



# 個人資料檔案盤點暨風險評鑑 教育訓練

2022.04.20

2022.05.02

# 大綱

2

- 為什麼需要保護個資
- 個人資料的定義
- 個資盤點實作說明
- 風險評鑑作業說明
- Q&A

3

# 為什麼需要保護個資

# 執行個人資料管理制度的目的

4

- 個資法第27條
  - 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。
- 個資法施行細則第12條
  - 個資法...第二十七條第一項所稱適當之安全措施...，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

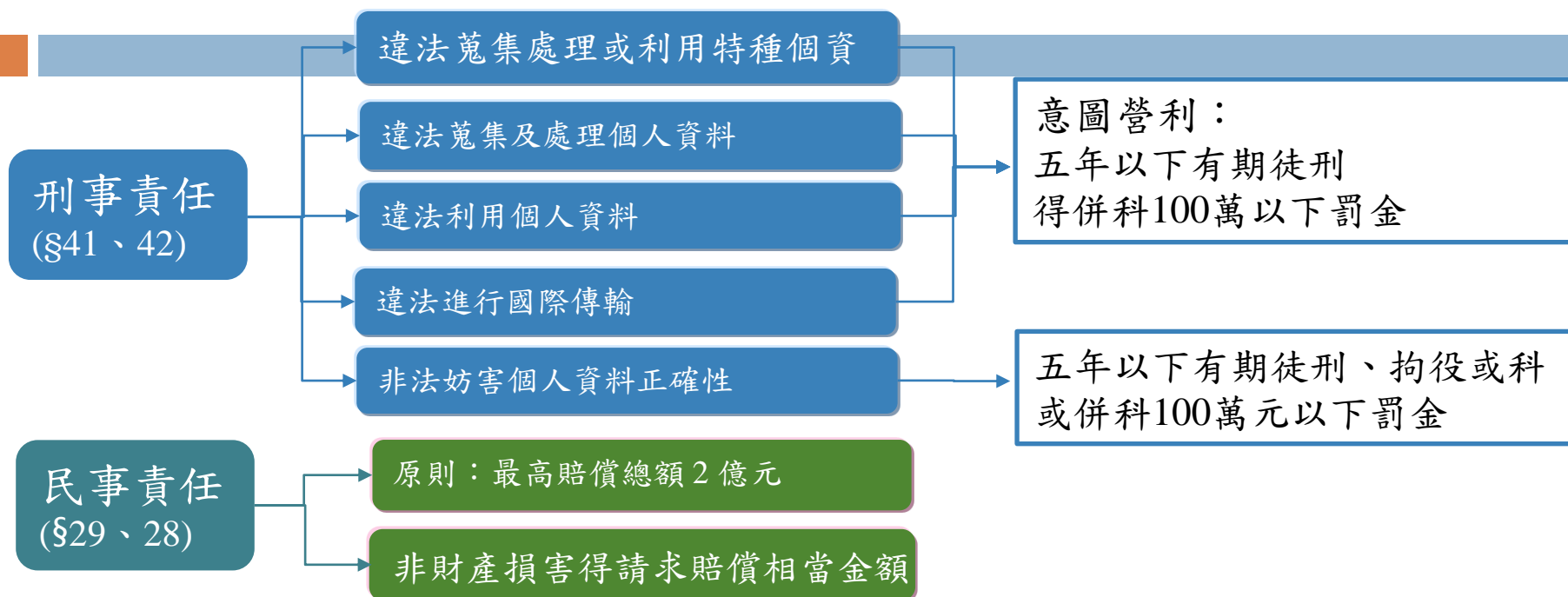
# 適當安全防護措施 (個資法施行細則§12)

5



# 法律責任-非公務機關

6



非公務機關違反本法規定，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。但能證明其無故意或過失者，不在此限。(§29)



# 個資法罰則說明

7

## □ 個人資料保護法第28條

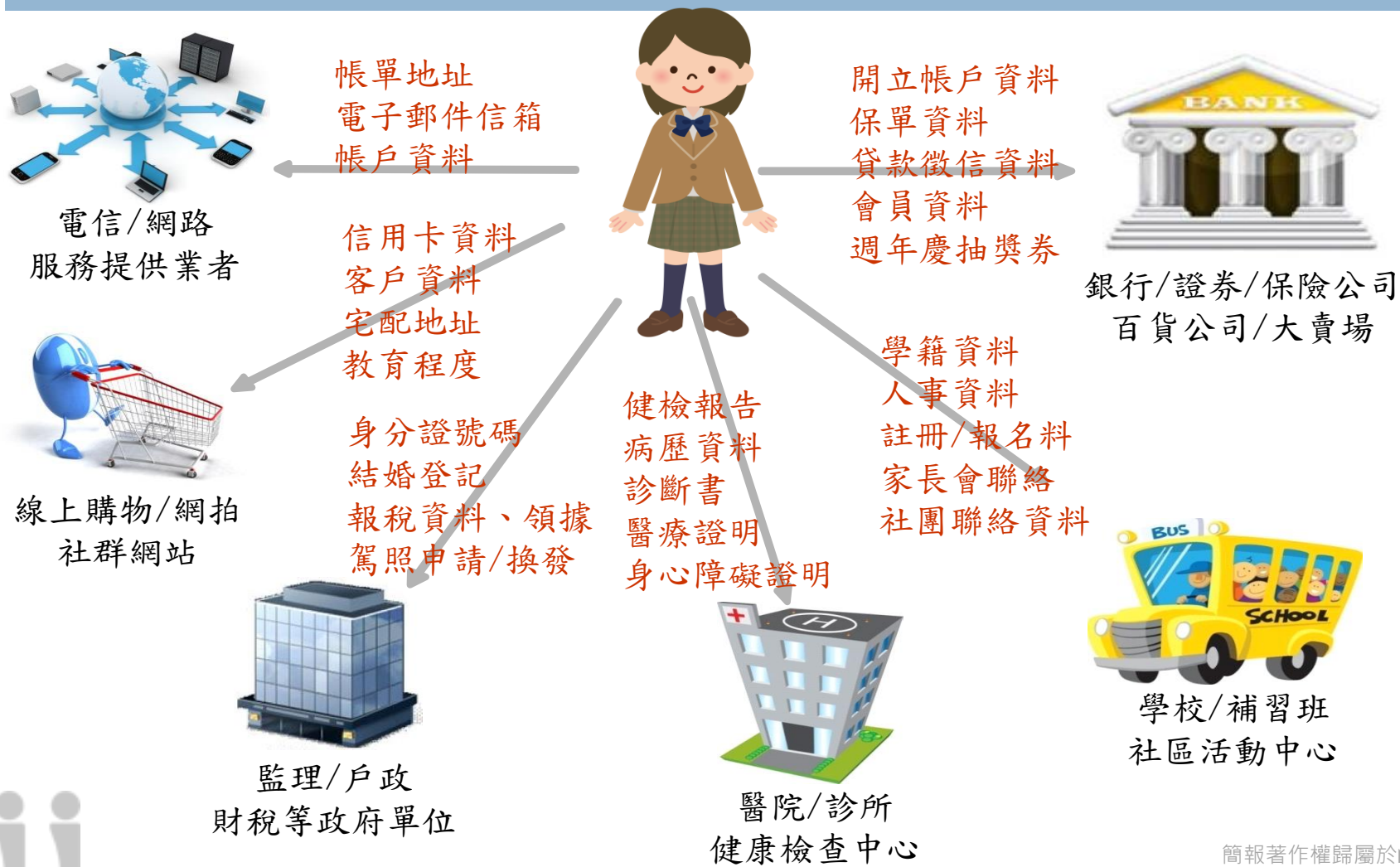
- 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
- 被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
- 依前二項情形，**如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。**
- 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。
- 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。
- 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

