個人資料風險評鑑與處理訓練課程

聯準科技服務有限公司
資深顧問 吳文進
Email: alexwu0513@gmail.com
Mobile: 0911-371837
October 21, 2016

1.

課程大綱

一、個人資料風險評估分析
二、個人資料風險等級判定
三、個人資料風險處理作業
四、風險再評估與殘餘風險處理
五、風險評鑑報告

2.

個資盤點與風險評鑑作業流程

作業流程	權責單位	相關文件
個人資料盤點(鑑別)	各單位/輔導廠商	個人資料項目盤點表
個資風險評估分析	各單位/輔導廠商	個人資料檔案風險評估彙整表
個資風險等級判定	各單位/輔導廠商	個人資料檔案風險處理計畫
撰寫風險評估報告	各單位/輔導廠商	個人資料風險評估報告
執行稽核檢查	個人資料保護稽核小組	
紀錄保存	各單位	

一、個人資料風險評估分析

風險評估執行時機

- 個人資料檔案風險評估作業應於每年內部稽核活動前執行
- 除定期每年執行一次外，亦應於
  - 營運組織變更
  - 作業流程改變
  - 新增或變更個人資料檔案
  - 發生重大個人資料外洩事件
- 針對變動範圍內的作業程序與個人資料檔案進行風險評估。

5.

風險評估分析(1/)

- 風險評估方法的主要考量因素
  - 風險發生之機率
  - 風險之影響/衝擊程度
- 個人資料檔案之風險評估應依據實際狀況，對照「影響及衝擊等級表」及「風險發生可能性等級表」之內容，並於「個人資料檔案風險評估彙整表」中進行六個評估構面之風險分析。

6.

影響及衝擊等級表

評估項目(構面)	影響及衝擊等級表(I)		
	輕微(1)	嚴重(2)	**非常嚴重(3)**
可識別性	個人資詢查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	僅可以間接識別特定當事人者(需要與其他資料進行對照、組合、連結等，始能識別該特定的個人)	**可以直接識別特定當事人者(不需要與其他資料進行對照、組合、連結等，就能識別該特定的個人)**
個資數量	20筆以下 (團體訴訟不成立)	一般個資21~20,000筆 特種個資20筆以內	**一般個資20,001筆以上 特種個資21筆以上**
敏感程度	僅有識別資料(未含其他個人活動、財務金融或特種個人資料)	含有個人活動資料或財務金融資料	**含有特種個人資料 (病歷、醫療、基因、性生活、健康檢查、犯罪前科)**
特定目的範圍內利用	僅於特定目的範圍內利用個人資料	有特定目的外利用個人資料，但符合例外條款	**有特定目的外利用個人資料，但不符合例外條款**
外部利用	無外部利用情形	無償委任關係外部利用	**有償委任關係外部利用**
國際傳輸	無國際傳輸情形	主管機關未規定之國際傳輸	**主管機關訂定規定之國際傳輸**

註記：評估項目參考NIST SP800-122選定，等級判定依據「個人資料保護法」之相關要求訂定，依據以上項目分項判定，最後依據最高衝擊原則，判定衝擊程度等級。

7.

風險發生可能性等級表

等級	可能性	發生機率	描述
3(高)	幾乎確定	65-100%	在大部分的情況下會發生
2(中)	有可能	11-65%	有些情況下會發生
1(低)	幾乎不可能	0-10%	只會在特殊的情況下發生

8.

風險評估分析(1/)

- 各單位須針對各項個人資料之使用及控管狀況，依據「影響及衝擊等級表」之各個構面，識別其組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將影響及衝擊程度記錄於「個人資料檔案風險評估彙整表」

9.

個人資料檔案風險評估彙整表

個人資料檔案風險評估彙整表(參考範例)

單位名稱：　　填表日期：　年　月　日

編號	個人資料檔案名稱	評鑑別	評估構面1	評估構面2	評估構面3	評估構面4	評估構面5	評估構面6	衝擊程度(I)	可能性(P)	風險		現有控制措施
			可識別性	個資數量	個資敏感程度	特定目的範圍內利用	外部利用	國際傳輸			風險值(R)=P×I	風險等級	
1	約聘人員契約書	第一次評鑑	3	2	1	1	1	1	3	1	3	2	實體安全控管(鐵櫃) 使用加密隨身碟
		風險再評鑑											
2	教師具證照名冊	第一次評鑑	2	3	3	2	2	1	3	2	6	3	存取權限控管/實體(機房)與環境安全控管
		風險再評鑑											
3	校友借書申請表	第一次評鑑	3	3	3	1	1	1	3	1	3	2	實體安全控管(檔案室) 設置存取控制權限
		風險再評鑑											
4	研討會廢室名單	第一次評鑑	1	2	1	1	1	1	2	2	4	2	實體安全控管(鐵櫃)
		風險再評鑑											
5	實習課程實施辦法與執行情形資料	第一次評鑑	3	2	1	1	1	1	3	1	3	2	存取權限控管/實體安全控管(鐵櫃上鎖)
		風險再評鑑											

風險值計算

- 識別風險發生之可能性(P)及影響/衝擊程度(I)，將此2項評分進行相乘，即求出該個人資料檔案之風險值。風險值(R) = P × I。

11.

