個人資料盤點與風險評估實務

教育機構驗證中心主導稽核員　黃攸德

大綱

- 個人資料與個人資料保護法
- 個人資料檔案盤點
- 個人資料檔案風險評鑑

個人資料與個人資料保護法

什麼是個人資料

個人資料保護法第2條

個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

- 直接
  - 身分證號、護照號碼、居留證號、指紋...
- 間接
  - 電話、地址、車牌、電子郵件帳號 ...

違反個資法，比想像更容易

公視新聞網

24H直播

公館圓環拆除 美國關稅政策 即時 熱門議題 影音 數位專題 深度報導 副刊 節目 國際記者

首頁 / 社福人權

顯示電信業者別 判台哥大違個資法

發布時間：2014/12/31 14:10 更新時間：2014/12/31 14:10

各家電信業者，共同建置了一個用戶資料庫，不過有民眾不滿台灣大哥大，將資料庫應用在自行開發的APP通訊軟體，沒有經過用戶同意，就公開用戶的手機電信公司，這位民眾向法院提出違反個資法的訴訟，法院最後認定台哥大違法，判賠500元。 這個由台灣大哥大開發，類似LINE的APP通訊軟體M+，下載後，手機通訊錄會自動顯示朋友們手機分屬那家電信公司，法務部退休專委、曾參與個資法修法的劉佐國意外發現，台哥大竟然未經用戶同意，就擅自使用手機可攜碼資料庫，將用戶所屬電信公司公開，他向台哥大和NCC投訴後，未獲得正面回應,決定提告。 ==台灣隱私權顧問協會前秘書長 劉佐國== 雖然是微不足道的事情 但是我覺得這欠缺一種 對當事人的尊重 同時既

https://news.pts.org.tw/article/282408

值得注意的，行動電話號碼所屬的「電信業者別」（如中華電信、台灣大哥大、遠傳等），是否屬於個資？司法實務認為，電信業者別是個人電話號碼之附屬資料，得與其他個人資料如姓名、國民身分證統一編號等資料，相互比對、組合、連結及勾稽後，據以作為「間接識別」特定個人之「社會活動」資料之一，亦屬個資法所定「聯絡方式」之個人資料（臺灣臺北地方法院103年度小上字第155號民事判決意旨參照）。即「電信業者別」透由與其他資訊連結，得以「間接識別」方式，推知某特定人使用某電信業者提供之服務，為該個人之「社會活動」，故電信業者別屬於個資。

https://www.ctee.com.tw/news/20230301700720-431305

保護個人資料目的

- 個人資料保護法第1條

  為規範個人資料之**蒐集、處理及利用**，以**避免人格權受侵害**，並促進個人資料之合理利用

  個人資料自主決定權、限制個人資料的使用

- **蒐集**：以任何方式取得個人資料
- **處理**：建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
- **利用**：將蒐集之個人資料為處理以外之使用

特種個資

- 特種個資(個人資料保護法第6條)

病歷、醫療、基因、性生活、健康檢查、犯罪前科

除法律有規定外，不得蒐集、處理、利用

※ 身心障礙手冊屬醫療的一部分，是特種個資

※ GDPR(歐盟一般資料保護規則)　**敏感個資**

宗教、政治理念、工會會員身分、種族或族群背景

要注意具外國身分者

非公務機關蒐集個人資料

個人資料保護法第19條

非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，**應有特定目的**，並符合下列情形之一者：

一、**法律明文規定**。

二、**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**。

三、當事人自行公開或其他已合法公開之個人資料。

四、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。

五、**經當事人同意**。

六、為增進公共利益所必要。

七、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。

八、對當事人權益無侵害。

當事人同意事項

個人資料保護法第8條

公務機關或非公務機關依第十五條或第十九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：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、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。

