紀錄移轉原因、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  □其他： |
| **10.資料安全稽核機制** | | | | |
| 10.1 | | 自我檢查個資安全維護  訂定機制文件（含檢查頻率、檢查程序、檢查範圍、檢查人員、檢查紀錄、改善紀錄、審核等） | □適用  □不適用  說明： | □訂定機制文件  □1年至少\_\_\_\_次自我檢查個資安全維護執行狀況  □提出評估報告  □採行改善機制  □其他： |
| 10.2 | | 內部個資安全維護稽核機制  訂定機制文件（含稽核頻率、稽核程序、稽核範圍、稽核人員、稽核紀錄、改善紀錄、審核等） | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第15條  □不適用  說明： | □訂定機制文件  □1年至少\_\_\_\_次內部稽核個資安全維護執行狀況  □內稽人員資格  □合格稽核資格  □管理人員  □法制人員  □資訊安全人員  □稽核結果之處理  □作成評估報告  □保留稽核紀錄  □回報管理階層審查  □立即檢討改善  □修正個資安全維護計畫  □其他： |
| 10.3 | | 外部個資安全維護稽核機制 | □適用  □不適用  說明： | □委請第三方稽核  □委請第三方驗證機構稽核  □其他： |
| 10.4 | | 執行頻率檢查 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第18條  □不適用  說明： | □資本額1000萬元以下或保有個資5000筆以下者，定期 執行一次安全維護措施  □資本額1000萬元以上或保有個資5000筆以上者，有定期每12個月執行一次安全維護措施  □界定個人資料之範圍  □個人資料之風險評估  □檢視個資蒐集目的是否已消失  □防止外部網路入侵對策  □演練異常存取行為因應機制  □檢測系統漏洞及修補  □更新及執行防毒軟體及檢測惡意程式  □檢查資通系統使用狀況及存取個資情形  □檢視個資存取權限  □全體員工教育訓練  □代表人及管理人員教育訓練  □資料安全稽核機制  □檢視安全維護計畫執行狀況及修正計畫  □其他： |
| **11.持續改善措施** | | | | |
| 11.1 | | 持續改善措施 | □適用  數位經濟相關產業個人資料檔案安全維護管理辦法第17條  □不適用  說明： | □敘明安全維護計畫未落實執行時應採取矯正預防措施  □敘明定期檢視或修正本計畫  □其他： |