個人資料保護專案計畫書（範本）

目錄

壹、依據

依（本公司全稱）（以下稱「本公司」）與＿＿＿＿＿＿＿＿＿＿（以下稱乙方）簽訂契約、個人資料保護法（下稱「本法」）辦理。

貳、目的

為落實本公司執行清潔服務業個人資料檔案之安全維護及管理，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

參、個人資料蒐集、處理及利用程序

一、 本公司於執行清潔服務業範圍內對個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

二、 個人資料蒐集程序

(一) 本公司於執行清潔服務業範圍內如需蒐集，除本法第 6 條第 1 項所定個人資料外，應有特定目的，並符合下列情形之一者：

1. 法律明文規定。
2. 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
5. 經當事人同意。
6. 為增進公共利益所必要。
7. 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
8. 對當事人權益無侵害。

(二) 本公司新增之業務如有涉及個人資料之蒐集，應報公司內核准後為之。如必須蒐集一人以上之個人資料或為執行業務而有必要持續蒐集個人資料時，得

以一次性報請核准後為之。

(三) 本公司於執行清潔服務業範圍內如需依本法第 19 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

1. 本公司名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依本法第 3 條規定得行使之權利及方式。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

(四) 本公司於執行清潔服務業範圍內如需依本法第 19 條規定向當事人蒐集個人資料時，有下列情形之一者，得免為前項之告知：

1. 依法律規定得免告知。
2. 個人資料之蒐集係本公司履行法定義務所必要。
3. 告知將妨害公共利益。
4. 當事人明知應告知之內容。
5. 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

(五) 本公司於執行清潔服務業範圍內如需依本法第 19 條蒐集非由當事人提供之個人資料時，應於處理或利用前(或於首次對當事人為利用時併同為之)，向當事人告知個人資料來源及本法第 8 條第 1 項第 1 款至第 5 款所列應告知事項。但有下列情形之一者，得免為告知：

1. 有本法第 8 條第 2 項所列各款情形之一。
2. 當事人自行公開或其他已合法公開之個人資料。
3. 不能向當事人或其法定代理人為告知。
4. 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

三、 個人資料處理程序

(一) 本公司於執行清潔服務業範圍內如需處理，除本法第 6 條第 1 項所定個人資料外，應有特定目的，並符合本法第 19 條所定特定情形之一。

(二) 本公司於執行清潔服務業範圍內需處理個人資料時，應由蒐集個人資料之承辦人設定處理權限範圍，並報經公司內核准後為之。

(三) 本公司保有之個人資料有誤或缺漏時，應由資料蒐集承辦人報經公司內核准後，補充或更正之，並留存相關紀錄。

四、 個人資料利用程序

(一) 本公司於執行清潔服務業範圍內對個人資料之利用，除本法第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之。

(二) 本公司於執行清潔服務業範圍內對個人資料之利用，有下列情形之一者，得為特定目的外之利用：

1. 法律明文規定。
2. 為增進公共利益所必要。
3. 為免除當事人之生命、身體、自由或財產上之危險。

4. 為防止他人權益之重大危害。

5. 基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

6. 經當事人同意。

7. 有利於當事人權益。

(三) 本公司就保有之個人資料有特定目的外利用之需求時，應由承辦人報經公司內核准後為之，並留存相關紀錄。

五、 本公司於執行清潔服務業範圍內如需蒐集、處理或利用本法第 6 條第 1 項所定個人資料（有關病歷、醫療、基因、性生活、健康檢查及犯罪前科），應有下列情形之一：

(一) 法律明文規定。

(二) 非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

(三) 當事人自行公開或其他已合法公開之個人資料。

(四) 基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

(五) 為協助本公司履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

(六) 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

六、 本公司於執行清潔服務業範圍內蒐集、處理或利用之個人資料、軌跡資料及蒐集相關告知及同意證據，如無其

他法令限制，將依清潔服務業契約書規定辦理。

七、 本公司應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

八、 個人資料刪除、銷燬程序

(一) 本公司應定期檢視個人資料之有效性及可用性，刪除或銷燬不必要之個人資料（得併同個人資料盤點程序進行）。

(二) 本公司保有個人資料蒐集之特定目的消失、期限屆滿或違法蒐集時，應主動或依當事人之請求刪除或銷燬該個人資料。但因執行業務所必須或經當事人書面同意者，不在此限。

