

## 個人資料保護計畫範例

### 一、委託案件名稱：

### 二、受委託單位：

### 三、受委託處理個人資料作業全境

#### 1. 受委託之個人資料檔案

說明案件執行過程中，所直接接觸之個人資料檔案彙整清冊如表1。

- (1) **編號**為檔案唯一識別號；
- (2) **資料檔案**填入足以代表資料內容的檔案名稱；
- (3) **資料內容類別**適用「個人資料保護法之特定目的及個人資料之類別」；該檔案的儲存型式（相同檔案不同型式應分列）；
- (4) **型式**標記，若一個檔案有紙本與電子2式，須識別為2個資料檔案，分別填寫；
- (5) **資料數量**，估計作業所涉及資料量之概估；
- (6) **作業內容**，勾選受託過程中針對所列資料檔案可能的操作項目
  - 1) 蒐集：對當事人直接或由外部機關（團體或人員）間接取得當事人資料。
  - 2) 衍生：由現有檔案進行衍生。（此時資料檔案欄位應填入衍生後的檔案名稱）
  - 3) 利用：使用該當事人資料，提供該當事人本人或對外部機關（團體或人員）服務[包含對外發布資料或傳送到外部機關（團體或人員）]。
  - 4) 存取：對於該檔案進行存取。
  - 5) 保管：對於該檔案進行保存。
  - 6) 編輯：對於該檔案紀錄進行修訂或刪除。
  - 7) 傳送：指受託單位內部傳送或受託單位對本局傳送。
  - 8) 委託：委託其他第三方蒐集或處理資料。
  - 9) 終止：作業終止（例如委託終止或委託期間該檔案作業終止）針對該檔案須為處理。

表 1：個人資料檔案清冊

編號	資料檔案	個人資料 內容類別	型式	資料 數量	保管 人	作業內容								
						蒐 集	衍 生	利 用	存 取	保 管	編 輯	傳 送	委 託	終 止
			<input type="checkbox"/> 電子 <input type="checkbox"/> 紙本											
			<input type="checkbox"/> 電子 <input type="checkbox"/> 紙本											

#### 2. 受委託之個人資料檔案

附件二十二：個人資料保護計畫範例（第1版）

☐計畫契約起迄期間：自 年 月 日至 年 月 日

☐固定期間：自 年 月 日至 年 月 日

3. 蒐集作業之風險分析

☐本委託案件不涉及自外部蒐集個人資料。

☐本委託案件有直接或間接蒐集個人資料，作業模式、風險分析與處理對策彙整如下。

表 2：蒐集作業之風險分析表

編號	資料檔案	蒐集作業			具體風險描繪	風險處理對策 (管理程序)
		來源	方法	依據		
		<input type="checkbox"/> 直接向 當事人蒐 集  <input type="checkbox"/> 間接蒐 集 (來源:____) 	<input type="checkbox"/> Email  <input type="checkbox"/> 網站  <input type="checkbox"/> 電話/現 場  <input type="checkbox"/> 口頭  <input type="checkbox"/> 傳真  <input type="checkbox"/> 紙本送 達  <input type="checkbox"/> 其他:____	<input type="checkbox"/> 法定職務 (法源:____)  <input type="checkbox"/> 當事人同意 <input type="checkbox"/> 書面： (同意書如附 件____ <input type="checkbox"/> 其他： 方式____ 舉證方式 ____		

4. 衍生作業之風險分析

☐本委託案件不涉及自原始個人資料衍生新的個人資料檔案。

☐本委託案件自原始個人資料衍生新的個人資料檔案，作業模式、風險分析與處理對策彙整如下。

表 3：衍生作業之風險分析表

編號	資料檔案	衍生作業		具體風險描繪	風險處理對策 (管理程序)
		來源	衍生方法		
		原始檔案/系統 名稱:_____ 	<input type="checkbox"/> 輸入/編輯 <input type="checkbox"/> 輸出/列印 <input type="checkbox"/> 影印 <input type="checkbox"/> 掃描 <input type="checkbox"/> 備份 <input type="checkbox"/> 其他:____		