## □ 個人資料保護法第29條

- 非公務機關違反本法規定，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。但能證明其無故意或過失者，不在此限。
- 依前項規定請求賠償者，適用前條第二項至第六項規定。

# 個資.....在那裡？

8



簡報著作權歸屬於NII  
簡報內容僅供參考，並非任何法律意見，請斟酌使用簡報



# 可能的個資外洩管道

9


- ▶ 問卷
- ▶ 內部人員
- ▶ 網購
- ▶ 掛馬網站、設計不良的網站
- ▶ APT攻擊、駭客
- ▶ 社群網站
- ▶ P2P軟體使用
- ▶ 入會申請單
- ▶ 客服中心
- ▶ 補習班
- ▶ 電子謄本系統
- ▶ 直銷公司
- ▶ 盜版光碟
- ▶ 即時通訊軟體(IM)
- ▶ 無個資保護認知
- ▶ 釣魚網站
- ▶ 委外廠商

# 扯！承辦員寄信夾錯檔

# 中正大學6千學生個資外洩

10

[一名網友今在臉書爆料，中正大學通識中心今天寄來一封電子郵件，附檔竟是 2015 到 2019 學年度所有入學的學士班個資，不僅有手機、身分證字號等，就連身心障礙等身份註記也一覽無遺。中正大學主秘坦承疏失，已懲處夾錯檔案釀禍的承辦人員]



The screenshot shows an Excel spreadsheet with the following columns: 學號 (Student ID), 中文姓 (Chinese Name), 身分證 (ID Card), 目前系 (Current Department), 目前系 (Current Department), 目前班 (Current Class), 目前年 (Current Year), 性別 (Gender), 出生年 (Year of Birth), 籍別身 (Residence/Status), and 入學 (Enrollment). The spreadsheet is titled '格式\_講座通知email名單\_1090420.xlsx' and is currently unsaved.

資料來源-蘋果新聞網2020/10/13

簡報著作權歸屬於NII  
簡報內容僅供參考，並非任何法律意見，請斟酌使用簡報

# 正確面對「個資法」

11

迴避個資法



過度恐慌

避免接觸個資

瞭解個資法



適當刪除與銷毀

安全處理與使用

維護個資正確



降低違法風險

12

# 個人資料的定義

# 何謂個人資料 (個資法§2、§6)

13

自然人的

- 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
- 聯絡方式
- 財務情況
- 社會活動

個資法§2

一般  
資料



特種  
資料

- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

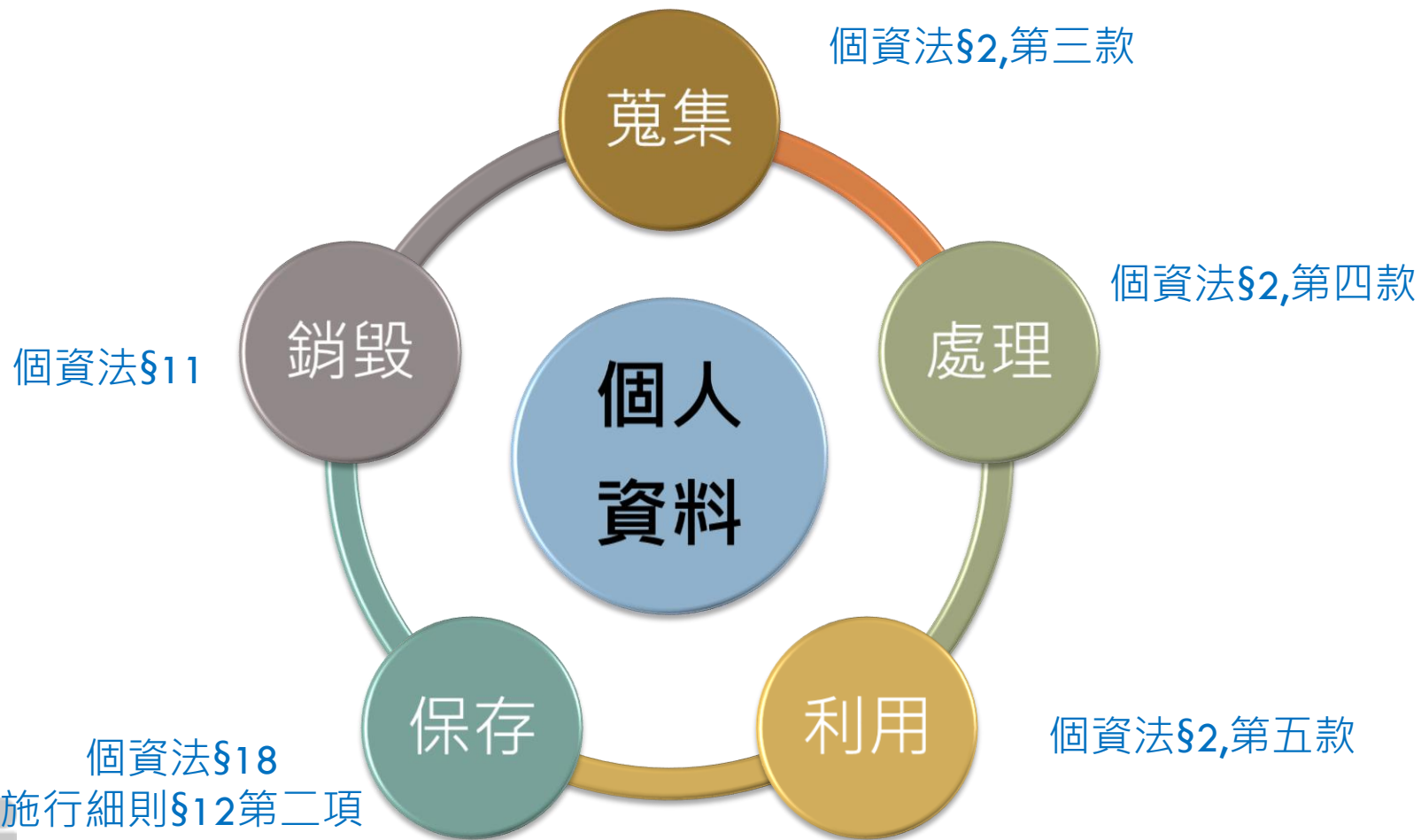
有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。(個資法§6)

其他  
資料

- 得以直接或間接方式識別該個人之資料

# 個人資料生命週期

14



# 蒐集之定義

15

- 何謂蒐集？ (§15符合特定目的)
  - 指以任何方式取得個人資料。
    - 直接蒐集：直接從當事人取得個人資料。(§8)
    - 間接蒐集：透過第三方取得個人資料。(§9)
      - 委外：如人力仲介、市調公司等。
      - 外部取得：如主管機關、聯合招募單位。