(三) 本公司於刪除或銷燬個人資料時，由承辦人報經公司內核准後為之，且應以適當方式記錄並確認其執行結果，並留存相關紀錄。

九、 個人資料之停止蒐集、處理或利用

(一) 本公司之個人資料之蒐集、處理或利用有違法之情事時，應主動或依當事人請求停止蒐集、處理或利用該個人資料。

(二) 本公司保有個人資料之正確性有爭議、蒐集之特定目的消失、期限屆滿者，應主動或依當事人之請求停止處理或利用該個人資料。但因執行職務所必須或經當事人書面同意者，不在此限。

(三) 依前開規定，擬停止蒐集、處理、利用個人資料時，

應由蒐集個人資料之承辦人報經本公司核准後為之。

(四)個人資料已停止處理或利用者，本公司應確實記錄。

十、 本公司違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

肆、受理當事人權利行使之作業程序

一、 申請人依本法第 10 條或第 11 條第 1 項至第 4 項規定向本公司請求查詢、閱覽或請求製給複製本、請求更正、補充、刪除、停止蒐集、處理或利用其個人資料時，應填具當事人權利行使申請書（附件 1），並檢附相關證明文件。

二、 申請事項如涉及個人資料之補充或更正，應請當事人載明記載錯誤或不完整事項、更正或補充之理由，並提出相關證明文件

三、 承辦人對於當事人請求答覆查詢、提供閱覽或製給複製本者，應注意有無下列不予核准之事由：

(一)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

(二)妨害公務機關執行法定職務。

(三)妨害該蒐集機關或第三人之重大利益。

四、 本公司受理當事人依本法第 10 條規定之請求，應於 15 日內，為准駁之決定；必要時，得予延長，延長之期間不得逾 15 日，並應將其原因以書面通知請求人。本公司受理當事人依第 11 條規定之請求，應於 30 日內，為准駁之決定；必要時，得予延長，延長之期間不得逾 30 日，並應將其原因以書面通知請求人。

五、 查詢或請求閱覽個人資料或製給複製本者，本公司得酌收必要成本費用。

伍、個人資料盤點管理程序

一、 個人資料盤點

(一) 本公司應定期（每年至少乙次）盤點於執行清潔服務業範圍內所需蒐集之個人資料。

(二) 為界定個人資料範圍，盤點作業應包括下列項目：

1. 檢視個人資料檔案

(1) 清查各作業流程中所使用之表單、紀錄，並辨識個人資料有關之表單、紀錄，歸納整理成個人資料檔案。

(2) 使用個人資料盤點表檢視其保有之個人資料檔案，確認個人資料檔案名稱、保有之依據及特定目的、個人資料種類。

(3) 使用個人資料盤點表檢視其保有之個人資料檔案之生命週期，包含蒐集、處理、利用之內容。

2. 建立個人資料檔案清冊

將個人資料檔案檢視之成果製作個人資料檔案清冊（附件 2），並妥善保管且定期維護該清冊。

二、 個人資料盤點表應妥善保管，承辦人亦得於個人資料檔案新增、刪除、修改或其他變動發生後，隨時更新個人資料盤點表。

陸、個人資料風險評估管理程序

本公司應訂及辦理個人資料風險評估作業。前開作業應包括下列項目：

一、 評估個人資料風險

(一)使用個人資料風險評估表就個人資料檔案內容進行價值識別。個人資料之價值識別得以個人資料之內容、個人資料之數量、個人資料檔案之識別程度，以及其他必要之項目為評估基準。

