財團法人多層次傳銷保護基金會（Multi-Level Marketing Protection Foundation）

財團法人多層次傳銷保護基金會
Multi-Level Marketing Protection Foundation

114年度「多層次傳銷事業個人資料檔案盤點暨風險評鑑教育訓練」及方法論試做

2025.07.29

大綱

- 個資檔案盤點表填寫試做說明
- 個資檔案風險評鑑表填寫試做說明
- 問題與討論

前言-個資盤點與風險評鑑之法源

個人資料保護法規定

- 依據個人資料保護法第27條及其施行細則第12條之規定，**非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。**
- 其中，包含：「**界定個人資料之範圍**」與「**個人資料之風險評估及管理機制**」。

實務上作法

- 實務上多以「**個資檔案盤點表與風險評鑑表**」作為落實上述措施之工具與證明。

前言-個資盤點與風險評鑑之法源

公平交易委員會法規命令規定

- 多層次傳銷業訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法作業辦法第3條第1項第3款：
- 「多層次傳銷事業就個人資料保護之規劃，應考量下列事項：

依已界定之個人資料範圍及個人資料**蒐集、處理、利用之流程**，**分析**可能產生之**風險**，並根據風險分析之結果，**訂定適當之管控措施**。」。

實務上作法

- 實務上多以「**個資檔案盤點表與風險評鑑表**」作為落實上述措施之工具與證明。

前言-個資盤點與風險評鑑常見作業流程

個資檔案盤點

確認單位經手 / 擁有之個資檔案及其管理情形

資產論？
作業流程風險節點論？

個資檔案風險評鑑

依組織所定之風險評鑑方法論，就個資檔案逐筆分析確認其風險等級

個資檔案風險處理

確認組織可接受風險值，並就超過者進行處理，例如：可接受風險值為中度風險，則就中度風險(不含)以上等級之個資檔案，需額外確認現行管控措施之適足性，就不足處擬定對策，強化相應管理措施或補償措施。