風險分布矩陣

- 將經由風險值計算公式所得之風險值，對應至「風險分布矩陣」以判斷風險值之分布情況。

風險分布矩陣			
	發生機率		
影響/衝擊程度	幾乎不可能(1)	有可能(2)	幾乎確定(3)
非常嚴重(3)	3(中度)	6(高度)	9(極高度)
嚴重(2)	2(低度)	4(中度)	6(高度)
輕微(1)	1(低度)	2(低度)	3(中度)

12.

二、個人資料風險等級判定

13.

決定可接受風險值

- 依下表列出可接受及不可接受之風險等級，作為本校各單位後續風險處理之依據。

風險值(R)	風險等級	風險判別與處理	
1 或 2	1	可接受風險	接受
3 或 4	2	可接受風險	持續監視
6 或 9	3	不可接受風險	立即控制

14.

決定可接受風險值（1/2）

- 各單位個人資料風險評估可接受之風險等級，每年需檢討並經本校「個人資料保護管理執行小組」開會決議並記載於會議紀錄中。

15.

三、個人資料風險處理作業

16.

個人資料風險處理作業（1/2）

- 依個人資料風險評估結果及可接受風險值之決議，由各風險項目負責人針對需降低風險值之個人資料擬訂「個人資料檔案風險處理計畫」，以期將風險降至可接受等級。

填製個人資料風險處理計畫

個人資料風險處理計畫(參考範例)

單位名稱：　　填表日期：　年　月　日

資產識別暨風險說明					風險處理措施		風險進度追蹤				
編號	個人資料檔案名稱	風險說明	風險值(R)=P×I	風險等級	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	處理結果
1	教師具證照名冊	1.紙本個資未儲存於上鎖的櫥櫃,易發生非授權存取及誤用 2.透過網際網路傳送個資未加密或設密碼保護,個資易外洩 3.存放個資隨身碟沒有加密或密碼保護功能,個資易洩漏	6	3	■接受風險 ■降低風險 □轉移風險 ■避免風險	1.目前未有經費修繕或採購新櫥櫃以存放個資 2.制定程序文件,明文規定禁止同仁透過網際網路傳送個資 3.採購有加密功能的隨身碟存放個資	張○○	104/12/15	104/12/01	林○○	已完成
					□接受風險 □降低風險 □轉移風險 □避免風險						

個人資料風險處理作業(2/2)

- 個人資料風險處理計畫之風險處理措施，應根據「個人資料保護法」對各項個人資料保護之安全要求目標，擬訂適當之處理措施及相關執行資源。
- 個人資料風險處理計畫應提報「個人資料保護管理執行小組」審查後執行，並列入追蹤管理。

四、風險再評估與殘餘風險處理

風險再評估

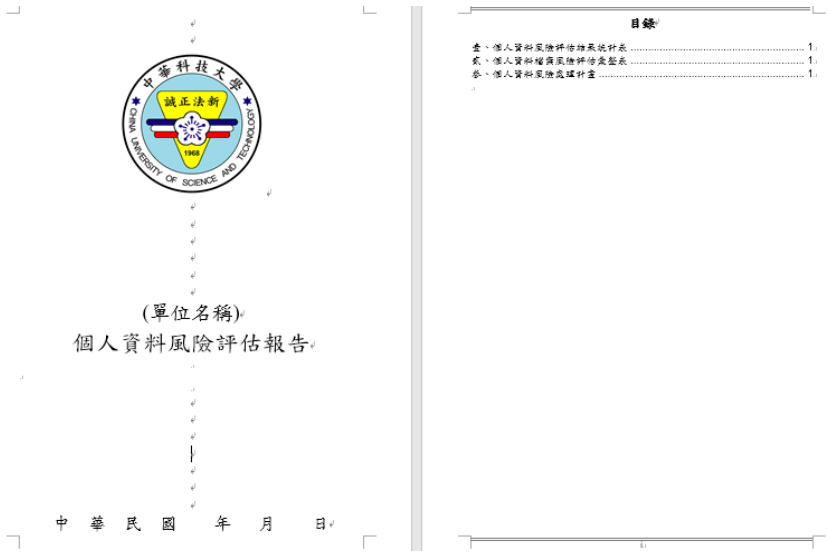
- 風險處理計畫於預訂完成日期結束後，須由各單位執行風險再評估，以確認風險處理計畫之執行是否達到預期目標。
- 進一步決定殘餘風險處理作法。

五、風險評鑑報告

撰寫個人資料風險評估報告

- 各單位依據個人資料檔案風險評估結果，撰寫「個人資料風險評估報告」，並陳單位主管確認。

個人資料風險評估報告



(單位名稱)
個人資料風險評估報告

中 華 民 國 年 月 日

目錄

壹、個人資料風險評估結果統計表 1
貳、個人資料檔案風險評估彙整表 1
參、個人資料風險處理計畫 1

Q&A

～如有任何問題，歡迎隨時來電詢問～