(二)於個人資料檔案內容價值識別後，應進行個人資料作業之具體風險類型識別（附件 3）。

(三)就識別出之風險，風險發生之衝擊程度及發生之可能性進行風險評估並區分等級。風險發生之衝擊程度得以損害高低以及其他必要之項目為評估基準（附件 4）。

(四)就風險發生之衝擊程度及發生之可能性進行識別後，應予以區分風險等級，並就高風險之個人資料檔案作業進行風險處理。

二、 處理個人資料風險

依風險評估結果進行風險處理，擬定具體對策。

三、 建立風險評估清冊

本公司應將風險評估之結果製作個人資料風險評估表（附件 5），並彙集成清冊後，妥善保管且定期維護之。

柒、個人資料安全管理作業程序

一、 資料安全管理

(一)本公司應建立個人資料檔案分級分類管理制度，並針對接觸人員建立安全管理規範。

(二)本公司應針對資料存取、系統存取、網路存取等設定控制機制。

(三)本公司設定資料存取控制時，應考量業務性質及作業之必要，根據資料處理之方式設計之。其處理方式包含但不限於記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或傳送。

(四)如有職務異動、變更、離職、負責人員調動、電腦報廢等因素，應立即進行權限變更。

二、 資料設備管理

(一)本公司應確實掌握蒐集、處理及利用個人資料檔案之相關業務流程負責人。

(二)於進用人員時，本公司應進行適當的安全性評估。

(三)本公司得要求相關人員簽訂保密協定，善盡保護個人資料之義務。

三、 資料設備管理

(一)個人資料檔案處理之相關設備及周邊環境應有相關控管保護機制，以確保檔案之安全性，不易遭外洩及竊取之可能。

(二)個人資料檔案處理，應有適當之監控措施，確保使用之軟/硬體設備為安全之控管版本，並應用防護及監控軟體進行個人資料保護及記錄。

四、 有關個人資料安全管理作業程序事項，本公司將參照資訊安全管理規範持續更新並辦理之。

捌、個人資料教育訓練宣導程序

一、 本公司將定期規劃個人資料保護與管理制度或個資法令之相關教育訓練，促使清潔服務業所屬人員了解個資保護之重要性，以提高蒐集、處理、利用個人資料之適法性及安全性意識，妥善保護個人資料。

二、 教育訓練之內容得包括：本法及施行細則、個人資料保護管理作業程序、個人資料盤點暨風險評估實作、個資外洩事件危機處理應變、個資保護作業內部稽核實作等。

三、 本公司為確保教育訓練之有效性，得以一定之方式（如測驗、有獎徵答、問卷調查等）進行評量。

玖、事故之預防、通報及應變程序

一、 事故通報：

本公司獲報並經初步確認屬個人資料外洩之危機事件後，應立即以電話、傳真或任何可資運用之溝通工具，將訊息傳達至公司內資深同仁乙位及主管並填寫個人資料事故通報單（附件 6）。

二、 事故應變

(一) 本公司應於接獲通報後 24 小時內進行事故分析。事故分析應包含確認事故之種類、事故嚴重程度、影響的範圍以及發生原因。

(二) 於事故分析後，應研擬事故應變處理措施避免事故擴大，並採取證據保全措施，避免異動或改變原始磁碟及證據，並填寫處理結果（同附件 6）。

(三) 於事故查明後，應即以適當方式通知當事人被侵害之事實以及已採取之措施。適當方式得依本法施行細則第 22 條規定為之。

拾、個人資料內部稽核程序

一、 本公司應定期（每年至少乙次）就執行清潔服務業範圍內所蒐集之個人資料辦理內部稽核作業。稽核人員並應於預定稽核日前一週內，製作稽核項目表予受稽核人員。

二、 稽核作業程序：

(一)稽核人員：本公司內部稽核程序之稽核人員由甲方指定稽核負責承辦人以及資深同仁乙位。

(二)稽核所發現之缺失，應作成稽核報告向公司內備查。

三、 稽核報告內容：

報告內容應包含個資管理制度之執行狀況以及稽核後之改善計畫，稽核項目如下：

(一)個人資料之蒐集、處理、利用之作業。

(二)當事人行使權利程序。

(三)個人資料盤點與風險分析。

(四)個人資料安全管理。

(五)個人資料教育訓練宣導。

(六)事故之預防、通報與應變程序。

(七)個人資料內部稽核。

(八)使用紀錄、軌跡資料及證據保存。

(九)持續追蹤改善。

拾壹、使用紀錄、軌跡資料及證據保存

一、 使用紀錄、軌跡資料、證據指下列資料：

(一)實施個人資料保護與管理制度之使用紀錄。

(二)個人資料檔案之使用紀錄或軌跡資料；前述軌跡資料指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（LOGFILES），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑…等，可用於比對、查證資料存取之適當性。

