個人資料保護補充約定

（一）本約定所稱「個人資料」，指「個人資料保護法」（以下簡稱個資法）第 2 條第 1 款所定義之範圍。

（二）廠商如因規模、性質或其他事由，部分無法符合本約定時，廠商應事先提出擬排除項目、原因、風險評估及替代改善措施，經機關審查同意排除之；前開擬排除項目，不包括法令規定之必要事項。

（三）廠商依本契約受機關委託蒐集、處理或利用個人資料時，應遵守下列約定：

1. 廠商基於本契約蒐集、處理或利用個人資料時，應符合個資法第15條或第16條要件等相關規定。
2. 廠商基於本契約蒐集、處理或利用特種個人資料時，應遵守個資法等相關規定，並檢附符合個資法第6條第1項但書各款任一要件之說明。
3. 廠商不得利用機關所提供或因執行本契約所蒐集之個人資料，為自己或他人利益從事本契約委託範圍以外之處理或利用行為，包括但不限於行銷或商業推銷等相關活動、連結比對廠商本身保有資料進行處理利用，或以任何方式或方法交付予履約無關之第三人。
4. 廠商僅得於機關以下指示之範圍內，蒐集、處理或利用個人資料：

   □預定蒐集、處理、利用

   (1)特定目的：

   (2)期間：

   (3)地區：

   (4)對象：

   (5)利用方式：

   □詳需求規範書。

   □機關保留指示之事項。

   □其他指示：

5. 廠商認為機關之指示有違反個資法、其他法律或法規命令者，應立即通知機關。

（四）安全措施

1. 廠商在執行業務所必須之範圍內，應依個資法第27條規定採行個資法施行細則第12條所規定之安全措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。
2. 前款安全措施應包含下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：
   (1) 配置管理之人員及相當資源。
   (2) 界定個人資料之範圍。
   (3) 個人資料之風險評估及管理機制。
   (4) 事故之預防、通報及應變機制。
   (5) 個人資料蒐集、處理及利用之內部管理程序。
   (6) 資料安全管理(含備援機制)及人員管理。
   (7) 認知宣導及教育訓練。
   (8) 設備安全管理。
   (9) 資料安全稽核機制。
   (10) 使用紀錄、軌跡資料及證據保存。
   (11) 個人資料安全維護之整體持續改善。
   (12) 其他本機關書面指示業務執行應注意事項。
3. 廠商因履行本契約，其負責蒐集、處理或利用個人資料之員工於契約期間內離職或留職停薪，廠商應於該員工離職或留職停薪日起__日內(視採購案規模及需求約定日數，以上文字參考後刪除)說明所負責系統之存取權限及完成鎖定帳號或停止系統權限之時點，並應更換離職或留職停薪職員工曾接觸之密碼。

（五）複委託予第三人執行

□廠商執行本契約，就涉及蒐集、處理或利用個人資料之業務，不得複委託第三人執行。

□廠商執行本契約，就涉及蒐集、處理或利用個人資料之業務，得複委託第三人執行（含資料上傳雲端平台），規定如下：

1. 廠商執行本契約，就涉及蒐集、處理或利用個人資料之業務擬複委託予第三人執行者，應事先取得機關書面同意。廠商於取得機關書面同意前，應先提供該第三人之名稱、聯絡資料、保密同意書及說明複委託執行業務之範圍或事項，與該第三人具備執行、配合本契約約定之能力之相關書面資料或該第三人出具之聲明書。
2. 廠商應依第1款規定限定受複委託第三人蒐集、處理、利用個人資料之範圍，並對該受複委託第三人依個資法相關規定進行適當之監督。受複委託第三人於委託範圍內蒐集、處理、利用個人資料之行為，視同廠商行為，廠商應負所有責任。
3. 廠商與該第三人之間應以契約約定，該第三人應在受複委託之範圍內負擔與廠商相同之本契約下之廠商義務與責任，機關並得直接對該第三人進行查核或要求改正。
4. 廠商並應確保該第三人，於受託執行業務期間屆滿或經機關要求時，將因履行複委託業務而取得之個人資料全數返還予廠商或機關其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予其他第三人利用；並提供該第三人刪除、銷毀或返還個人資料之時間、方式、地點等紀錄或證明。
5. 廠商如需將個人資料儲存或備份於第三人之雲端平台，亦為本契約所約定之複委託，除依前4款之約定辦理外，廠商於取得本機關書面同意前，除第1款文件外，應另提供評估個人資料之敏感性、儲存或備份於雲端平台之必要性、雲端平台服務之安全性、雲端平台服務業者是否可以配合刪除個人資料等事項之書面報告。
6. 廠商委由雲端平台服務業者提供雲端平台以履行契約時，本機關得指示廠商另行與該雲端平台服務業者約定安全維護措施，例如資料備援機制等。