個人資料類別節錄

C001 辨識個人者

- 姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等

C003 政府資料中之辨識者

- 身分證統一編號、統一證號、稅籍編號、保險憑證號碼、退休證之號碼、證照號碼、護照號碼等

C011 個人描述

- 年齡、性別、出生年月日、出生地、國籍、聲音等

https://law.pdpc.gov.tw/LawContent.aspx?id=FL010631

個人資料之蒐集、處理或利用

個人資料保護法第5條

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，**不得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**

個資法損害賠償

個人資料保護法第28、29條

- 違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。
- 如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以**每人每一事件新臺幣五百元以上二萬元以下**計算
- 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。

個人資料檔案盤點

盤點個人資料檔案目的

- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合
- 知道保護標的
  - 機關內部擁有哪些個人資料檔案
- 了解保護標的
  - 蒐集目的、法令依據、資料來源、資料範圍、處理、利用、保存期限、數量

個人資料檔案形式

- 紙本
- 電子檔
  - 儲存於硬碟、USB、光碟、磁帶等儲存媒體之數位資料檔案
- 資料庫
  - 儲存於資通系統內的數位資料

個人資料檔案盤點表的內容

個人資料檔案名稱
特定目的
檔案形式
個人資料來源(蒐集方式)
個人資料類別
特種個資
資料範圍(個資欄位)
處理
利用
揭露
保存數量
儲存期限
銷毀方式
控制措施(保護措施)

教育機構常用的個人資料類別

C〇〇一 辨識個人者
C〇〇二 辨識財務者
C〇〇三 政府資料中之辨識者
C〇一一 個人描述
C〇一二 身體描述
C〇二一 家庭情形
C〇二三 家庭其他成員之細節
C〇五一 學校紀錄
C〇五二 資格或技術
C〇五七 學生（員）、應考人紀錄
C〇六一 現行之受僱情形
C〇六二 僱用經過
C〇六三 離職經過
C〇六四 工作經驗
C〇六五 工作、差勤紀錄
C〇六六 健康與安全紀錄
C〇六八 薪資與預扣款
C〇七二 受訓紀錄
C〇八一 收入、所得、資產與投資
C一一一 健康紀錄
C一一三 種族或血統來源

https://law.pdpc.gov.tw/LawContent.aspx?id=FL010631

如何盤點個資檔案

- 先列出單位的全部業務(參見各單位的業務職掌)，盤點業務行為與作業流程、個人業務職掌，其中是否含有個資。
- 該盤點什麼？
  - 業務行為流程中的紙本表單/作業紀錄，系統或個人電腦的電子資料 **(系統主機內上傳之附件)， 包含備份檔案**
  - 業務行為流程中個資如何獲得(蒐集)、處理、利用、儲存、銷毀
  - 業務行為流程中以各種形式儲存或尚未銷毀之個資

個人資料檔案盤點表

個人資料檔案盤點表(僅供參考)

紀錄編號：　　日期：　　年　　月　　日

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		
			□紙本 □電子檔 □資料庫 □其他 請說明：				**特種個資** □醫療 □病歷 □基因 □性生活 □健康檢查 □犯罪資料 **一般個資** 請詳列：	□直接 □間接 來源：	□紙本 □傳真 □網站 □系統 □Email □電話 □其他 請說明：	□無 □記錄 □輸入 □儲存 □編輯 □更正 □複製 □檢索 □刪除(銷毀) □輸出 □連結 □內部傳送 對象：	□無 □通知 □聯繫 □統計 □分析 □其他 請說明：	□無 □**外部傳送** 對象及資料範圍 □**國際傳送** 對象及資料範圍	□無 □有 請說明：	□無 □庫房 □置物櫃 □個人電腦 □系統資料庫 □其他 請說明：	□自訂 □法定 **期限** **保有個資總數**	□無 □刪除 □碎紙 □破壞 □水銷 □焚毀 □其他 請說明：	□每周 □每月 □每季 □半年 □一年 □其他 請說明：	□無 □庫房上鎖 □庫房專人管理 □庫房進出紀錄 □公用置物櫃上鎖 □公用置物櫃專人管理 □公用置物櫃鑰匙借還紀錄 □個人置物櫃上鎖 □個人電腦登入需密碼 □個人電腦螢幕保護程式 □個人電腦個資檔案加密 □資訊系統設有權限控管 □其他 請說明：	