(三)其他必要之證據保存資料。

二、 作業程序

(一)使用紀錄、軌跡資料、證據之管理

1. 本公司得指定專人管理各種使用紀錄、軌跡資料、證據。
2. 各項使用紀錄、軌跡資料、證據之保存，依檔案法與相關法令及資訊安全管理規範之規定為之。

(二)使用紀錄、軌跡資料、證據之銷毀或刪除

1. 本公司應於清潔服務業執行結束後（一定期間）將超過保管期限之使用紀錄、軌跡資料、證據等銷毀或刪除。如前開使用記錄、軌跡資料、證據為電子紀錄者，本公司應向貴局出具切結書，確保前開電子紀錄業已消除或毀滅至無法回復之程度。
2. 各項使用紀錄、軌跡資料、證據之銷毀或刪除，依檔案法與相關法令及資訊安全管理規範之規定

為之。

拾貳、持續追蹤改善程序

本公司將隨時依據清潔服務業執行狀況，注意相關技術發展及法令修正等事項，檢討本公司個人資料檔案安全維護計畫是否合宜，並予必要之修正。

附件 1 當事人權利行使申請書

<table>
<tr><td>申請事項</td><td colspan="2">□查詢、閱覽□製給複製本
□補充、更正□刪除□停止處理、利用□停止違法蒐集、處理或利用</td></tr>
<tr><td>原因說明</td><td colspan="2"></td></tr>
<tr><td>欲申請之資料</td><td colspan="2"></td></tr>
<tr><td colspan="3">當事人基本資料</td></tr>
<tr><td colspan="3">姓名：
電話：
住址：
證明文件：□身分證□健保卡□駕照□護照□其他</td></tr>
<tr><td colspan="3">代理人基本資料（非本人申請時）</td></tr>
<tr><td colspan="3">代理人姓名：
代理人之住址：
代理人之電話：
與當事人之關係：
證明文件：□委託書
其他身分份證明文件：□身分證□健保卡□駕照□護照□其他</td></tr>
<tr><td>申請人簽名</td><td colspan="2">（非本人申請時，應由代理人簽名並加蓋當事人印章）</td></tr>
<tr><td>備註</td><td colspan="2">1.查詢、閱覽、製給複製本之申請於受理日起 15 日內回覆，延長期間不得超過 15 日，並且將書面通知延長原因。
2.補充、更正、刪除、停止處理、利用、停止違法蒐集處理或利用之申請，於受理日起 30 日內回覆，延長期間不得超過 30 日，並且將延長原因以書面通知當事人。
3.具有本法第 10 條但書及第 11 條但書之特定要件時，將拒絕申請，並告知原因。
4.對於查詢、閱覽、製給複製本之申請，得酌收成本費用。</td></tr>
<tr><td colspan="3">處理情形（受理單位填寫）</td></tr>
<tr><td rowspan="3">擬辦事項</td><td>是否延長回覆期間
□無延長回覆期間
□延長回覆期間，延長____天。
（延長原因：_____）</td><td>批示</td></tr>
<tr><td>准駁情形
□同意申請
□拒絕申請，（原因：_____）</td><td rowspan="2"></td></tr>
<tr><td>以上事項擬奉核示後函復當事人</td></tr>
</table>

附件 2 個人資料盤點表

單位名稱	
盤點人員	

主要業務、職掌	細部作業名稱	個人資料檔案名稱	主管單位	保有單位	檔案形態	保有依據	是否需告知	特定目的	個人資料類別
					□紙本類 □電子類 □電子檔-可攜式媒體 □系統資料庫		□Y □N		