（六）當事人權利行使時之義務

機關若受理當事人依個資法第3條規定行使當事人權利時，廠商應於機關指定期限內，配合提供必要資料或說明；當事人若逕向廠商及其受託人行使個資法第3條所定權利者，廠商及其受託人應依相關規定予以答覆，於有疑義時應通知機關協助處理，並留存所有紀錄以供機關查核。

（七）配合義務

1. 廠商依個資法第15條第2款或第16條但書第7款規定，經當事人同意而為蒐集或特定目的外利用時，就該同意內容與取得方式應事先送交機關審查。廠商依個資法第6條第1項第6款規定，經當事人書面同意而為蒐集、處理及利用者，亦同。
2. 機關於本契約期間內，得要求廠商提供或說明涉及個人資料業務之處理流程相關資料(包括但不限於所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理利用等相關資料)，廠商不得拒絕，並應於機關指定期限內提供。

（八）緊急事故通知義務

1. 廠商有因執行本契約，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，於發現後，應立即通知機關，並配合機關調查及採取因應措施，以避免或降低損害。
2. 前款因應措施，包括但不限於下列項目：
   (1) 中斷入侵或洩漏途徑。
   (2) 緊急儲存尚未被破壞資料。
   (3) 啟動備援程序或替代方案。
   (4) 事件原因初步分析。
   (5) 評估受侵害個人資料類別及數量。
   (6) 檢視防護及監測設施功能。
   (7) 記錄事件經過。

(8) 內部調查完成前保存相關證據。

(9) 提出解決或修復方案。

(10) 通知保有相同資料組室或其他單位。

(11) 洽商專業人員協助或進駐處理。

(12) 涉及刑事責任者，移請檢警鑑識或調查。

(13) 發布新聞稿、網站公告。

3. 個資事件發生後，廠商應配合機關依個資法第12條規定通知當事人，內容包括侵害事實及因應措施說明、建議當事人處理事項、提供查詢及協助管道、賠(補)償當事人處理事務相關費用等補救措施。前開通知，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

4. 因本點調查、採取因應及補救措施、通知當事人而衍生之相關費用，由廠商支付。

(九) 定期查核

1. 廠商應定期（每　　）自我查核個人資料安全措施之執行情形，記錄於「個人資料委外廠商自我查核檢查表」，並提供作業說明及佐證資料，向機關提報備查。

2. 機關於必要時，得派員或委託專業人員監督廠商執行自我查核，亦得派員或委託專業人員進行實地查核，並記錄於「個人資料委外作業查核檢查表」，廠商應予配合。

(十) 履約中或契約終止時資料的刪除或返還

1. 除機關、廠商雙方另有約定或法律另有規定外，廠商應於受託執行業務期間屆滿或經機關要求時，將因履行受託業務而取得之個人資料全數返還予機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予第三人利用；並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄。

2. 前款返還，廠商得以交付機關指定之第三人為之。

3. 第1款刪除、銷毀作業，機關於必要時，得實地查訪，廠商應予配

合。

(十一)廠商履行本約定，如有應改善之缺失，機關得以書面敘明理由請廠商限期改善。

(十二)廠商違反第 2 點至第 10 點，或機關依前點提出限期改善要求，廠商未依期限改善時，機關得依情節輕重為以下的處理：

1. 通知廠商終止或解除契約之部分或全部。
2. 通知廠商暫停履約。
3. 計罰【□契約總價的千分之_____】【□ _____元】懲罰性違約金，並得按次計罰。

(十三)廠商因執行本契約業務而違反個資法、個資法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。機關如因廠商執行本契約而違反個資法、個資法施行細則，而遭受損害時，得向廠商請求損害賠償。若因此遭第三人請求損害賠償時，應由廠商負責處理並承擔一切法律責任（如於訴訟中，廠商應協助機關為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償機關因此對第三人所負之損害賠償責任）。

個人資料委外廠商自我查核檢查表

查核項目	查核結果	說明	備註
1. 已識別出受委託個人資料蒐集、處理或利用個人資料之範圍、類別、特定目的及期間	□符合 □不符合 □不適用		如：於契約敘明委託範圍內涵蓋之個人資料範圍、類別、特定目的及期間
2. 已針對受委託之個人資料檔案配置管理人員及相當資源	□符合 □不符合 □不適用		如：檢視受委託範圍內是否有指派專人管理個資安全並投入足以維護安全措施之相當資源(如：人、設備等)
3. 已將受委託之個人資料檔案進行適當盤點並完成風險評鑑與處理作業	□符合 □不符合 □不適用		如：是否進行個資盤點及風險評鑑作業，並根據風險評鑑結果調整安全維護措施強度
4. 已針對受委託之個人資料檔案規劃個人資料事故通報機制(包含違反個資法、其他個人資料保護法律或法規命令時，已規劃向委託機關通知及	□符合 □不符合 □不適用		如：是否建立整體個資事故通報機制(需包含溝通管道、應變處理原則)、是否將相關通報機制納入契約條款
5. 已將受委託之個人資料檔案規劃蒐集、處理及利用程序	□符合 □不符合 □不適用		如：是否建立涵蓋全組織個人資料檔案蒐集、處理及利用程序
6. 已針對涉及受委託之個人資料人員施以宣導及教育訓練	□符合 □不符合 □不適用		如：針對涉及個人資料之人員進行宣導及教育訓練