## 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。

## 第 9 條

公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，**應於處理或利用前，向當事人告知**個人資料來源及前條第一項第一款至第五款所列事項。

# 處理之定義

16

- 何謂處理？ (§15符合特定目的)
  - 指為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 (§11)、複製、檢索、刪除、輸出、連結或內部傳送。
    - 新增文件、建檔案、輸入系統。
    - 編輯檔案、刪除檔案、儲存檔案、複製檔案。
    - 檢索查詢、更正錯誤、製作連結。
    - 內部傳送至別部門/單位。



# 利用之定義

17

- 何謂利用？ (§16符合特定目的及目的外之利用)
  - 指將蒐集之個人資料為處理以外之使用。
    - 對當事人使用其個資：如使用通訊錄打電話或寄信、E-mail。
    - 揭露第三方：如提供檢調單位調查、提供主管機關備查、提供勞健保給勞健保機構、提供報稅資料給國稅局、稅捐單位。



18

# 個資盤點實作說明

# 個資盤點注意事項-1

19

- 每年應至少執行一次個資檔案鑑別作業
- 資料類型：電子與紙本應分開列示
- 數量：每年經手量與總量
- 個資生命週期之各項權責，非單一部門或窗口之業務
  - ▣ 需要各單位充分配合及整合協調
  - ▣ 耗費時間與人力

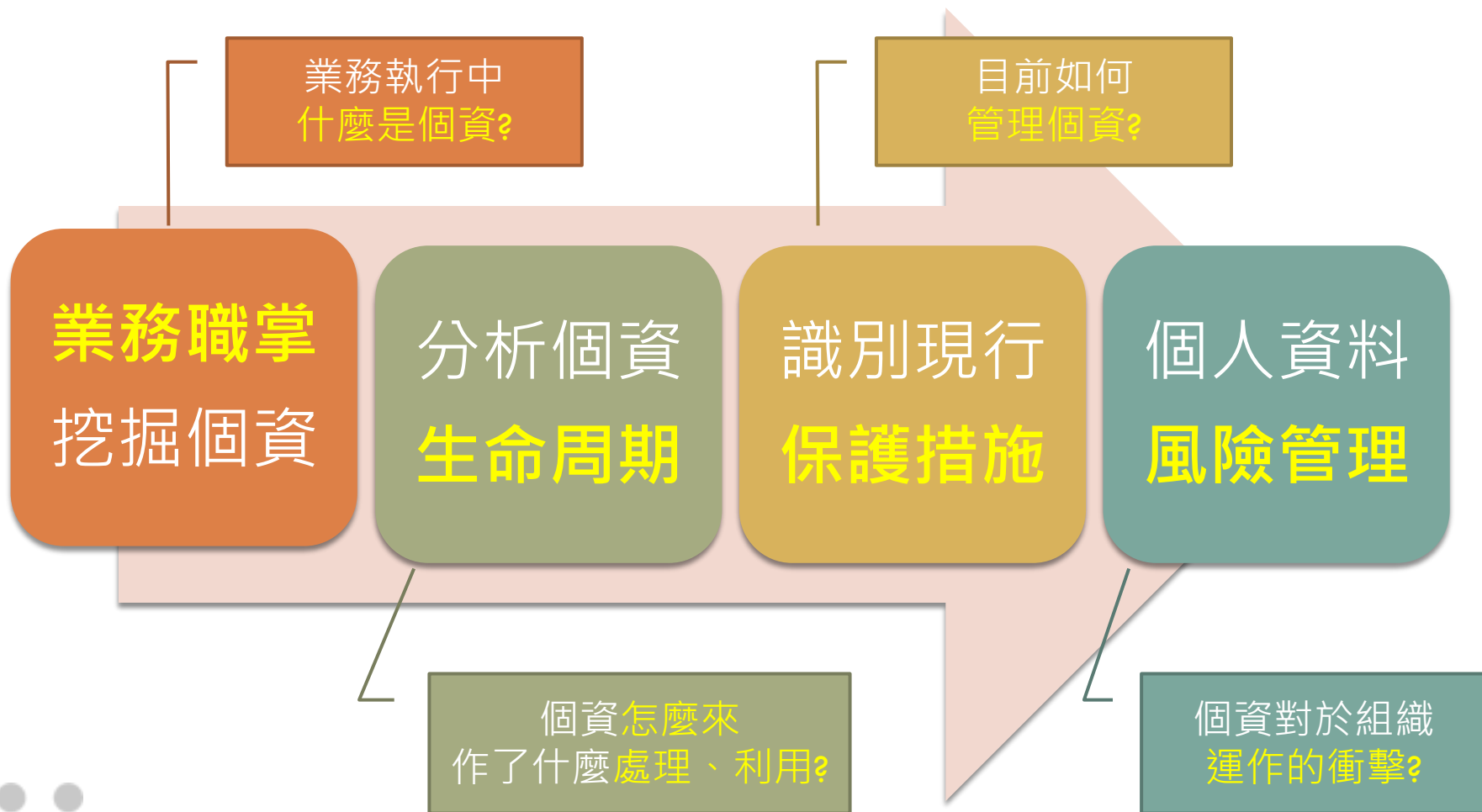
# 個資盤點注意事項-2

20

- 得因應變動情況，調整個資清冊
  - 組織變更
  - 作業流程改變
    - 處理方式或使用表單調整，適當調整清冊欄位
    - 業務增加會簽單位，於處理單位欄位註記
  - 個資資產異動
    - 依個資檔案屬性變動，刪除或增加個資資產
    - 一次性業務之銷毀
  - 因應法規之修改
    - 法律/保存依據若有修訂、調整
    - 保存期限改變

# 個資檔案盤點程序

21



# 從業務面識別出個人資料檔案技巧(1)

22

- 在開始執行識別個人資料檔案前
  - ▣ 應清楚自己的個人業務(工作內容)
  - ▣ 應清楚什麼是個人資料
- 接著你(妳)可以想想~~

處理的個人資料怎麼來的？

處理業務時，這些個人資料是被呈現在那裡(例如XX表單，或XX系統)？

這些你(妳)所經手處理的個資，需不需要再提供給其他內部單位或外部單位？

如果需要提供給內部單位，你(妳)是用什麼方式提供？

如果需要提供給外部單位，是否有相關法規依據，或是跟外部單位之間有沒有契約或類契約關係？用什麼方式提供給外部單位

# 從業務面識別出個人資料檔案技巧(2)

23

## □ 接著可以想想~~

資料若由你(妳)進行最後的保存，你(妳)有沒有針對這些資料依法規要求訂定保存期限？

通常你(妳)多久會檢視資料要不要銷毀或刪除？

你(妳)所處理的資料，有沒有確實銷毀或刪除？

你(妳)以什麼方式進行銷毀或刪除？

資料若由你(妳)進行最後的保存，保存、放置的位置在那裡？適不適當？

資料保存、放置的位置有沒有相關的控制方式(例如系統存取權限設定管理)？

# 個人資料檔案清冊說明

24

業務職掌  
挖掘個資

分析個資  
生命周期

識別現行  
保護措施

個人資料  
風險管理

流程名稱	個人資料檔案名稱	資料類型	個人資料範圍	數量	保有依據	特定目的	個人資料類別	特種資料	蒐集		
									來源	方式	單位



# 個資業務流程 (識別來源/個人資料流分析)

25

- 識別出業務流程主要的元件
  - ▣ 工作執掌一覽表、業務分層明細表
  - ▣ 紙本：表單/作業紀錄等
  - ▣ 電子：系統/個人電腦 等相關自動化儲存設備
- 個人資料流分析
  - ▣ 個人資料如何透過業務流程被蒐集、處理、利用、保存、銷毀等行為
  - ▣ 非例行業務之個資流(會簽業務，資料留存時)