資料來源	內部傳送	外部傳送	委外	個人資料項目	特種個人資料	保管方式	保存期限	銷毀方式	備註	單位名稱
				□姓名 □生日 □身分證號 □護照號碼 □特徵 □指紋 □婚姻 □家庭 □教育 □職業 □聯絡方式 □財務情況 □社會活動 □ 其他：_____	□無 □病歷 □醫療 □基因 □性生活 □健康檢查 □犯罪前科		□法定保存期限：_____ □ 自訂保存期限：_____			

個資盤點表填寫說明

欄位	填寫說明
主要業務、職掌	依單位業務、職掌內容、業務項目等，列出主要的作業流程名稱。
細部作業名稱	前項作業流程名稱，依其日常的辦理流程，再個別區分成細部作業。
個人資料檔案名稱	包含可識別當事人之個人資料檔案名稱。
主管單位	負責制定該個人資料檔案項目與欄位之部門。
保有單位	保存及管理個人資料檔案之部門。
檔案形態	檔案型態分為下列四種： 1.紙本類：指實體紙本文件。 2.電子類：包含報表、文件掃描檔、照片、圖片、傳真、影像檔等相關電子文件檔案，如WORD、EXCEL、PDF、WMV 等數位型式之檔案。 3.電子檔-可攜式媒體：指上述數位形式文件保存於可攜式媒體。 4.系統資料庫：指個人資料僅保存於資訊系統內，未另外列印成紙本或另存成電子檔案。需分筆列示於個人資料盤點清冊。
保有依據	是否有法定保有依據或契約。
是否需告知	請判斷是否需依本法第 8 條及第 9 條規定，蒐集、處理或利用個人資料時應明確履行告知義務。 如需告知，請填 Y；得免為告知，請填 N。
特定目的	依法務部公告之「個人資料保護法之特定目的及個人資料之類別」填寫個人資料蒐集或處理之特定目的。
個人資料類別	依法務部公告之「個人資料保護法之特定目的及個人資料之類別」填寫個人資料類別。
資料來源	該個人資料檔案取得管道或建立之方法。

內部傳送	與該個人資料檔案之蒐集、處理或利用有關之內部部門。
外部傳送	與組織之個資檔案提供外部利用有關，本項指無法歸屬於承辦人之情形。
委外	提供之服務與個資檔案之蒐集、處理及利用流程有關，且會接觸到個資內容之委外機（構）或人員。
個人資料項目	姓名、生日、身分證號碼、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等。
特種個人資料	病歷、醫療、基因、性生活、健康檢查、犯罪前科。
保管方式	該個人資料檔案之保管方式（如：放置於辦公室檔案櫃並上鎖、儲存於承辦人電腦並將檔案加密、資料庫主機…等）。
保存期限	法定保存期限：該個人資料檔案依據檔案法等相關法律規定之保存期限(如:3 年、5 年…等)，並請說明法定依據。 自訂保存期限：該個人資料檔案依據本機關自訂之保存期限（如：3 年、5 年…等）。
銷毀方式	該個人資料檔案之銷毀方式（如：由總務單位統一辦理銷毀作業…等）。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