大綱

- 個資檔案盤點表填寫試做說明
- 個資檔案風險評鑑表填寫試做說明
- 問題與討論

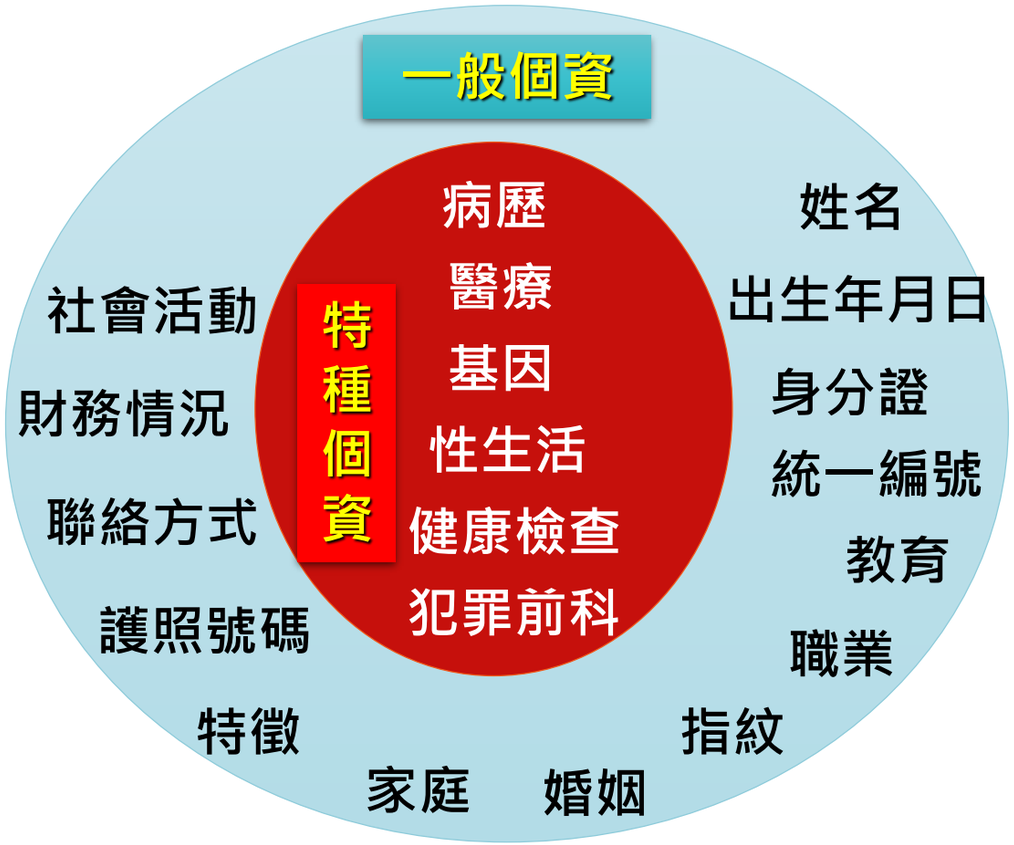
個資盤點目的與效益

針對組織各單位所擁有之個人資料檔案（含實體檔案、電子檔案及系統資料），進行盤點作業，以達成下列目的與效益：

釐清 / 清查	管控 / 稽核	追蹤軌跡與紀錄
對內部面向： 清查組織所擁有之個人資料檔案	對內部面向： 組織方面，作為內稽內控之一環	對內部面向： 面對重大個資議題，便於掌握方向及擬訂處理
對外部面向： 釐清組織個人資料檔案之分佈情形	對外部面向： 主管機關查核之重要依據	對外部面向： 證明組織對於個人資料管理之運作及控管

個人資料之定義

原則 **現生存之自然人**
(個資法§2)



得以直接或間接方式識別該個人之資料

例外 **不適用個資法規定**
(個資法§51)

- ×自然人為單純個人或家庭活動之目的，如：家庭旅遊
- ×於公開場所或公開活動所蒐集、處理或利用之未與其他個人資料結合之影音資料，如：行車記錄器所錄存畫面
- ×法人資料(公司行號)
- ×往生者資料**(個資法施行§2)**
- ×去識別化之個人資料

個人資料盤點項目

單位因執行業務或輔助組織經營所必要而蒐集、處理或利用之個人資料，含**經手、使用或產出**

委託法人、團體或自然人蒐集、處理或利用個人資料者，亦應進行盤點。

個人資料盤點表填寫說明

填表日期： → 可做為版控

編號	權責單位/人員	作業流程	個資檔案名稱	檔案類型	蒐集目的	處理或利用目的

◆ **權責單位/人員**

- 個資檔案之蒐集/處理/利用/保管單位與人員。

◆ **作業流程**

- 可參考作業流、作業手冊、業務慣用名稱，或填寫通俗可具體認知名稱。

◆ **個資檔案名稱**

- 定義：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。
- 請填入個資檔案/表單/系統之名稱。

★ 單位僅經手個資檔案者，亦須盤點。

個人資料盤點表填寫說明(續)

編號	權責單位/人員	作業流程	個資檔案名稱	檔案類型	蒐集目的	處理或利用目的	特定情形

◆ **檔案類型**

實體檔案	電子檔案	系統資料
紙本、光碟或其他有形體之檔案等	文字檔(TXT, Word, Excel, PDF等)、影像檔(JPG, GIF等)、錄音檔(WAV, RA, MP3)或其他種類之電子檔案等	使用系統輸入或查詢所產出資料

◆ **蒐集目的**

- 基於什麼目的，取得個人暨客戶之個資 。可參考「附錄一_特定目的之項目」填寫。

◆ **處理或利用目的**

- 蒐集而來之個資，於實際使用時是基於什麼目的 。可參考「附錄一_特定目的之項目」填寫。

◆ **特定情形**

- 保有個資之正當法定依據。

個人資料盤點表填寫說明(續)

個人資料類別			
機密性價值 高(4)	機密性價值 中(3)	機密性價值 低(2)	機密性價值 無(1)

- **機密性價值 高(4)**
  - 個資法第6條定義之特種個資屬之，如：病歷、醫療、健康檢查、犯罪前科。
- **機密性價值 中(3)**
  - 信用卡卡號/授權碼、金融帳戶號碼、身分證字號/護照號碼/居留證號碼、生日、性別、國籍、生物辨識/相片。
- **機密性價值 低(2)**
  - 姓名、聯絡資訊 、習慣/興趣 、資格/執照/證照、家庭情形/婚姻、帳號/密碼、薪資/所得/報酬。
- **機密性價值 無(1)**
  - 公司/職業/受雇情形 、cookies/網路識別碼、操作軌跡、員工編號，無法從中直接識別特定人。

個人資料盤點表填寫說明(續)