附件二十二：個人資料保護計畫範例（第1版）

--	--	--	--	--	--

5. 利用作業之風險分析

☐ 本委託案件不涉及利用個人資料檔案（含外部傳送）。

☐ 本委託案件利用個人資料檔案（含外部傳送），作業模式、風險分析與處理對策彙整如下。

表 4：利用作業之風險分析表

編號	資料檔案	利用作業			具體風險描繪	風險處理對策 (管理程序)
		利用方式	方法	利用目的		
		<input type="checkbox"/> 發布或 傳送（對 象）  <input type="checkbox"/> 其他：	<input type="checkbox"/> 人員親 送 <input type="checkbox"/> 郵寄 <input type="checkbox"/> 傳真 <input type="checkbox"/> Email <input type="checkbox"/> 網站 <input type="checkbox"/> 其他：			

6. 存取作業之風險分析

☐ 本委託案件不涉及存取現有個人資料檔案。

☐ 本委託案件存取現有個人資料檔案，作業模式、風險分析與處理對策彙整如下。

表 5：存取作業之風險分析表

編號	資料檔案	存取作業			具體風險描繪	風險處理對策 (管理程序)
		存取	方法	存取人員		
		原始檔案/ 系統名稱： _____	<input type="checkbox"/> 閱覽 <input type="checkbox"/> 內部網 路連線 <input type="checkbox"/> VPN <input type="checkbox"/> 網際網 路 <input type="checkbox"/> 網站 <input type="checkbox"/> 其他：			

7. 保管作業之風險分析

附件二十二：個人資料保護計畫範例（第1版）

☐ 本委託案件不涉及保管個人資料檔案。

☐ 本委託案件保管個人資料檔案，作業模式、風險分析與處理對策彙整如下。

表 6：保管作業之風險分析表

編號	資料檔案	保管作業		具體風險描繪	風險處理對策 (管理程序)
		保管方式	保管場地		
		<input type="checkbox"/> 儲存個人電腦（電子） <input type="checkbox"/> 儲存於可攜式媒體（USB, 記憶卡, 行動硬碟等） <input type="checkbox"/> 儲存於資料庫/主機（電子） <input type="checkbox"/> 存放個人櫃/抽屜（紙本） <input type="checkbox"/> 存放共用櫃（紙本） <input type="checkbox"/> 存放紙箱（紙本） <input type="checkbox"/> 存放檔案室（紙本） <input type="checkbox"/> 其他____			

8. 編輯作業之風險分析

☐ 本委託案件不涉及編輯（修改或刪除）個人資料檔案紀錄。

☐ 本委託案件針對個人資料檔案紀錄進行編輯（修改或刪除），作業模式、風險分析與處理對策彙整如下。

表 7：編輯作業之風險分析表

編號	資料檔案	編輯作業	具體風險描繪	風險處理對策 (管理程序)
		<input type="checkbox"/> 單筆紀錄表修訂（或廢棄）（紙本） <input type="checkbox"/> 電子檔案紀錄維護（電子） <input type="checkbox"/> 應用系統操作維護（電子） <input type="checkbox"/> 資料庫紀錄操作維護（電子） <input type="checkbox"/> 其他：_____		

附件二十二：個人資料保護計畫範例（第1版）

9. 傳送（包含受託單位內部傳送或受託單位對本局傳送）作業之風險分析

☐ 本委託案件不涉及傳送個人資料檔案。

☐ 本委託案件傳送資料檔案，作業模式、風險分析與處理對策彙整如下。

表 8：傳送作業之風險分析表

編號	資料檔案	傳送作業		具體風險描繪	風險處理對策 (管理程序)
		資料流向	傳送方式		
			<input type="checkbox"/> 人員親送		
			<input type="checkbox"/> 郵寄		
			<input type="checkbox"/> 傳真		
			<input type="checkbox"/> Email		
			<input type="checkbox"/> 應用系統：		
			<input type="checkbox"/> 其他：		