查核項目	查核結果	說明	備註
7.已針對受委託之個人資料檔案落實安全管控措施	□符合 □不符合 □不適用		如：針對處理、儲存個人資料之設備進行網路或實體限制措施；依資料敏感程度規劃資料儲存加密、上鎖等措施
8.已將受委託之個人資料檔案納入日常或定期稽核的範圍中	□符合 □不符合 □不適用		如：定期或不定期進行稽核並將稽核發現進行矯正預防措施
9.已瞭解委託機關保留指示事項，並配合指示事項辦理相關活動	□符合 □不符合 □不適用		如：1.事先約定受託範圍內之資訊設備使用及管控， 如：禁止USB使用等 2.事先約定資料傳輸、儲存需進行加
10.已規劃當委託關係終止或解除時，將保存之個人資料或載體返還委託機關或刪除、銷毀之管理機制	□符合 □不符合 □不適用		如：以紙本或其他載體交遞資料，應具備簽收確認機制(具名)，並確認是否轉做其他使用及儲存於載體保存之資料是否如實刪除 如：內部電腦、資訊設備之共用資料夾及其他資訊出口(如網際網路、Email寄件備份等)，應一併檢查

查核項目	查核結果	說明	備註
11. 進行複委託時已將委託機關有關個資保護要求納入複委託契約之內容	□符合 □不符合 □不適用		如：是否允許複委託應納入契約規範；受託廠商及複委託廠商均應有適當個資安全維護措施及保密協議，並對複委託方進行監督

填表說明：

一、查核結果欄：由委外廠商依查核實際狀況，參考相關佐證資料填具查核結果。

(一)符合:實際作業已依查核內容制定相關規範,並已有相關實作紀錄,或已建立標準規範而尚未有實際作業。

(二)不符合：完全未依查核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

(三)不適用：實際作業排除查核內容之適用。

二、說明欄位：應記錄查核之參考佐證資料，或簡述實際作業狀況。

個人資料委外作業查核檢查表

查核項目	查核內容	查核結果	說明
1.人員及資源配置	1.1 是否已配置專責人員或組織管理及維護保有之個人資料？	□符合 □不符合 □不適用	
	1.2 配置適當資源？（如：人、設備等）	□符合 □不符合 □不適用	
2.界定個人資料	2.1 是否定義個人資料並建立盤點清冊？	□符合 □不符合 □不適用	
	2.2 個人資料是否包含特種個資？若有，是否詳述其法令依據及蒐集內容？	□符合 □不符合 □不適用	
	2.3 個資盤點是否確實？	□符合 □不符合 □不適用	
3.風險評估	3.1 進行風險評估？	□符合 □不符合 □不適用	
	3.2 製成風險評鑑表？	□符合 □不符合 □不適用	
	3.3 針對風險進行因應？	□符合 □不符合 □不適用	
4.事故通報應變	4.1 有通報及應變程序？	□符合 □不符合 □不適用	
	4.2 事故發生時確實通報？	□符合 □不符合 □不適用	當年度無事故者，4.2-4.6應填不適用

查核項目	查核內容	查核結果	說明
	4.3 事故發生後採取應變措施？	□符合 □不符合 □不適用	
	4.4 於期限內通知當事人？	□符合 □不符合 □不適用	
	4.5 事後採取預防措施？	□符合 □不符合 □不適用	
	4.6 將事故處理情形通知機關？	□符合 □不符合 □不適用	
5.蒐集處理利用之內部管理程序	5.1 資料蒐集、處理具備特定目的並具有法定要件？	□符合 □不符合 □不適用	
	5.2 依規定取得當事人同意（當事人同意之情形）？	□符合 □不符合 □不適用	
	5.3是否清楚直接或間接蒐集個人資料之適法性，如履行告知義務及時點（未履行告知義務時，是否符合免告知之情形）？	□符合 □不符合 □不適用	
	5.4 告知內容是否包含個資法第八條規定項目？	□符合 □不符合 □不適用	若符合個資法第八條第二項或第九條免告知則填不適用
	5.5 個人資料之利用，符合特定目的之範圍？	□符合 □不符合 □不適用	
	5.6 是否已訂定個人資料蒐集、處理及利用目	□符合 □不符合	