盤點人：　　單位主管：

個資檔案群組原則

- 相同作業行為流程之紙本文件、電子檔案、系統資料庫，其資料範圍、蒐集、處理、利用等活動均相同者，可將之群組化，列為同一筆個資檔案資產
- 備份檔案獨立盤點

個人資料檔案清冊欄位說明(1)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **盤點單位**：填寫業務單位名稱。
- **作業流程名稱**：說明該作業流程的目標或用途。
- **個人資料檔案名稱**：由作業流程中所產出或衍生出之個人資料檔案，如申請書表單名稱及電子表單(檔案)名稱等。
- **檔案形式**：
  - **紙本**(以紙本形式存在之文書資料報表等資訊)
  - **電子檔**(係指儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊)
  - **資料庫**(儲存於資通系統上之數位資訊)。

個人資料檔案清冊欄位說明(2)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **特定目的**：作業流程中，向當事人宣告之蒐集、處理或利用其個資之目的，可以有多個特定目的
- **保有依據**：辦理此業務有關的法令法規、內部規章(辦法、要點、公文、會議紀錄)等。
- **個人資料類別**：作業流程所經手之當事人個人資料類別。
- **個人資料範圍**：如有特種個資要勾選，一般個資請填寫個人資料檔案表單上的欄位名稱，例如：姓名、身分證字號、系所、職稱、電話、地址、銀行帳號等。

教育機構常用的特定目的

- 人身保險(001)
- 人事管理(002)
- 全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險(031)
- 存款與匯款(036)
- 兵役、替代役行政(042)
- 志工管理(043)
- 非公務機關依法定義務所進行個人資料之蒐集處理及利用(063)
- 保健醫療服務(064)
- 契約、類似契約或其他法律關係事務(069)
- 計畫、管制考核與其他研考管理(078)
- 教育或訓練行政(109)
- 產學合作(110)
- 場所進出安全管理(116)
- 會計與相關服務(129)
- 資(通)訊與資料庫管理(136)
- 資通安全與管理(137)
- 圖書館管理(146)
- 衛生行政(156)
- 調查、統計與研究分析(157)
- 學生(員)(含畢、結業生)資料管理(158)
- 學術研究(159)
- 體育行政(169)
- 其他經營合於營業登記項目或組織章程等，為辦理教學、研究、行政及服務等相關事宜所需（181）

個人資料檔案清冊欄位說明(3)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **蒐集：**
  - 方式(直接、間接，間接蒐集請填寫資料來源單位)
  - 方法(依表格選項勾選或自行填寫)
- 若作業流程中有**使用外部雲端服務蒐集個資**
  - 蒐集方法可勾選網站，或勾選其他並填寫雲端服務，皆備註使用哪家服務商。
  - 個資檔案形式勾選其他，並填寫電子檔(雲端服務)，及備註Google表單、OneDrive等。
  - 儲存方式請勾選其他並填寫雲端服務，若會下載至個人電腦彙整並**刪除**雲端服務上的資料請**多勾選個人電腦**。

個人資料檔案清冊欄位說明(4)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **處理**：分為記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送，勾選內部傳送請務必註記傳送對象。
- **利用**：處理以外之使用，包含聯絡當事人、統計分析等。
- **揭露**：外部傳輸或國際傳輸等，請務必註記傳送對象及個人資料範圍。
- **委外**：若有委託給第三方請勾選有並述明委託什麼業務給哪個單位。如：學雜費收取，將學生個資傳送至OO銀行系統