10. 委託作業之風險分析

☐ 本委託案件不涉及委託第三方執行個人資料檔案作業。

☐ 本委託案件委託第三方執行資料檔案作業，作業模式、風險分析與處理對策彙整如下。

表 9：委託作業之風險分析表

編號	資料檔案	委託作業		具體風險描繪	風險處理對策 (管理程序)
		委託對象/項目	傳送檔案方式		
			<input type="checkbox"/> 人員親送		
			<input type="checkbox"/> 郵寄		
			<input type="checkbox"/> 傳真		
			<input type="checkbox"/> Email		
			<input type="checkbox"/> 應用系統：		
			<input type="checkbox"/> 其他：		

11. 終止作業之風險分析

☐ 本委託案件終止時，不必進行個人資料檔案處置。

附件二十二：個人資料保護計畫範例（第1版）

☐ 本委託案件終止時，個人資料檔案處置作業模式、風險分析與處理對策彙整如下。

表 10：終止作業之風險分析表

編號	資料檔案	終止作業		具體風險描繪	風險處理對策 (管理程序)
		處理方式	證明方式		
		<input type="checkbox"/> 刪除（電子）	<input type="checkbox"/> 作業過程錄影		
		<input type="checkbox"/> 碎紙（紙本）	<input type="checkbox"/> 由貴機關派員監督		
		<input type="checkbox"/> 銷燬（紙本）	<input type="checkbox"/> 作業具結		
		<input type="checkbox"/> 返還	<input type="checkbox"/> 其他		
		<input type="checkbox"/> 其他			

12. 其他風險分析

表 11：其他作業之風險分析表

編號	資料檔案	全景說明	具體風險描繪	風險處理對策 (管理程序)

四、受託處理期間個人資料保護方法：

依據前述全景可能產生之風險，本計畫將實施以下控制保護個人資料，以預防執行本案期間，案件相關之個人資料被竊取、竄改、毀損、滅失或洩漏。

1. 對作業之個人資料的保護原則

2. 作業程序中之個人資料的保護方法

附件二十二：個人資料保護計畫範例（第1版）

3. 對人員宣導、訓練與管理方法
4. 對作業區域與儲存區域之保護
5. 對作業區域與儲存區域所涉及之處理設備之保護
6. 對資料傳遞過程之保護
7. 對個人資料檔案作業保存之證據

**五、個人資料保護措施之檢查：**

為確保個人資料保護之落實，本計畫採用以下方式自我查核，貴機關於必要時得派員或委託專業人員監督執行自我查核，或依契約要求派員或委託專業人員進行實地查核。

1. 檢查項目表列（參閱附件）
2. 檢查周期
3. 檢查人員
4. 檢查報告與報告提交
5. 發現缺失或事故之改善方式

附件二十二：個人資料保護計畫範例（第1版）

**六、個人資料之安全事故通報應變流程：**

本計畫期間若發現資訊安全或個人資料被竊取、竄改、毀損、滅失或洩漏等事故時，將依以下程序進行通報及應變，處理完成後提交事故報告書（報告書依「經濟部標準檢驗局個人資料保護管理作業程序」附件十九「個人資料安全事故處理報告大綱」規定格式撰寫），並依貴機關要求執行通知當事人事宜。

**七、其他專案特別要求事項：**

附件

個人資料委外廠商自我查核檢查表

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。

查核項目	查核結果	說明（請填寫檢核結果或抽核發現）	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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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採行之補救措施）	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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

附件二十二：個人資料保護計畫範例（第1版）

查核項目	查核結果	說明（請填寫檢核結果或抽核發現）	備註
5. 已將受委託之個人資料檔案規劃蒐集、處理及利用程序	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用		如：針對涉及個人資料之人員進行宣導及教育訓練
7. 已針對受委託之個人資料檔案落實安全管控措施	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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、儲存需進行加密
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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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

附件二十二：個人資料保護計畫範例（第1版）

查核項目	查核結果	說明（請填寫檢核結果或抽核發現）	備註
			訊出口（如網際網路、Email 寄件備份等），應一併檢查
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	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 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