個人資料類別			
機密性價值 高(4)	機密性價值 中(3)	機密性價值 低(2)	機密性價值 無(1)

★ 補充

◆ **機密性價值 高(4)**

- 醫療：病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。
- 病歷：一、醫師依醫師法執行業務所製作之病歷。二、各項檢查、檢驗報告資料。三、其他各類醫事人員執行業務所製作之紀錄。
- 健康檢查：健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。
- 犯罪紀錄：指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

個人資料盤點表填寫說明(續)

保存資訊		
儲存位置	資料保存期限	保存依據

◆ **儲存位置**

- 端視檔案類型，填寫實際儲存位置，如：資料庫（應填寫名稱）、資訊系統（應填寫名稱）、伺服器、行動硬碟、外部雲端硬碟NAS、其他儲存媒體、公務用個人電腦、部門公用槽、個人檔案櫃、檔案室、倉庫、庫房等。（可複數）

◆ **資料保存期限**

- 期限訂定之依據依序為：**法令明文規定→組織內規（含組織整體或單位內規）→實際作業所需**。
- 依實際作業所需訂定，應注意合理性、必要性與關聯性。
- 除非法律明文規定，原則不得有「永久保存」之概念。

◆ **保存依據**

- **法令明文規定→組織內規（含組織整體或單位內規）→實際作業需求**。
- 「實際作業需求」，應詳細說明基於何項業務執行之何種情事、困難或規劃而訂出該保存期限。

個人資料盤點表填寫說明(續)

對應一致性

檔案類型	儲存位置
實體檔案	➢ 檔案室、部室檔案櫃、個人座位檔案櫃 ➢ 經手不留存；但如有暫存期間，也可填寫暫存處
電子檔案	個人電腦、部門共用槽（請填寫位置或名稱）
系統資料	資訊系統（請填寫系統名稱）

個人資料盤點表填寫說明(續)

流向分析			
來源	蒐集方式	資料傳輸對象	
		內部單位	外部單位

◆ **來源**

- 指個人資料從何處取得（即直接前手為何）？
- 如填寫單位名稱、資訊系統名稱等。（可複數）

◆ **蒐集方式**

- 直接蒐集：個人資料是以組織名義直接從當事人處取得。
- 間接蒐集：個人資料是透過其他自然人、機關或法人取得。
- 內部傳輸：個人資料是透過組織內部其他單位或資料庫所取得。

◆ **傳輸對象**

- 指針對單位保有資料，按作業流程，後續會再傳輸或交至何處（即後手為何）？
- 區分內部單位與外部單位，請全數列出。
- 如填寫單位名稱、資訊系統名稱等。（可複數）

個人資料盤點表填寫說明(續)