# 個人資料範圍\_蒐集欄位

26

個人資料範圍(\$2)	內容
姓名	中文姓名、英文姓名
出生年月日	民國/西元 出生年月日
國民身分證統一編號	身分證字號
員工編號 / 學號	員編、員工編號、工號、學號
護照號碼	護照號碼 或 居留證號碼
特徵	身高、體重、性別、年齡、血型、照片、 <b>生物辨識系統資料</b> (虹膜、掌紋、臉部)、捺印指紋、指紋資料庫、指紋辨識門禁系統
婚姻	婚姻狀況 ( 已婚、未婚、單身 )
家庭	家庭背景、家庭成員關係
教育	學經歷、專長、證照、專業訓練、語文能力、班級、科系
職業	服務單位、職稱、公務人員職等、評分表分數、差勤紀錄、工作績效
聯絡方式	手機、公務電話、住家電話、 <b>E-mail</b> 、戶籍住址、住家住址、公司住址
財務情況	<b>金融帳號</b> 、 <b>薪資</b>
社會活動	會員證號

# 個資數量

27

## □ 每年

- ▣ 年度蒐集約略數量

## □ 總量

- ▣ 單位保存總數量

## □ 計算方式

- ▣ 以紀錄/檔案裡的個資量為計數基礎

- 例如：一份通訊錄紙本/電子檔裡有10筆通訊資料  
每年：約10筆；總量：約10筆



# 保有依據

28



## 法律明文規定

EX. 大學法、學生輔導法、全民健康保險法、會計法...

## 執行業務所需

因應提供之業務/服務，內部制定之辦法或要點。

EX. 明新學校財團法人明新科技大學組織規程、學生選課辦法、校內工讀助學金實施要點 ... ..

## 當事人同意

當事人自願提供個人資料

EX. 同意書

# 特定目的及個人資料類別

29

- 法務部於104/12/30修正公布
  - ▣ 182項特定目的；134項個人資料類別

The screenshot shows the official website of the Ministry of Justice of the Republic of China. The header includes the Ministry's logo and name in Chinese and English, along with a Google Custom Search bar. A navigation menu lists various services like 'Ministry Introduction', 'Online Services', 'Legal Database', etc. The main content area is titled 'Personal Information Protection' and includes a breadcrumb trail, social media icons, and a publication date of 101/10/01.

## (101年)個人資料保護法之特定目的及個人資料之類別修正總說明及對照表

修正「電腦處理個人資料保護法之特定目的及個人資料之類別」，並修正名稱為「個人資料保護法之特定目的及個人資料之類別」，定自中華民國一百零一年十月一日生效，業經法務部會同內政部、財政部、教育部、經濟部、交通部、文化部、蒙藏委員會、僑務委員會、中央銀行、行政院衛生署、行政院環境保護署、國立故宮博物院、行政院大陸委員會、行政院經濟建設委員會、金融監督管理委員會、行政院國軍退除役官兵輔導委員會、行政院原子能委員會、行政院國家科學委員會、行政院農業委員會、行政院勞工委員會、公平交易委員會、行政院公共工程委員會、行政院原住民族委員會、行政院體育委員會、客家委員會、國家通訊傳播委員會修正發布施行。

參考來源：<https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL010631>

# 列舉-個人資料保護法之特定目的

30

## 特定目的 - 共182項

代號	修正特定目的項目
○○一	人身保險
○○二	人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）
○○三	入出國及移民
○○四	土地行政
○○五	工程技術服務業之管理
○三一	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
○四二	兵役、替代役行政
○四三	志工管理
○六九	契約、類似契約或其他法律關係事務
○七三	政府資訊公開、檔案管理及應用
一〇九	教育或訓練行政
一一〇	產學合作
一一八	智慧財產權、光碟管理及其他相關行政
一五八	學生（員）（含畢、結業生）資料管理
一五九	學術研究
一三五	資（通）訊服務
一三六	資（通）訊與資料庫管理
一三七	資通安全與管理

# 個人資料類別-節錄學校相關

31

## □ 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

## □ C002 辨識財務者

- ▣ 金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等

## □ 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

# 個人資料類別-節錄學校相關

32

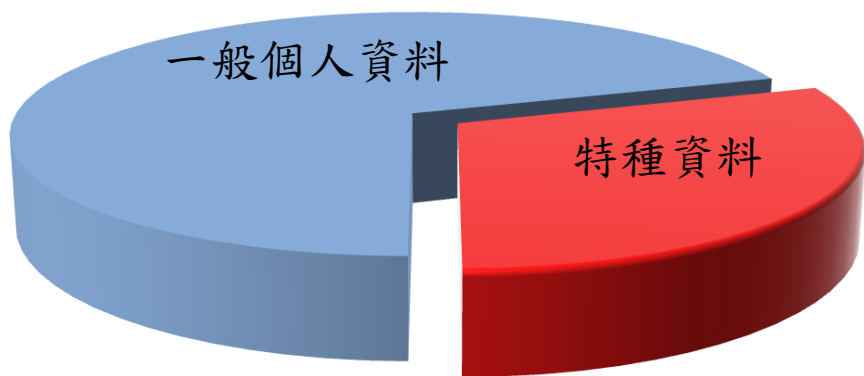
- C052 資格或技術
  - ▣ 學歷資格、專業技術、特別執照（如飛機駕駛執照等）、政府職訓機構學習過程、國家考試、考試成績或其他訓練紀錄等
- C061 現行之受僱情形
  - ▣ 僱主、工作職稱、工作描述、等級、受僱日期、工時、工作地點、產業特性、受僱之條件及期間、與現行僱主有關之以前責任與經驗等
- C081 收入、所得、資產與投資
  - ▣ 總收入、總所得、賺得之收入、賺得之所得、資產、儲蓄、開始日期與到期日、投資收入、投資所得、資產費用等
- C111 健康紀錄 (§6)
  - ▣ **醫療報告、治療與診斷紀錄**、檢驗結果、**身心障礙種類、等級**、有效期限、**身心障礙手冊證號**及聯絡人等



# 特種資料

33

## □ 確定蒐集客體



### 特種資料

病歷

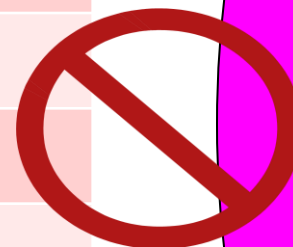
醫療

基因

性生活

健康檢查

犯罪前科



原則不得蒐集處理或利用

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。 (§6)

# 特種資料得蒐集、利用或處理之例外情況

34

- 法律明文規定。
- 公務機關執行法定職務或非公務機關執行法定義務所必要，  
且有適當安全維護措施。
- 當事人自行公開或其他已合法公開。
- 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、  
處理或利用。