附件 3 風險情境表

風險大分類	風險子分類	個資潛在風險事件
1.紙本類	1.1 處理	1.1.1 紙本文件於內部處理過程中，長時間不使用或下班時收存於辦公室上鎖之資料櫃。
	1.2 保存	1.2.1 紙本文件之保存（含暫存區）地點具備進出管控措施。
		1.2.2 紙本文件歸檔、入倉（庫）或集中保管前，確實清點數量及內容。
		1.2.3 紙本文件存放地點有消防、滅火、溫度控制等設施。
	1.3 傳遞	1.3.1 紙本文件於內部傳遞過程中，具有簽收/點收等控管措施。
		1.3.2 紙本文件提供外部利用均有公文往返等使用紀錄。
	1.4 銷毀	1.4.1 包含個資之紙本文件均不進行回收使用。
		1.4.2 紙本文件於內部進行銷毀時，均銷毀致無法辨識。
		1.4.3 紙本文件交由受委託廠商銷毀前，已簽訂包含雙方權利義務及賠償條款之契約或保密協議。
		1.4.4 紙本文件交由受委託廠商進行銷毀時，妥善進行監銷並留存紀錄。
2.電子類	2.1 傳輸	2.1.1 同仁透過對外寄發、傳輸個資檔案均進行加密。
		2.1.2 同仁對外傳輸個資檔案均有傳輸記錄，如 Email 寄件備份、FTP 傳輸記錄、網路硬碟等。
	2.2 保存	2.2.1 存於本機電腦之個資檔案，均有加密或存放於專用且安全之資料夾。
	2.3 銷毀	2.3.1 電子檔案保存期限屆滿後均進行

		刪除。
3.電子檔-可攜式媒體	3.1 傳遞	3.1.1 將個人資料檔案使用可攜式媒體傳遞時，均進行加密。
	3.2 銷毀	3.2.1 儲存個人資料之可攜式媒體不再使用或損毀時，均進行刪除資料或實體破壞。
4.系統資料庫	4.1 存取權限	4.1.1 資訊系統之使用者帳號均定期審查。
		4.1.2 系統具備職務區隔機制，給予適當之存取權限。
	4.2 使用紀錄	4.2.1 資訊系統具有記錄使用者活動日誌功能。
		4.2.2 單位主管或其授權人員定期審查資訊系統使用者之活動日誌。
5.委外作業類	5.1 選商	5.1.1 委外案件均會評估及選擇可提供符合組織對個人資料保護需求之受委託廠商（如一年內未曾發生個資外洩事件、重大資安事件或有無通過 ISO 27001、BS10012、TPIPAS、ISO29100 等驗證）。
	5.2 簽約	5.2.1 在委託外部單位處理個人資料有簽訂契約，並包含適當安控措施是否足夠。
		5.2.2 組織與受委託廠商所簽訂之契約中包含是否得將個人資料處理作業進行轉包/分包之規定。
		5.2.3 若允許轉包/分包，受委託廠商與其複委託廠商（下包商）所簽訂之契約已要求複委託廠商實行與受委託廠商相同等級之安控措施。
		5.2.4 組織與受委託廠商所簽訂之契約中明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式。

	5.3 履約	5.3.1 於委託外部單位處理個人資料契約期間內，定期監督或實地審查受委託廠商之安控措施是否落實執行。
		5.3.2 組織定期依據與受委託廠商所簽訂之契約進行監督，當資料逾保存期限或契約終止時確認有關個人資料之銷毀、交還原組織或其他處理之方式。
	5.4 小額採購	5.4.1 如以小額採購方式委託外部單位蒐集、處理、利用或銷毀個人資料時，均簽訂書面協議並落實監督作業。

附件 4 個資流程衝擊分析表

單位名稱	
評估人員	

作業流程名稱		衝擊分析項目				衝擊值	備註	單位名稱
主要業務、職掌	細部作業名稱	個資數量	個資敏感度	損害組織信譽	個資當事人隱私衝擊	衝擊值係以衝擊構面之評分加總		
		5:每年產生大於 1000 筆	5: 包含姓名、身分證號、私人連絡方式(電話+地址)、財務情況、指紋、特種個資	5:若作業發生個資外洩事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾集結遊行抗爭或上級機關關切等情形。	5: 洩漏資訊，對個資當事人造成重大影響，如：勒索、綁架。			
		3:每年產生 100~1000 筆	3: 包含姓名、身分證號、護照、私人聯絡方式(電話及地址)、其他非特種特資欄位	3:若作業發生個資外洩事故，將導致機關形象、信譽受到嚴重損害，如：導致 3 家以上媒體報導負面新聞或造成民眾至機關抗議或陳情等情形。	3: 洩漏資訊，對個資當事人有部分影響，如：遭受不明騷擾、詐騙。			
		1:每年產生小於 100 筆	1: 僅含姓名、聯絡方式(電話)	1:若該作業發生個資外洩事故，將導致機關形象、信譽受到輕微損害，如：導致部分媒體報導負面新聞、造成多位民眾電話抱怨等情形。	1: 洩漏資訊，對個資當事人產生些微影響			