個人資料檔案清冊欄位說明(5)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **方式**：勾選個人資料檔案的保存方式，**要對應到檔案形式**
  - 檔案在光碟、行動硬碟、USB 勾選其他，並加說明，再勾選放置何處
  - 使用外部雲端服務蒐集個資請勾選其他，並填寫雲端服務，若會下載至個人電腦彙整請**多勾選個人電腦**
- **保存期限/數量(筆)**：

保存期限 => 要明確
  - 法定，請註明相關法規

數量(筆) ==> 歷史資料(已知) + 今年新增(變動中)
  - 尚未銷毀的都算(使用中、庫房的歷史資料)

同時有不同的檔案形式，分別寫明每種檔案形式的保存年限及數量

個人資料檔案清冊欄位說明(6)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **銷毀**：超過保存期限的個人資料檔案如何銷毀與銷毀頻率
  - 同時有不同的檔案形式，應說明各檔案形式的銷毀方式及銷毀頻率

    要留下紀錄， **保存3年備查**

    =>個資檔案名稱、銷毀資料內容及數量、主管核可、執行證據(照片)
- **現有控制措施： 這裡只是舉例，請依實際情況修訂勾選**

庫房環境安全(地震、淹水、消防、防潮、入侵、CCTV)

個人資料檔案清冊欄位說明(7)

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		

- **個資檔案價值即資料的敏感程度**

1. 不含自然人之姓名及國民身分證統一編號(或護照號碼)
2. 1. 含自然人之姓名或國民身分證統一編號(或護照號碼)
   2. 含自然人之姓名及員工編號或學號
3. 1. 含自然人之姓名及國民身分證統一編號(或護照號碼)
   2. 含自然人之姓名或國民身分證統一編號(或護照號碼)及財務情況（如：薪資、金融帳號）
4. 自然人之姓名或國民身分證統一編號(或護照號碼)及特種個人資料。

個人資料盤點表填寫範例

個人資料檔案盤點表(僅供參考)

紀錄編號：AC20260015　　日期： 115 年 5 月 12 日

盤點單位	作業流程名稱	個人資料檔案名稱	檔案形式	特定目的	保有依據	個人資料類別	個人資料範圍	蒐集		處理	利用	揭露	委外	儲存		銷毀		現有控制措施	檔案價值
								方式	方法					方式	期限	方式	頻率		
主計室	政府補助計畫憑證審核業務	工讀費支出憑證黏貼表	■紙本 □電子檔 ■資料庫 □其他 請說明：	129	商業會計法	C00一 C00二 C三一	**特種個資** □醫療 □病歷 □基因 □性生活 □健康檢查 □犯罪資料 **一般個資** 請詳列： 學號、姓名、出生年月日、聯絡方式、地址、金融帳戶、薪資	■直接 □間接 來源： 本人	■紙本 □傳真 □網站 □系統 □Email □電話 □其他 請說明：	□無 ■記錄 ■輸入 ■儲存 □編輯 □更正 □複製 □檢索 ■刪除(銷毀) ■輸出 □連結 □內部傳送 對象：	□無 ■通知 ■聯繫 □統計 □分析 □其他 請說明：	■無 □**外部傳送** 對象及資料範圍 □**國際傳送** 對象及資料範圍	□無 ■有 請說明： 紙本委託OO廠商水銷	□無 ■庫房 ■置物櫃 □個人電腦 ■系統資料庫 □其他 請說明：	□自訂 ■法定 **期限** 10年 **保有個資總數** 紙本8000筆 資料庫8000筆	□無 ■刪除 □碎紙 □破壞 ■水銷 □焚毀 □其他 請說明：	□每周 □每月 □每季 □半年 ■一年 □其他 請說明：	□無 ■庫房上鎖 ■庫房專人管理 □庫房進出紀錄 □公用置物櫃上鎖 □公用置物櫃專人管理 □公用置物櫃鑰匙借還紀錄 ■個人置物櫃上鎖 □個人電腦登入需密碼 □個人電腦螢幕保護程式 □個人電腦個資檔案加密 ■資訊系統設有權限控管 □其他 請說明：	3