# 個人資料檔案清冊說明

35

業務職掌  
挖掘個資



分析個資  
生命周期



識別現行  
保護措施



個人資料  
風險管理

蒐集			處理						利用						
來源	方式	單位	處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍

# 蒐集

36

## □ 蒐集來源

- 當事人
- 某系統提供
- 別單位、網站、問卷

## □ 蒐集方式

- 直接蒐集(§8)：直接從當事人取得個人資料
- 間接蒐集(§9)：透過第三方(明新科大以外的組織)取得個人資料

## □ 蒐集單位：對當事人蒐集之源頭單位



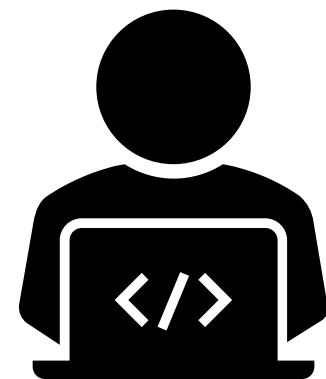
校內系統  
(直接)

校外系統  
(間接)

# 處理

37

- 處理方式(描述資料蒐集後之處理流程)
  - ▣ 1.報名者至活動報名系統報名 (Input)
  - ▣ 2.彙整統計建置電子表單 (或輸入至XX系統)
  - ▣ 3.查詢、列印使用
  - ▣ 4.內部傳送至A、B、C部門會簽
  - ▣ 5.儲存至個人電腦/內部伺服器主機
- 處理單位
  - ▣ 1.自己單位
  - ▣ 2.其他協助處理單位(下一關)



# 保存

38

- 保存單位：最終保存紙本或電子檔案或資料庫等資產之單位
- 保存期限：法律 > 辦法 > 內規
  - 保存10年
  - 離職後保存2年
  - 單位不留存
  - 業務持續期間

保存期限訂定參考方向：

- 一、法律明文規定
- 二、大專校院類檔案保存年限基準表



# 銷毀

39

- 形式：銷毀的方式
  - 碎紙機銷毀
  - 檔案刪除
  - 集中統一銷毀 / 委外銷毀
  - 提出系統需求單由資訊單位刪除
- 頻率：多久銷毀一次
  - 每年檢視
  - 每年一次
  - 檔案持續更新/覆蓋



# 利用

40

- 期間：利用個資期間
  - ▣ 業務期間
- 地區：利用地區
  - ▣ 境內、國外
- 單位：利用單位
  - ▣ 自己單位
- 方式：利用或揭露個資之方式
  - ▣ 聯絡當事人(如使用通訊錄打電話或E-mail)
  - ▣ 揭露





# 揭露

41

- 對象：揭露之機關、單位
  - 提供主管機關備查、提供勞健保給勞健保機構、提供報稅資料給國稅局、稅捐單位
- 方式目的：提供之方式
  - 透過系統上傳、E-mail方式、公文方式、彌封寄送、存放光碟片寄送
- 揭露個資範圍：揭露給第三方哪些個資欄位



# 個人資料檔案清冊說明

42

業務職掌  
挖掘個資



分析個資  
生命周期



識別現行  
保護措施



個人資料  
風險管理

處理

利用

處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍
------	------	------	------	------	------	----	----	----	----	------	------	--------

現有控制措施



# 現有控制措施

43



紙本文件  
(Document)

- 上鎖倉庫、資料櫃、抽屜、防潮箱.....

電子檔案  
(Data)

- 個人電腦帳密管理
- 儲放於 **XX系統** 帳密管理
- 共享資料夾權限管理
- 備份硬碟上鎖管理.....

# 個人資料檔案清冊說明(cont.)

44

業務職掌  
挖掘個資



分析個資  
生命周期



識別現行  
保護措施



個人資料  
風險管理

利用							現有控制措施	個資範圍評估	個資檔案管理角色
期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍			



# 隱私衝擊分析 (個資範圍評估值)

45

衝擊影響程度	個資範圍評估值	個資範圍
極高	4	符合下列一項： ●含自然人之姓名及特種個資。 ●含國民身分證統一編號 (或護照號碼) 及特種個資。
高度	3	符合下列一項： ●含國民身分證統一編號(或護照號碼)及其他個資。 ●含自然人之姓名及財務情況 (如：帳號)。
中度	2	含自然人之姓名或學號及其他個資，但不包含國民身分證統一編號、財務情況或特種資料。
一般	1	符合下列一項： ●屬於保管單位，但不接觸個資。 ●兩項其他個資(含)以上，但不包含姓名、學號、國民身分證統一編號、財務情況等無法直接識別當事人之項目組合。

# 個資檔案清冊說明

個人資料檔案名稱	資料類型	個人資料範圍	利用							現有控制措施	個資範圍評估值
			期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍		
學生聯絡資訊檔	電子	姓名、職稱、聯絡方式	業務期間	臺灣	各業務單位	聯絡當事人	無	無	無	承辦人儲存於PC，登入需帳號密碼	2
身心障礙者名冊(含附件)	紙本	姓名、身分證字號、出生年月日、聯絡方式、醫療	業務期間	臺灣	人事室	揭露	教育部	系統上傳	姓名、身分證字號、出生年月日、聯絡方式	歸檔上鎖保存，調閱需填單	4

# 個人資料管理角色

47



## 資料控制者 (Data Controller)

決定個人資料處理之目的  
與方法之主體。

主導該作業流程/業務



## 資料處理者 (Data Processor)

實際執行個人資料處理之  
主體，依資料控制者指示  
行事之主體。

協助或經手該作業流程/業  
務



## 共同資料控制者 (Joint Data Controller)

二個或二個以上資料控制  
者共同決定個人資料處理  
之目的及方法之主體。

有兩方(含)以上主導該作業  
流程/業務

# 個資檔案管理角色

48

個人資料檔案名稱	資料類型	個人資料範圍	處理單位	保存單位	現有控制措施	個資檔案管理角色
學生聯絡資訊檔	電子	姓名、職稱、聯絡方式	各單位	各單位	承辦人 <b>儲存於PC</b> 登入需帳號密碼	<b>資料控制者</b>
畢業名冊(含附件)	紙本	姓名、身分證字號、出生年月日、聯絡方式	各系辦	教務處	單位不留存	<b>資料處理者</b>



# 不須盤入個人資料檔案之個人資料

49

## ◆ 剔除下列不受個資法保護的資料 (§ 51)

- 自然人為**單純個人**（例如：社交活動等）或**家庭活動**（例如：建立親友通訊錄等）而蒐集、處理或利用的個人資料。
  - 上述資料屬**私生活目的**所為，與職業或業務職掌無關。
- 於**公開場所或公開活動**中所蒐集、處理或利用之**未與其他個人資料結合**之影音資料。
  - 在網際網路上張貼影音個人資料，屬表現自由之一部分。

# 個資盤點清冊諮詢常見問題(1/2)

- 公開資訊不需列入盤點，例如學校官網查詢到之同仁姓名、單位、分機等資訊。
- 不清楚個資流程角色定義。
- 不同資料類型(電子/紙本)未分開盤點。(面臨之風險不同)
- 蒐集過多個人資料範圍(欄位之合理性與最小化)
- 個資數量未區分**每年數量**與**保有之總數量**。
- 保存期限的合理性(**法律 > 內部辦法或要點 > 當事人同意**)。