個資流程衝擊分析表填寫說明

欄位	填寫說明
主要業務、職掌	依個資盤點表之「主要業務、職掌」欄位填寫。
細部作業名稱	依個資盤點表之「細部作業名稱」欄位填寫。
個資數量	依每年保有個資之筆數，以「衝擊分析項目」個資數量欄位所述級距進行評估。
個資敏感度	保有之個資資料，以「衝擊分析項目」個資敏感度欄位所述級距進行評估。
損害組織信譽	保有之個資資料，以「衝擊分析項目」損害組織信譽欄位所述級距進行評估。
個資當事人隱私衝擊	保有之個資資料，以「衝擊分析項目」個資當事人隱私衝擊欄位所述級距進行評估。
衝擊值	個資數量、個資敏感度、損害組織信譽、個資當事人隱私衝擊之評分加總。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

附件 5 個資流程作業風險評估表

單位名稱	
評估人員	

作業流程名稱		風險控管分類			衝擊值(A)	個資侵害風險發生可能性(B)	風險值	備註	單位名稱
主要業務、職掌	細部作業名稱	風險大分類	風險子分類	個資檔案控管措施(風險情境)	從個人資料衝擊分析將衝擊值帶入	5：控管嚴謹度低、經常被忽略、現行個資檔案控管方式沒有詳細規範。	風險值=個資作業流程衝擊值(A)×風險發生可能性(B)		
						3：控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。			
						1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。			
						0：不適用			

個資流程作業風險評估表填寫說明

欄位	填寫說明
主要業務、職掌	依個資流程衝擊分析表之「主要業務、職掌」欄位填寫。
細部作業名稱	依個資流程衝擊分析表之「細部作業名稱」欄位填寫。
風險大分類	依「細部作業名稱」囊括之個人資料檔案形態填入，詳細內容請參考風險情境表。 若「細部作業名稱」囊括之個人資料檔案含委外作業，則需加入委外作業類。
風險子分類	依前欄之風險大分類展開風險子分類逐一填入，詳細內容請參考風險情境表。
個資檔案控管措施(風險情境)	依前欄之風險子分類展開該類別風險情境，詳細內容請參考風險情境表。
衝擊值	從個人資料衝擊分析表將衝擊值填入。
個資侵害風險發生可能性評估	以「個資侵害風險發生可能性」欄位所述級距進行評估。 於受評估之個資作業流程中，該風險情境不存在者，填「0」(不適用)。
風險值	個資作業流程衝擊值x風險發生可能性。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

附件 6 個人資料事故通報單及處理結果

<table>
<tr><th colspan="4">通報單位填寫</th></tr>
<tr><td>通報單位</td><td></td><td>通報時間</td><td>年　　月　　日
時　　分</td></tr>
<tr><td>個資事故說明</td><td colspan="3">一、個資事故發生與發現之日期與時間：

二、洩漏情形

三、遭受揭露之個資範圍與敘述：(如：個人資料檔案名稱、個人資料類別及個人資料數量等)

四、遭受揭露個資之儲存媒體：(如：紙本、電子檔案、系統資料庫、光碟片、USB碟、可攜式硬碟或記憶卡等)</td></tr>
<tr><td>承辦人</td><td colspan="2">資深同仁</td><td>主管</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><th colspan="4">受理事故承辦人處理結果</th></tr>
<tr><td>承辦人</td><td></td><td>辦理時間</td><td>年　月　日
時　分</td></tr>
<tr><td>事故分析及判定</td><td colspan="3">經分析後判定為：
□ 個資事故/事故權責單位名稱：
□ 疑似個資事件（持續觀察，暫不處理）
□ 非個資事件　（不處理，逕行結案）
說明：</td></tr>
<tr><td>承辦人</td><td colspan="2">資深同仁</td><td>主管</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
</table>