盤點人：　　單位主管：

個人資料檔案盤點頻率

- **定期：**
  - 每年至少盤點一次，並將結果紀錄於「個人資料檔案清冊」
- **不定期：**
  - 當單位或業務流程有新增及變動時，應重新進行盤點

  例如：

  1. 業務變動導致特定目的新增、變更、消失或期限屆滿時
  2. 業務變動導致蒐集、處理或利用之資料或作為有變動時
  3. 稽核發現與實際盤點結果不一致時

個資檔案風險評鑑

風險評鑑目的

- 識別及分析內外部對個資檔案的潛在危害
  - 找出弱點及危害，評估風險
  - 在有限的資源下，集中資源優先改善不可接受的損害

風險評估方法

- 個資檔案的風險評估

  個資檔案發生安全事件時(個資被竊取、洩漏、竄改或毀損)，考量個資檔案價值、對當事人與組織造成的「影響/衝擊程度」及事件發生之「可能性」

  風險值=檔案價值*MAX(影響/衝擊程度)*MAX(可能性)

  ※風險評估法提供參考，請依據單位組織的特性進行調整

個資檔案風險評估--影響/衝擊構面

- 對當事人的影響/衝擊
  - 對當事人損害程度
- 對組織財務的影響/衝擊
  - 個資檔案的個資數量

對當事人的影響/衝擊

1. 個資檔案機敏等級低，資料外洩對不致影響個人權益或僅導致個人權益輕微受損。(如：個資檔案價值「1」者)
2. 資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益部份受損。（如：含身分證號，個資檔案價值「2」者）
3. 資料外洩資料外洩可能導致個人隱私遭冒犯，當事 人 個人權益嚴重受損。（如：含身分證號、財務資訊，個資檔案價值「3」）
4. 資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，當事人個人權益非常嚴重受損。（如：含特種個資、特種身分、輔導紀錄等，個資檔案價值「4」以上者）

對組織財務的影響/衝擊

1. 個資檔案之個資數量 <= 499 筆
2. 個資檔案之個資數量 500~4,999 筆
3. 個資檔案之個資數量 5,000~49,999 筆
4. 個資檔案之個資數量 >= 50,000 筆

個資檔案風險評估--發生可能性

等級	教育訓練	管控措施及法遵	內部監控暨個資安全
1	業務相關人員近一年接受3小時以上個資教育訓練課程	訂有完整管控程序且各項措施落實執行 完全遵守個資法及其相關規定	近三年內未發生過個資安全通報紀錄 已建立內部稽核或監督管理機制，每年執行稽核，並確實持續改善
2	業務相關人員近一年接受3小時以內個資教育訓練課程	小部分管控程序不完善或小部分管控措施未落實執行 有小部分未確實遵守個資法相關規定，可能受行政懲罰	近三年內曾發生個資安全二次以內(含二次)通報紀錄 已建立內部稽核或監督管理機制，但未每年執行稽核或監督管理機制
3	業務相關人員近一年未接受個資相關教育訓練	缺乏管控程序或大部分控制措施未落實執行 未確實遵守個資法相關規定，可能有刑事責任	近三年內曾發生個資安全三次以上(含三次)通報紀錄 未建立內部稽核或監督管理機制

個資檔案風險評估表(僅供參考)

個人資料檔案風險評估表(僅供參考)

紀錄編號：AC20260001　　填表日期： 115 年 5 月 20 日

項次	保有單位	流程名稱	資產名稱	檔案形式	資產價值(V)	衝擊		可能性			衝擊(I)	可能性(P)	風險值 R=V*I*P
						構面1	構面2	構面3	構面4	構面5			
						對當事人損害程度	對學校財務影響程度	教育訓練	內部監督稽核	個資安全通報紀錄			
1	主計室	政府補助計畫憑證審核業務	工讀費支出憑證黏貼表	紙本	3	3	3	1	2	1	3	2	18
2	主計室	政府補助計畫憑證審核業務	工讀費支出憑證黏貼表	資料庫	3	3	3	1	2	1	3	2	18