# 個資盤點清冊諮詢常見問題(2/2)

- 將校外系統列為「個人資料檔案名稱」(校外系統本校無資料之控制權)。
- 未依規定留存個資，如核銷單據正本已送財務處，但同仁自行留存影本(特定目的已完成，不應繼續留存其個資)。
- 清冊欄位定義不清楚，如：
  - 特定目的
  - 個資類別
  - 蒐集方式(直接蒐集/間接蒐集)
- 未識別「揭露」，如資料會提供給校外單位。

52

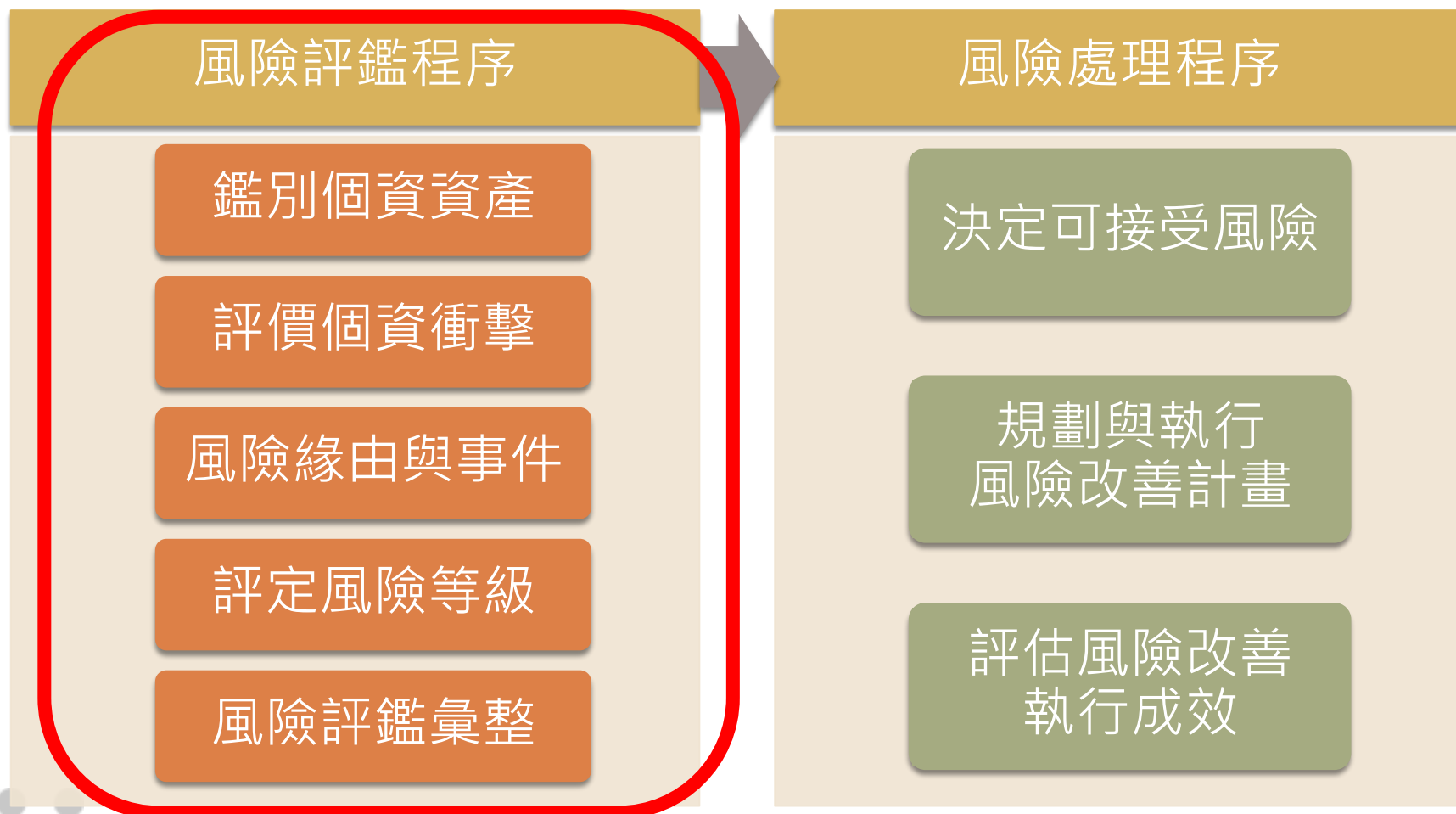
# 風險評鑑作業說明

# 風險管理所帶來的效益

53

- 識別個人資料檔案 → 我需要保護什麼
- 識別風險來源、事件 → 我需要採取何種對策
- 計算風險 → 我需要多少時間、人力、或成本來  
保護個人資料檔案

# 風險評鑑與風險處理



# 風險評鑑工具

55

## □ 風險評估表

	A	B	C	D	E	F	G	H	
1	風險評估表(紙本)			機密等級： <input type="checkbox"/> 機密 <input checked="" type="checkbox"/> 限閱 <input type="checkbox"/> 內部 <input type="checkbox"/> 公開					
2	文件編號：			填表日期：_____年_____月_____日					
3	個資資產編號：			蒐集單位：					
4	流程名稱：			保有單位：					
5	個人資料檔案名稱：			個資範圍評估值：					
6	個人資料範圍：								
7	資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0	
8							0		
9									
10									
11									
12									

# 風險緣由與事件

56

風險緣由

誘發

事件

**定義：可能導致風險的要項**

- 未告知個資法要求應告知事項
- 教育訓練不足
- 資料銷毀處理程序不當或不足(如：儲存媒體內之資料沒有適當刪除就丟棄或重覆使用)

**定義：所發生的變動或特定情況**

- 未遵循法令法規
- 不熟悉法令法規及內部規範。
- 個人資料被竊取、竄改、毀損、滅失或洩漏。



# 風險評估分析構面表-1-1

57

評估值	衝擊影響
4	<p><b>嚴重傷害：</b></p> <ol style="list-style-type: none"><li>1. 個資保管數量<b>50,001筆以上</b>，若全數外洩，對組織造成財務影響(損失超過1000萬元以上)。</li><li>2. <u>對組織形象造成嚴重的影響</u>，該風險對組織造成嚴重的衝擊(電視及平面媒體或海外媒體大肆負面報導)。</li><li>3. <u>該風險產生會造成嚴重違反法令之情形</u>，該風險會造成同仁與其直屬主管遭受法律上的求償及刑事訴訟，高階主管可能需下台負責。</li></ol>
3	<p><b>重大傷害：</b></p> <ol style="list-style-type: none"><li>1. 個資保管數量<b>5,001-50,000筆</b>以內，若全數外洩，對組織造成財務影響(損失低於1000萬元以內)。</li><li>2. 對組織形象造成嚴重的影響，該風險對組織造成重大的衝擊(平面媒體的負面報導)。</li><li>3. 該風險會造成同仁與其直屬主管遭受法律上的求償。</li></ol>