流向分析				
是否涉及委外廠商	是否涉及國際傳輸	組織扮演角色		
		資料控制者	資料處理者	資料協同控制者

◆ **委外廠商**

➢ 該項作業或檔案，是否涉及委外廠商（業務委託外部組織，其中涉及個資蒐集 / 處理 / 利用）。

◆ **國際傳輸**

➢ 該項作業或檔案，是否有傳輸至臺灣以外的國家或地區，並請填寫國家或地區名稱（如有）。

◆ **資料控制者**

➢ 公司為可以決定該個人資料處理或利用之方式及目的者。

◆ **資料處理者**

➢ 公司為其他法人或自然人，蒐集、處理或利用個人資料者。

◆ **資料協同控制者**

➢ 公司聯合其他法人、自然人進行蒐集，並可以決定該個人資料處理或利用之方式及目的者。

大綱

個資檔案盤點表填寫試做說明

個資檔案風險評鑑表填寫試做說明

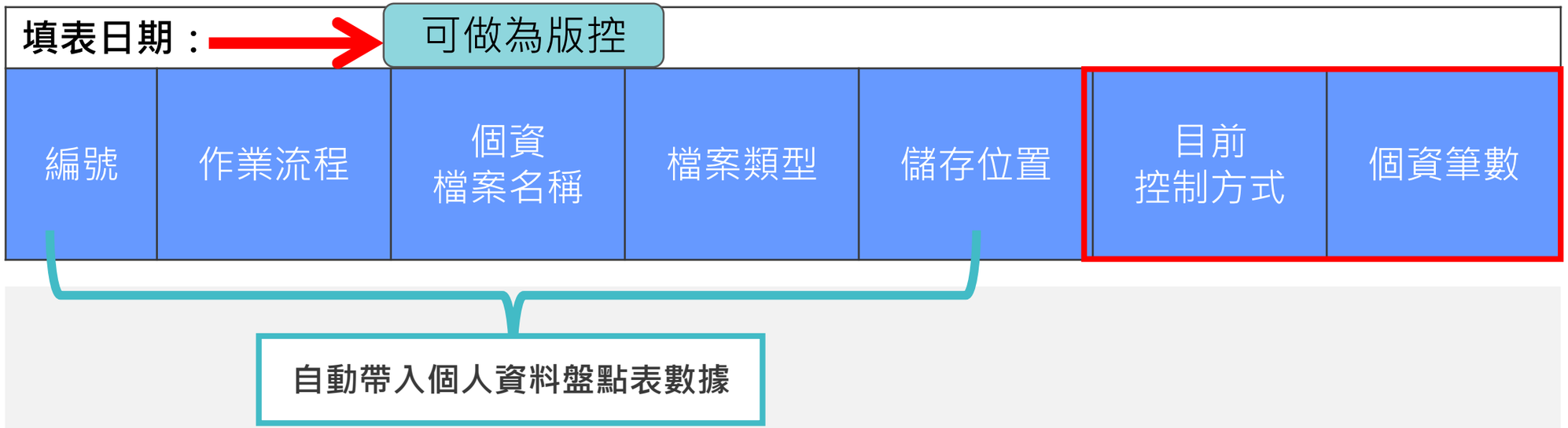
問題與討論

個資風險評鑑目的與效益

針對組織各單位之盤點作業結果，就每項個資檔案進行風險評鑑作業，以達成下列目的與效益：

分析風險分布	確認風險落點	矯正預防/追蹤改善
就個人資料進行風險等級區分及分析	瞭解超出可接受風險之個人資料檔案及其位置、保管狀況	依評鑑結果，進行後續改善及因應措施

風險評鑑表填寫說明



◆ **目前控制措施**

- 就該個資檔案現有之管控措施，如：檔案櫃鑰匙管控、檔案室進出紀錄、電子檔案加密、系統權限帳密管控等。

◆ **個資筆數**

- 以當年度單位或系統可能產出的資料、經手數量或儲存文件作估計，以人數計算，一人代表一筆個資。共分四個區間未滿1萬、1萬到5萬未滿、5萬到25萬未滿、25萬以上。

風險評鑑表填寫說明(續)

對應一致性

檔案類型	儲存位置	目前控制方式
紙本檔案	➢ 檔案室、部室檔案櫃、個人座位檔案櫃、外倉 ➢ 經手不留存；但如有暫存期間，仍請填寫暫存處（通常為個人抽屜、檔案櫃）	鑰匙管控、出入登記、門禁系統
電子檔案	個人電腦、部門共用槽	帳密管控、權限管控、檔案加密
系統資料	資訊系統	帳密管控、權限管控、資料庫遮罩

風險評鑑表填寫說明(續)

CIA等級			弱點威脅評鑑			
機密性	完整性	可用性	因威脅及弱點而產生之情境(一)	發生可能性	因威脅及弱點而產生之情境(二)	發生可能性

◆ **機密性**

- 依個人資料保護法令、國際標準及對於當事人權益影響程度作劃分。參照「個人資料類別」圈選欄位，共分四級。

◆ **完整性**

- 依**資料毀損恢復時間**，評估本公司所保有之個資檔案被竄改、刪除/銷毀、毀損時，對於單位（含本公司其他單位）或作業流程之影響程度，共分四級。

◆ **可用性**

- 依**使用單位數量、使用時間長短**，評估該類別之個資檔案，被多少單位業務或作業流程所使用，或其使用頻率，共分四級。

★ CIA等級各項等級說明，可參考「CIA評估定義」填寫。

風險評鑑表填寫說明(續)

CIA等級			弱點威脅評鑑			
機密性	完整性	可用性	因威脅及弱點而產生之情境(一)	發生可能性	因威脅及弱點而產生之情境(二)	發生可能性

◆ 因威脅及弱點而產生之情境(一)(二)