填表人：　　單位主管：

風險值的分布

風險值=個資檔案價值*MAX(衝擊)*MAX(可能性)

- 檔案價值 1 ~ 4
- 衝擊值 1 ~ 4
- 可能性 1 ~ 3

風險值 1、2、3、4、6、8、9、12、16、18、24、27、32、36、48

風險的控管與處理

- 考量政策目標及現有資源決定可接受風險值，經**負責人/管理人/委員會議核定**
  - 20/80 原則
  - 影響/衝擊為高的高價值個資檔案，發生風險的可能性應該低

    風險值=檔案價值*MAX(影響/衝擊程度)*MAX(可能性)

    可接受風險值=4*4*1=16
- 大於可接受風險值之個資檔案
  - 擬定風險改善計畫
  - 改善完成後，評估改善成效

風險處理方法

避免

改變計畫以徹底消滅風險源

轉移

將風險的責任與財務損失轉嫁給第三方

降低

採取預防措施減低風險發生的「可能性」或造成的「影響程度」

接受

處理風險的成本遠高於損失本身時，選擇保留並承擔該風險

個資檔案風險改善計畫表(僅供參考)

個資檔案風險改善計畫表(僅供參考)

紀錄編號；20260001　　填表日期： 115 年 5 月 28 日

編號	作業流程名稱	個人資料檔案名稱	現況說明	改善方式	改善措施	處理人員	預計完成時間	風險擁有者	實際完成時間	確認完成
1	政府輔助計畫憑證審核業務	支出憑證黏貼表(紙本)	與其他單位共用庫房，庫房資料未上鎖，可能為他人偷窺、洩漏、毀損	□避免 □轉移 ■降低 □接受	購買可上鎖鐵櫃置於庫房，放置本單位資料，鑰匙專人保管	陳東爾	本年 7 月 30 日			
2	政府輔助計畫憑證審核業務	支出憑證黏貼表(資料庫)	作業系統未定期更新，可能被駭客攻擊，以致資料洩漏、竄改、毀損	■避免 □轉移 □降低 □接受	固定每季查檢更新，並填表紀錄	林木森	本年 6 月 30 日			
				□降低 □接受						

備註：
1. 改善計畫須經風險擁有者審核，實際改善完畢後，填寫實際完成時間再交由風險擁有者確認完成。
2. 確認改善措施完成後，至風險評鑑彙整表進行風險再評鑑作業，確認風險等級確實下降至可接受風險。

個資檔案風險評鑑彙整表(僅供參考)