# 風險評估分析構面表-1-2

58

評估值	衝擊影響
2	<p><b>中度傷害：</b></p> <ol style="list-style-type: none"><li>1. 個資保管數量<b>501-5000筆</b>以內，若全數外洩，對組織造成財務影響(損失低於100萬元以內)。</li><li>2. 對組織形象造成輕微的影響，該風險造成的衝擊可接受。</li><li>3. 該風險會造成同仁與其直屬主管遭受內部的懲處。</li></ol>
1	<p><b>低度傷害：</b></p> <ol style="list-style-type: none"><li>1. 個資保管數量<b>500筆以內</b>，若全數外洩，對組織造成財務影響(損失低於100萬元以內)。</li><li>2. 該風險造成任何關於法令法規的影響有限。</li></ol>

# 衝擊影響評估範例

59

校內舉辦本年度個資宣導教育訓練，由參加者自行上網報名。本次活動共計509位報名，承辦人已保留10年的歷史資料。

資料週期	風險緣由	事件	衝擊影響
全階段	教育訓練不足	不熟悉法令法規及內部規範	3
蒐集	未告知個資法要求應告知事項	未遵循法令法規	2
處理	未訂定保存期限	個人資料被竊取、竄改、毀損、滅失或洩漏	3
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏	2

# 風險評估分析構面表-2

60

評估值	可能性
4	<p><b>該風險常導致此事件發生</b></p> <ol style="list-style-type: none"><li>1. 年度內曾發生類似的事件2次以上。</li><li>2. 組織未採用任何的控制或管理措施。(如：無制定保存年限且資料皆無銷毀、未識別法律依據且未對個資當事人進行告知)</li></ol>
3	<p><b>該風險曾導致此事件發生</b></p> <ol style="list-style-type: none"><li>1. 年度內曾發生類似的事件。</li><li>2. 個人資料保護之程序機制已建立，惟未落實執行或程序機制不完整。(如：已制定保存年限但未銷毀、未進行安全管控機制)</li></ol>
2	<p><b>該風險可能導致此事件發生</b></p> <ol style="list-style-type: none"><li>1. 3年內曾發生類似的事件。</li><li>2. 個人資料保護之程序機制未建立，但仍採有部分之控制措施。(如：尚未建立個資保護機制但進行文件上鎖、機敏檔案已進行加密控管)</li></ol>
1	<p><b>該風險導致此事件發生的機會極低</b></p> <ol style="list-style-type: none"><li>1. 3年以上未曾發生類似的事件。</li><li>2. 個人資料保護之程序機制已建立並落實執行。</li></ol>

# 可能性評估範例

61

承上，本校第一次舉辦個資宣導教育訓練，於報名網站已依據個資法第8條，告知當事人相關應告知事項，要求填寫姓名、班級或單位與聯絡電話，報名資料一直保留於該網站上。

資料週期	風險緣由	事件	可能性
全階段	教育訓練不足	不熟悉法令法規及內部規範	3
蒐集	未告知個資法要求應告知事項	未遵循法令法規	1
處理	未訂定保存期限	個人資料被竊取、竄改、毀損、滅失或洩漏	3

# 個資檔案風險值計算

□ 風險值 = 個資範圍評估值 X (衝擊影響 + 可能性)

	A	B	C	D	E	F	G	H
1	風險評估表(紙本)			機密等級： <input type="checkbox"/> 機密 <input checked="" type="checkbox"/> 限閱 <input type="checkbox"/> 內部 <input type="checkbox"/> 公開				
2	文件編號：			填表日期：____年____月____日				
3	個資資產編號：			蒐集單位：				
4	流程名稱：			保有單位：				
5	個人資料檔案名稱：			個資範圍評估值：				
6	個人資料範圍：							
7	資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0
8							0	
9								
10								
11								
12								

風險值  
取  
最大值

# 風險評估範例

63

## 學生保險清冊

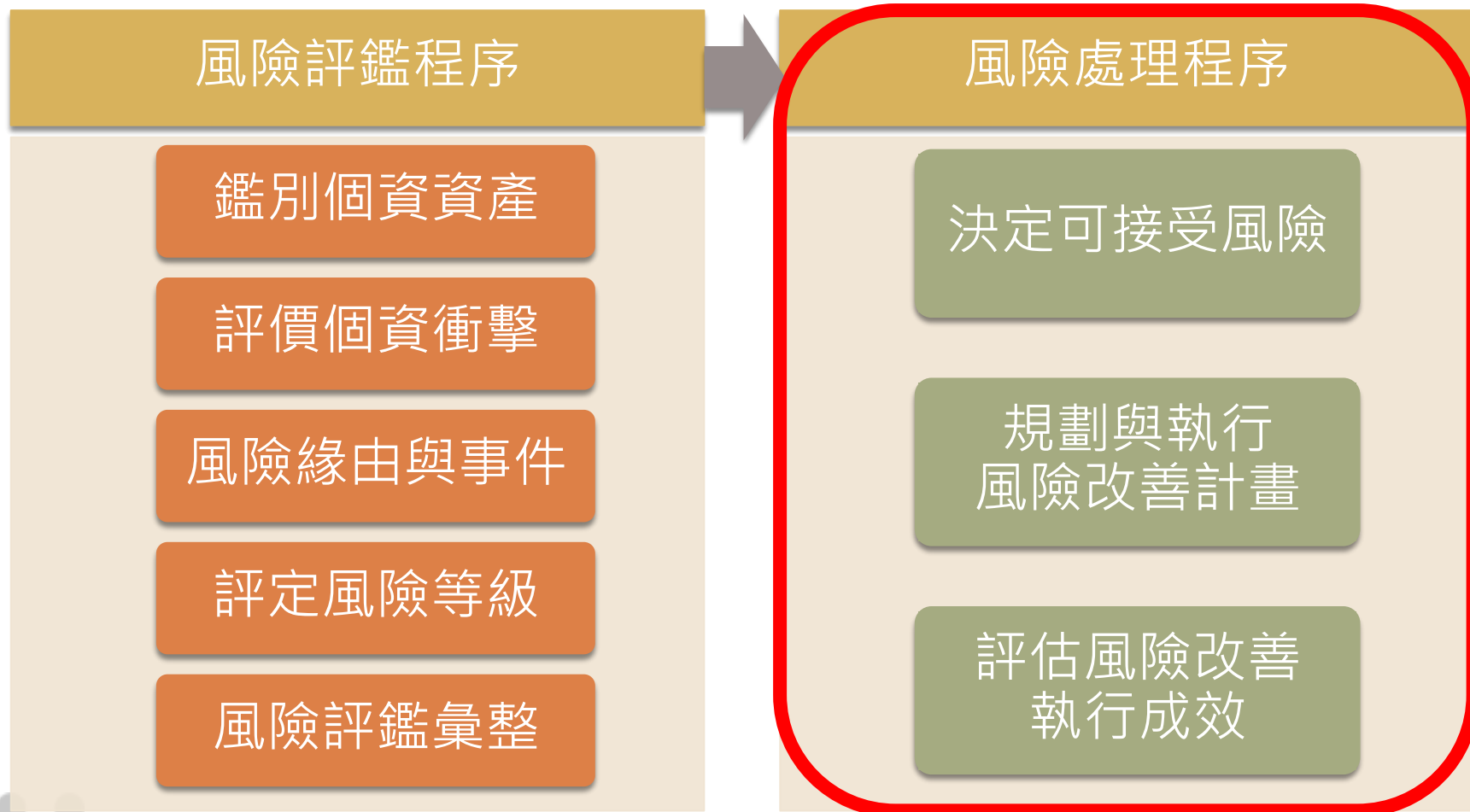
- 個資範圍評估值=3

## 風險值

- 取最大值 = 18

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
全階段	教育訓練不足	不熟悉法令法規及內部規範	3	1		12
蒐集	未告知個資法要求應告知事項	未遵循法令法規	1	3		12
處理	未訂定保存期限	個人資料被竊取、竄改、毀損、滅失或洩漏	3	3		18
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏	1	1		6