針對檔案之保密管理或措施，而有竊取、竄改、毀損或外洩風險，如：未有作適當去識別化
針對檔案之存取權限管理或措施，而有竊取、竄改、毀損或外洩之風險，如：單位同仁已轉調他部門，但未將系統權限作變更
針對檔案傳輸之管理或措施，而有竊取、竄改、毀損、遺失或外洩之風險，如：檔案未加密即進行轉送，導致資料洩露
針對檔案處理或利用之安全管理或措施，而有竊取、竄改、毀損、遺失或外洩之風險，如電腦攜出後遺失
針對檔案保存或歸檔之管理或措施，而無法辨識保存期限、逾越保存期限或提早銷毀或刪除，如：保存期間之起算時點不明，無從計算保存時間、未定期執行檔案銷毀而逾保存期限
針對檔案之儲存位置建立、管理或措施，而有竊取、竄改、毀損、遺失或洩露之風險，如：含有個資之文件，擺放至部門雲端資料夾未有管控方式、離職同仁未有交接機制、檔案調閱機制未有落實執行
存取檔案之軌跡或紀錄之保存，而有無法或困難進行問題追蹤或證據保存

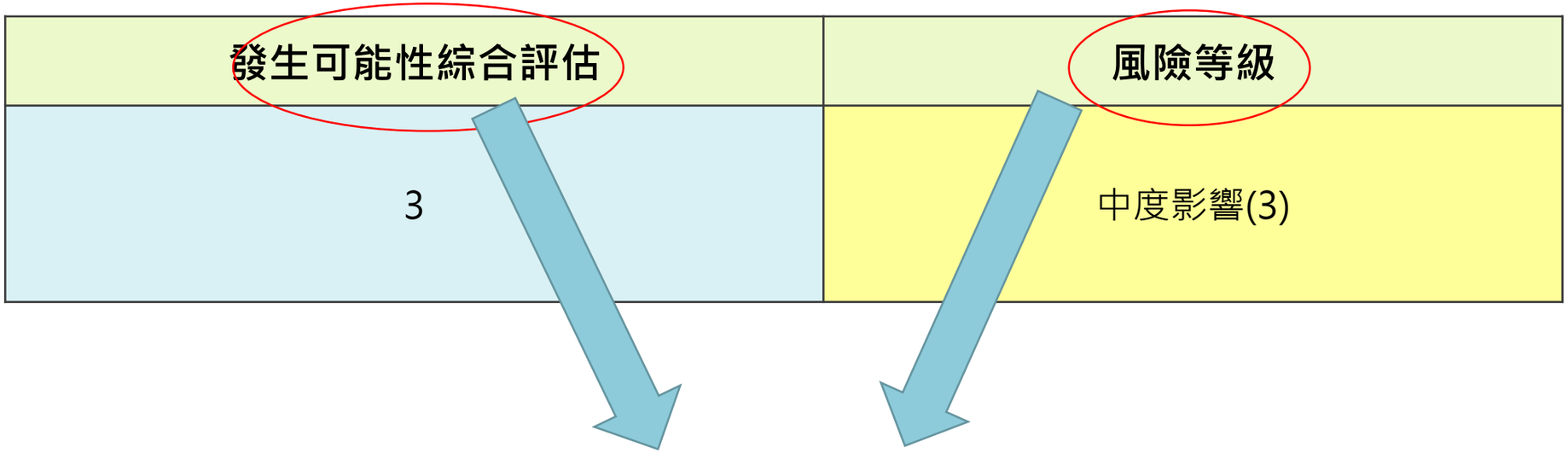
◆ 發生可能性

風險評鑑表填寫說明(續)

發生可能性		
等級	權值	定義
高度	3	(1)一年內情境發生4次(含)以上 (2)風險未曾發生但風險存在，旦發生可能性超過60%
中度	2	(1)一年內情境發生2至3次 (2)風險未曾發生，但發生可能性31~60%
低度	1	(1)一年內情境發生0~1次，或 (2)風險未曾發生，但發生可能性不到30%
分級定義說明	同時滿足多條件時，以滿足較高量化分級之條件為主 例：某風險一年內雖發生不到一次，但感受到風險的存在，但評斷後認為發生可能性有50%左右，評等為2。	

針對定義(2) 評核標準		
	公司尚未有規範	公司有規範
未落實安全措施	3	2
有落實安全措施	2	1

風險評鑑表填寫說明(續)



若函數沒有問題，填列完成發生頻率之選項後，即會呈現上表之顯示數值及風險等級。

大綱

- 個資檔案盤點表填寫試做說明
- 個資檔案風險評鑑表填寫試做說明
- 問題與討論

歡迎提問
敬祈指教

THANK YOU

數位轉型．軟體技術．資安產業．數位經濟