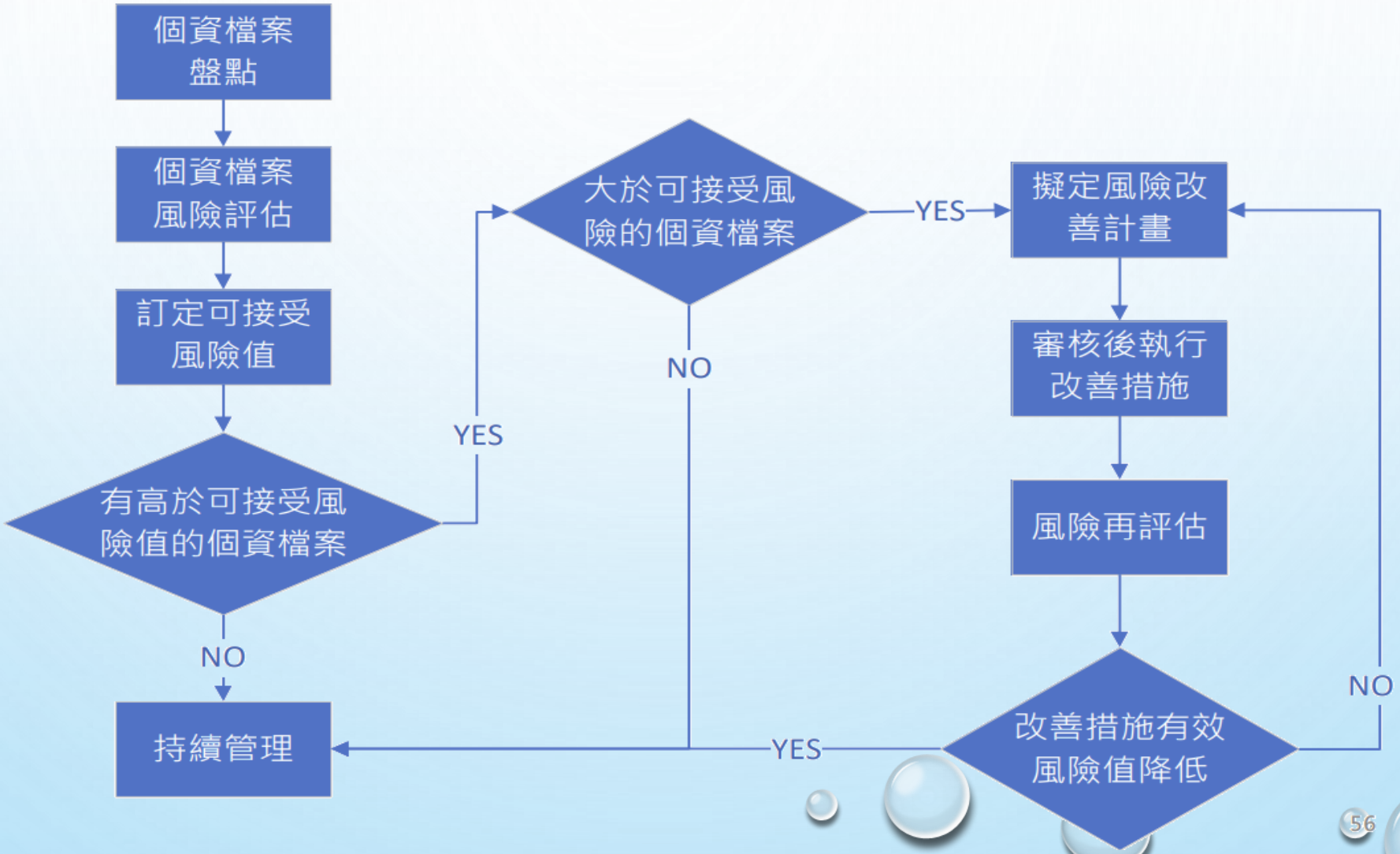
個人資料檔案風險評鑑彙整表(僅供參考)

紀錄編號：AC20260001　　填表日期：115 年 5 月 26 日

項次	保有單位	業務流程名稱	個資檔案名稱	檔案形式	資產價值(V)		衝擊		可能性			衝擊(I)	可能性(P)	風險值 R=V*I*P
							構面1	構面2	構面3	構面4	構面5			
						評鑑別	對當事人損害程度	對學校財務影響程度	教育訓練	內部監督稽核	個資安全通報紀錄			
1	主計室	政府補助計畫憑證審核業務	工讀費支出憑證黏貼表	紙本	3	初評	3	3	1	2	1	3	2	18
						複評								
2	主計室	政府補助計畫憑證審核業務	工讀費支出憑證黏貼表	電子檔	3	初評	3	3	1	2	1	3	2	18
						複評								
						初評								
						複評								
						初評								
						複評								
						初評								
						複評								
						初評								
						複評								
						初評								
						複評								

填表人：　　單位主管：

個資檔案風險評鑑流程


個資檔案盤點
個資檔案風險評估
訂定可接受風險值
有高於可接受風險值的個資檔案
YES
NO
持續管理
大於可接受風險的個資檔案
YES
NO
擬定風險改善計畫
審核後執行改善措施
風險再評估
改善措施有效風險值降低
NO
YES

Q & A

感謝您的聆聽