財團法人台灣中小企業聯合輔導基金會  
委外專案受託單位個人資料保護檢查表

|  |  |
| --- | --- |
| 專案名稱  (契約編號) | 113年度財團法人台灣中小企業聯合輔導基金會「財團法人台灣中小企業聯合輔導基金會官網維護案」（採購案號：113CB002） |
| 受託  單位名稱 |  |
| 受託蒐集、處理及利用之個人資料 |  |
| 查核人員 |  |
| 查核日期 | 年 月 日 |

| **查核項目** | **可取得證據** | **受託單位自評** | | | **受託單位**  **補充說明** | **委託本會查核** | | | **委託本會**  **查核備註** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **符合** | **不符合** | **不適用** | **符合** | **不符合** | **不適用** |
| **1.配置管理之人員及相當資源** | | | | | | | | | |
| * 1. 配置專責人員   或組織 | * 個人資料管理組織相關文件 * 個人資料管理專人名冊 |  |  |  |  |  |  |  |  |
| 1.2 配置適當資源 | * 相關會議結論或決議事項 * 預算表或資源規劃相關文件 |  |  |  |  |  |  |  |  |
| **2.界定個人資料之範圍** | | | | | | | | | |
| 2.1進行個人資料檔案盤點 | * 契約/協議範圍內的個人資料盤點紀錄 |  |  |  |  |  |  |  |  |
| 2.2建立個人資料檔案清冊 | * 契約/協議範圍內的個人資料盤點清冊 |  |  |  |  |  |  |  |  |
| 2.3個人資料檔案識別確實 | * 個人資料盤點清冊或紀錄(清冊內容須包含蒐集、處理或利用個人資料之範圍、類別、特定目的及期間等欄位) |  |  |  |  |  |  |  |  |
| **3.個人資料之風險評估及管理機制** | | | | | | | | | |
| 3.1進行個人資料檔案風險評估 | * 契約/協議範圍內的個人資料檔案風險評估紀錄、或評估結果 |  |  |  |  |  |  |  |  |
| 3.2針對個人資料檔案風險進行處理 | * 依風險評估結果提出的風險處理計畫或相關規劃 |  |  |  |  |  |  |  |  |
| **4. 事故之預防、通報及應變** | | | | | | | | | |
| 4.1具備事故通報及應變程序 | * 個人資料事故通報及應變程序 |  |  |  |  |  |  |  |  |
| 4.2事故發生後採取應變措施 | * 個人資料事故通報紀錄 * 個人資料事故處理紀錄 |  |  |  |  |  |  |  |  |
| 4.3事故發生後於期限內通知當事人 | * 個人資料事故後通知當事人相關紀錄 |  |  |  |  |  |  |  |  |
| 4.4事故發生後採取預防措施 | * 個人資料事故檢討相關紀錄 |  |  |  |  |  |  |  |  |
| 4.5將事故處理情形及補救措施通知本會 | * 事故處理情形及補救措施通知委託本會之相關公文或紀錄 |  |  |  |  |  |  |  |  |
| **5. 個人資料蒐集、處理利用之內部管理程序** | | | | | | | | | |
| 5.1個人資料蒐集、處理與利用具備特定目的並具有法定要件，或依規定取得當事人同意 | * 契約/協議範圍內個人資料蒐集、處理與利用之特定目的說明 * 對應之法定要件說明 * 當事人同意書 |  |  |  |  |  |  |  |  |
| 5.2特定目的外之利用行為符合法定要件 | * 特定目的外之利用行為符合法定要件之說明 * 當事人同意書 |  |  |  |  |  |  |  |  |
| 5.3履行告知義務（未履行告知義務為符合免告知之情形） | * 履行告知義務之相關紀錄 |  |  |  |  |  |  |  |  |
| 5.4對複委託方依個資法進行監督 | * 與複委託方間之契約包括個人資料保護相關監督條文、其他監督及管理程序 * 對複委託方之個人資料保護監督紀錄 |  |  |  |  |  |  |  |  |
| 5.5提供當事人權利行使管道 | * 提供當事人行使個人資料查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用、以及刪除等權利之方式 |  |  |  |  |  |  |  |  |
| 5.6將當事人權利行使回覆情形做成紀錄供本會備查 | * 回覆當事人權利行使請求之紀錄 |  |  |  |  |  |  |  |  |
| 5.7契約終止或解除時，刪除、銷毀所持有之個人資料 | * 專案契約/協議內有關個人資料刪除與銷燬之規定 * 若為延續專案，前期契約/協議結束時之個人資料刪除及銷毀紀錄 * 若為新案，預定執行之個人資料刪除及銷燬之相關程序 |  |  |  |  |  |  |  |  |
