機密等級：內部文件

農業部
桃園區農業改良場

個人資料委外管理作業與稽核指引

第 1.0 版

113 年　8　月　22　日　　頒行

目 錄

壹、 適用範圍

本指引適用於本場委託其他機關辦理個人資料蒐集、處理或利用有關之業務，應依個人資料保護法(以下簡稱個資法)施行細則第 8 條之要求，對受託機關為適當之監督，特訂立本指引，以作為本場監督稽核之依據。

貳、 對受託機關個資保護之基本要求

對受委託機關之各項管理措施要求，均應明文規範於契約、公文或其他合作協議文件中。以下為個資保護管理基本要求事項：

一、 符合個資法與施行細則之要求。

二、 符合個資法施行細則第 12 條第 2 項第 1 款至第 11 款之安全維護事項。

三、 使用去識別化的個資做測試。

四、 僅授權業務必要人員存取個資。

五、 確保個資備份、傳輸、保存方式、銷毀方式與過程及實體防護的安全性。

六、 應於契約或招標文件中增加個資保護條款，詳細條款參閱附錄之個資保護參考條文。

七、 應用系統內含個資之委外開發維護專案，委外契約應一併遵循「契約文件之資通安全規範參考條文」。

參、 受託機關個資保護措施

一、 資訊安全基本防護措施

(一) 個資應用系統應有權限管控。

(二) 個人資料電子檔案應加密或設定密碼予以保護，以確保儲存與傳遞安全。

(三) 個人資料紙本文件於離座逾半小時，應置於個人專用之櫃子或抽屜。非上班時間，應予以上鎖。

(四) 處理個人資料之個人電腦或筆記型電腦設備，應啟動螢幕保護機制。

(五) 傳遞個人資料紙本文件，應確保以安全方式進行。

(六) 個人資料紙張背面不可再生利用，且銷毀個人資料紙本文件，應以碎紙機、水銷或焚燒等其他足以徹底銷毀之方式處理。

(七) 刪除個人資料電子檔案，應以適當方法確實刪除；儲存大量個人資料之儲存媒體，應透過格式化方式刪除或予以消磁。

二、 人員管控

(一) 受託機關人員應充分瞭解資訊安全防護措施相關規定並確實遵守。

(二) 受託機關人員經本場檢核有未遵守前述安全需求規範時，得要求受託機關重新提供符合需求之人員。

(三) 受託機關人員均應簽署保密切結書。

(四) 受託機關人員離職或異動時，應將其帳號及權限停用或刪除。

(五) 受託機關人員違反個資相關法令、本場相關規定時，依契約議處。

三、 個資管理教育訓練

(一) 受託機關人員應接受個資法相關教育訓練。

(二) 受託機關人員應接受資訊安全教育訓練。

肆、 受託機關複委託之約定

一、 複委託應告知本場

受託機關如依據契約得以再分包其工作，若分包之受託單位有異動時，應事先告知本場，始可進行分包作業。

二、 複委託之管理(分包管理)

受託機關對其分包之受託單位，應比照本場對受託機關之管理機制進行管理，並負有與受託機關相同的個資管理與資訊安全義務。

伍、 受託機關之定期報告義務

一、 定期報告個資管理作業情形

受託機關應定期填寫「個人資料委外管理監督檢核表」，並定期向業務管理單位報告個資管理作業執行狀況。

陸、 委託關係終止之應辦事項

一、 返還個資並刪除所保有之個資

委託關係終止並啟動退場機制時，應要求受託機關於指定期限內，將所處理的個資(含書面文件、磁性媒介、電子檔案與資料庫資料)交還本場，並刪除所有屬於該專案所蒐集處理或儲存之個資。

二、 提供刪除作業證明文件

受託機關應提供完成個資刪除作業之證明文件。

柒、 本機關之監督與稽核義務

一、 事前安全評估與契約簽訂

含個資處理或利用之業務委託他人前，應審慎評估安全上可能的潛在風險，並與選定之受託機關，簽訂適當的個資保護與資訊安全契約，課以相關的安全管理責任。

二、 保密義務協議

受託機關因提供服務而接觸本場個資之相關人員，均應依本場規定簽署保密切結書，以規範相關人員之保密責任。

三、 委託執行業務之監督與稽核作業

(一) 依據契約上的要求或雙方議定的結果，視需要進行週期性稽核，稽核項目視契約或雙方議定項目進行。

(二) 承辦人應對下列事項進行必要之監督：

1. 確認受託機關是否依據專案預定之蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間，執行作業。
2. 受託機關是否確實符合下列事項：(此為個資法施行細則第 12 條規定)

(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。

3. 若允許受託機關進行分包時，其約定之保護事項是否符合本場要求。

4. 受託機關是否建立機制於違反個資法規、委外契約條款或雙方議定的結果時，向本場通知及採行必要之補救措施。

5. 受託機關於接獲當事人行使權利之要求時，應立即通知本場。

6. 委託關係終止並啟動退場機制時，受託機關儲存個人資料載體之返還，及刪除受託機關持有個人資料之機制。

(三) 委託他人進行蒐集、處理或利用個人資料時，應定期以『個人資料委外管理監督檢核表』監督受託人執行之狀況，並保留確認結果記錄。

(四) 若經本場認定該受託機關服務品質及安全性無法滿足本場要求時，本場得要求受託機關提出改善措施，如仍無法符合本場需求，則依據契約進行後續處置。

捌、 附錄

一、 契約文件之個資保護規範參考條文

(一) 廠商應提供「個人資料檔案安全維護計畫」，說明委託蒐集、處理或利用個人資料之範圍、類別、特定目的及期間。另說明受託機關如何依據個人資料保護法施行細則第 12 條第 2 項第 1 款至第 11 款要求，善盡個資保護管理之責。

(二) 廠商人員至本場處所工作時，應簽訂外部人員保密切結書並遵守本場「個資保護管理政策」相關規定。

(三) 廠商應依個人資料保護法之要求，訂定個資保護管理相關的政策與程序，及提供足夠培訓，以確保廠商人員執行安控措施，並履行契約中有關蒐集、處理及利用個人資料的責任。

(四) 廠商應防止個人資料洩漏並禁止盜用，並禁止為契約範圍外之影印、複製、加工及利用。

(五) 廠商若要將個人資料相關作業再委託其他公司，必須徵得本場同意授權後，始得為之；複委託之機關亦應遵守本契約所要求之個資保護管理相關規範。

(六) 廠商應於契約終止或解除並啟動退場機制時，返還個人資料之載體並銷毀/刪除所持有之個人資料。

(七) 廠商若發現有違反個人資料保護法事件，必須即時通知本場，說明事件的原委與應變措施，若有任何損失發生，則須負賠償責任。

(八) 廠商應定期向本場進行個人資料保護管理狀況報告，並交付「個人資料委外管理監督檢核表」。本場得視需要，進行實地稽核。

(九) 專案過程傳遞之資料載體(包括但不限於隨身碟/可攜式硬碟/光碟片等儲存媒體)於使用完畢，必須確保資料已於載體中以無法復原方式刪除或銷毀。

(十) 應用系統內個資遭外洩或侵害情事，廠商必須於第一時間通報本場，並說明目前已採取之因應措施與受影響程度。

(十一) 本場得視需要，邀請專家學者共同至廠商處所，就個資保護之實體安全、存取控制、通訊與作業管理及個人資料保護法施行細則第 8 條之要求，與廠商所提交之「個人資料檔案安全維護計畫」及「個人資料委外管理監督檢核表」，對廠商進行稽核作業，廠商不得拒絕。

玖、 附件

一、 個人資料委外管理監督檢核表