查核項目	查核內容	查核結果	說明
	的消失或屆滿之資料銷毀、刪除程序？	□不適用	
	5.7 是否有定期檢核及記錄以確認特定目的外之利用？	□符合 □不符合 □不適用	
	5.8 目的外利用是否符合法定要件？	□符合 □不符合 □不適用	
	5.9 是否利用因執行本契約所蒐集之個人資料進行行銷？	□符合 □不符合 □不適用	
	5.10 是否提供個人資料予第三人？	□符合 □不符合 □不適用	
	5.11 是否有進行複委託，進行前是否得機關同意並經複委託廠商簽訂保密協議？	□符合 □不符合 □不適用	無複委託應填不適用
	5.12 是否定期對複委託方進行監督並記錄？	□符合 □不符合 □不適用	無複委託應填不適用
	5.13 當事人權利行使流程？	□符合 □不符合 □不適用	
	5.14 將當事人權利行使回覆情形做成紀錄供機關備查？	□符合 □不符合 □不適用	
	5.15 是否清楚瞭解個人資料之使用及其保存期限？	□符合 □不符合 □不適用	
	5.16 契約終止或解除，是否刪除、銷毀所持有之個人資料？	□符合 □不符合 □不適用	

查核項目	查核內容	查核結果	說明
	5.17 契約終止或解除，是否返還個人資料之載體？	□符合 □不符合 □不適用	
	5.18 員工離職時，是否依規定繳回其使用或保管之資訊資產(如個人電腦、隨身碟)？	□符合 □不符合 □不適用	
	5.19 新承接人員是否有變更各系統密碼？	□符合 □不符合 □不適用	
6.資料安全與人員管理	6.1 是否進行去識別化作業？	□符合 □不符合 □不適用	
	6.2 是否有資料存取控制措施？	□符合 □不符合 □不適用	
	6.3 是否進行加密？	□符合 □不符合 □不適用	
	6.4 資料之傳送是否進行管控？	□符合 □不符合 □不適用	
	6.5 使用資訊系統或其他系統進行個人資料交換時，是否有採取適當保護措施(如傳輸過程中進行加密)？	□符合 □不符合 □不適用	
	6.6 是否有遠端存取控管措施(如限制遠端存取個人資料、傳輸過程加密)？	□符合 □不符合 □不適用	

查核項目	查核內容	查核結果	說明
	6.7 保有資料者是否遵守保密協定？	□符合 □不符合 □不適用	
	6.8 人員進出情形是否具體掌控？	□符合 □不符合 □不適用	
7.認知宣導與教育訓練	7.1 是否確實進行認知宣導與教育訓練？	□符合 □不符合 □不適用	
	7.2 是否進行課後評量？	□符合 □不符合 □不適用	
	7.3 是否對新進人員進行教育訓練？	□符合 □不符合 □不適用	
8.設備安全管理	8.1 是否對設備及環境進行控管與保護？	□符合 □不符合 □不適用	
	8.2 是否定期檢查或維護更新設備？	□符合 □不符合 □不適用	
	8.3 是否針對存放個人資料之媒體於報廢或再利用前進行處理(如硬碟消磁)？	□符合 □不符合 □不適用	
9.稽核機制	9.1 是否設有稽核制度？	□符合 □不符合 □不適用	
	9.2 是否定期實施稽核？	□符合 □不符合 □不適用	
10.紀錄保存	10.1 是否保存個資(含紙本及數位檔案)管理紀	□符合 □不符合	

查核項目	查核內容	查核結果	說明
	錄(如存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄)？	□不適用	
	10.2 受委託管理含有個人資料之資訊系統，是否已建立必要之使用紀錄、軌跡資料(Log Files)及證據之保存措施？	□符合 □不符合 □不適用	
11.持續改善	11.1 是否定期檢視個資保護措施？	□符合 □不符合 □不適用	
	11.2 是否針對缺失進行改善？	□符合 □不符合 □不適用	
	11.3 是否依機關所提出之建議進行改善？	□符合 □不符合 □不適用	

填表說明：

一、查核結果欄：依查核實際狀況，參考相關佐證資料填具查核結果。

(一)符合：實際作業已依查核內容制定相關規範，並已有相關實作紀錄，或已建立標準規範而尚未有實際作業。

(二)不符合：完全未依查核內容要求制定相關程序，或完全未依相關程序執行並產生實作紀錄。

(三)不適用：實際作業排除查核內容之適用。

二、說明欄位：應記錄查核之參考佐證資料，或簡述實際作業狀況。