| 5.8契約終止或解除，返還個人資料之載體 | * 契約/協議內有關個人資料載體返還之規定 * 若為延續專案，前期契約/協議結束時之個人資料載體返還紀錄 * 若為新案，預定執行之個人資料載體返還程序 |  |  |  |  |  |  |  |  |
| 5.9已簽署個人資料刪除、銷毀及載體返還切結書 | * 契約內有關簽署個人資料切結書之規定 * 若為延續專案，前期契約結束時之個人資料切結書簽署紀錄 |  |  |  |  |  |  |  |  |
| **6.資料安全管理及人員管理** | | | | | | | | | |
| 6.1針對個人資料進行去識別化 | * 應去識別化之個人資料 |  |  |  |  |  |  |  |  |
| 6.2個人資料存取區分個人帳號及權限 | * 契約/協議範圍內，包括個人資料之應用系統帳號及權限設定 |  |  |  |  |  |  |  |  |
| 6.3個人資料存放於儲存媒體有加密機制 | * 契約/協議範圍內，須加密個人資料檔案之儲存媒體 |  |  |  |  |  |  |  |  |
| 6.4針對個人資料之傳送進行管控 | * 個人資料檔案傳輸管理程序或相關規定 * 個人資料檔案以電子郵件傳送之實作 |  |  |  |  |  |  |  |  |
| 6.5處理個人資料人員均簽署保密協定 | * 契約相關人員簽署之保密協定(相關人員若未成年，例如工讀生，保密協定應有法定代理人簽署) |  |  |  |  |  |  |  |  |
| 6.6針對個人資料儲存場所施行人員進出管控 | * 門禁進出管理方式 * 門禁進出紀錄 |  |  |  |  |  |  |  |  |
| **7.認知宣導及教育訓練** | | | | | | | | | |
| 7.1處理個人資料之人員均接受個人資料保護認知宣導之教育訓練 | * 人員教育訓練或宣導紀錄(例如教育訓練課程表、簽到表等) |  |  |  |  |  |  |  |  |
| 7.2 針對教育訓練課程進行課後評量 | * 課後評量結果紀錄 |  |  |  |  |  |  |  |  |
| **8.設備安全管理** | | | | | | | | | |
| 8.1 針對處理個人資料設備及環境進行控管之保護 | * 包括個人資料的攜帶式儲存媒體(如隨身碟)之管理方式 * 包括個人資料之筆記型電腦於辦公室外使用之安全相關規定 |  |  |  |  |  |  |  |  |
| 8.2 處理個人資料設備應安裝防毒軟體並更新 | * 契約/協議相關人員電腦設備之防毒軟體更新設定及版本 |  |  |  |  |  |  |  |  |
| 8.3 處理個人資料設備應設定螢幕保護程式 | * 契約/協議相關人員電腦設備之螢幕保護程式設定情形 |  |  |  |  |  |  |  |  |
| **9.資料安全稽核機制** | | | | | | | | | |
| 9.1 定期實施個人資料安全自我評核 | * 個人資料安全自我評核紀錄 |  |  |  |  |  |  |  |  |
| 9.2 製作個人資料安全評核報告 | * 個人資料安全評核報告 |  |  |  |  |  |  |  |  |
| **10.使用紀錄、軌跡資料及證據保存** | | | | | | | | | |
| 10.1 保存因應事故發生所採取行為之紀錄 | * 事故通報及應變相關表單與紀錄 |  |  |  |  |  |  |  |  |
| 10.2 保存提供當事人行使權利之紀錄 | * 當事人行使權利相關表單與紀錄 |  |  |  |  |  |  |  |  |
| 10.3 保存個人資料保護教育訓練紀錄 | * 個人資料保護相關教育訓練之簽到表或相關紀錄 |  |  |  |  |  |  |  |  |
| 10.4保存個人資料系統存取紀錄 | * 個人資料相關應用系統存取log、權限新增、變動及刪除紀錄 |  |  |  |  |  |  |  |  |
| 10.5保存個人資料更正與刪除之紀錄 | * 契約/協議期間進行個人資料更正、刪除之紀錄 |  |  |  |  |  |  |  |  |
| **11. 個人資料安全維護之整體持續改善** | | | | | | | | | |
| 11.1配合法規、技術更新改變，定期檢討個人資料保護措施 | * 相關討論會議紀錄(例如使用微軟XP或OpenSSL之安全風險) |  |  |  |  |  |  |  |  |
| 11.2針對個人資料安全自我評核結果進行改善 | * 個人資料安全自我評核結果 * 改善紀錄 |  |  |  |  |  |  |  |  |
| 11.3 依委託本會所提出之建議進行改善 | * 委託本會提出之改善意見(例如公文或電子郵件等) * 改善紀錄 |  |  |  |  |  |  |  |  |