# 風險評鑑與風險處理





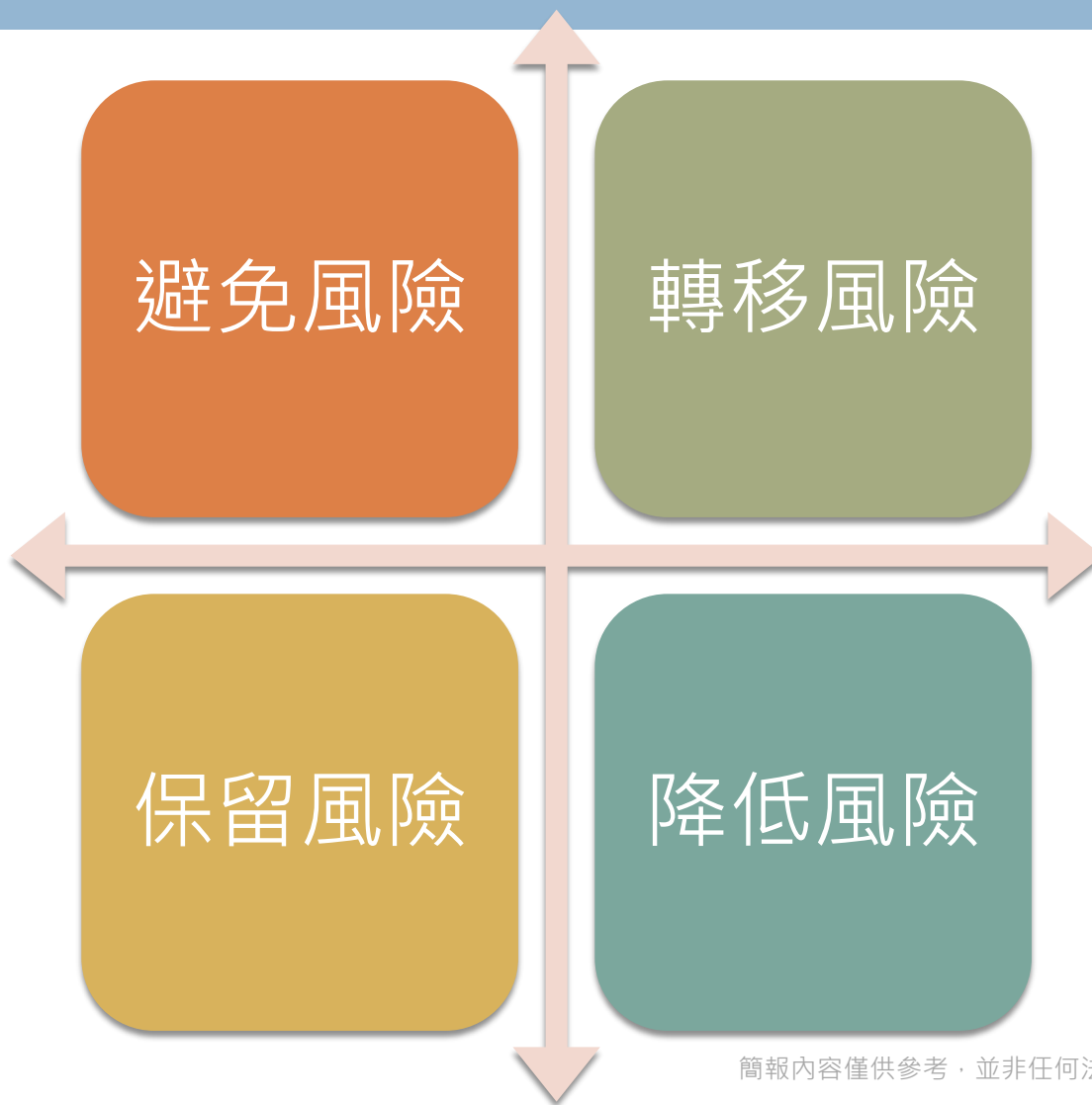
# 風險控管原則

65

- 決定組織可接受之風險值
- **高於可接受風險值者，優先控管或處理**
- 確認、控制及降低安全風險至可接受程度所採取的程序



# 風險控制策略



# 風險控制策略

- 避免風險
  - ▣ 修改作業方式或採用技術以避開風險
  - ▣ 經由政策或作業程序以禁止從事高風險交易或活動
- 轉移風險
  - ▣ 轉移相關之營運風險至他者，例如：承保商、供應商
- 保留風險
  - ▣ 知悉且客觀地接受風險
- 降低風險
  - ▣ 選擇適當之控制措施以降低風險
  - ▣ 藉由加強各項作業之內控以降低風險發生之機會

# 風險控制措施之選擇考量

- 時效性
  - ▣ 控制執行時間及有效期限為何
- 人力
  - ▣ 每年需要多少工時來監控和維護
  - ▣ 負責執行、監控及維護的人員需要接受多少訓練
  - ▣ 必須容易執行，了解對使用者造成多少程度不便
- 成本
  - ▣ 控制成本 < 資產價值, 威脅損失
- 法規或合約要求

# 風險處理階段

- 依據風險評鑑的結果，對於超出可接受程度之風險，進行處理
  - 降低風險發生機率
  - 降低風險造成之損害
- 風險處理計畫
  - 改善活動/控制措施
  - 風險進度追蹤
  - 風險再評鑑

# 風險處理工具

## □ 個人資料風險處理計畫表

個人資料檔案風險處理計畫										機密等級： <input type="checkbox"/> 機密 <input checked="" type="checkbox"/> 限閱 <input type="checkbox"/> 內部 <input type="checkbox"/> 公開										
文件編號：										版 次：1.0										
										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				風險再評鑑				
項次	單位	個資資產編號	資料類型	流程名稱	個人資料檔案名稱	個資評估值	風險緣由	事件	原風險值	風險處理型式	改善活動/控制措施	承辦人	預定完成日期	實際完成日期	覆核人員	風險處理進度	衝擊影響	可能性	風險值	覆核人員
										<input type="checkbox"/> 接受風險 <input type="checkbox"/> 降低風險 <input type="checkbox"/> 轉移風險 <input type="checkbox"/> 避免風險										
										<input type="checkbox"/> 接受風險 <input type="checkbox"/> 降低風險 <input type="checkbox"/> 轉移風險 <input type="checkbox"/> 避免風險										
										<input type="checkbox"/> 接受風險 <input type="checkbox"/> 降低風險 <input type="checkbox"/> 轉移風險 <input type="checkbox"/> 避免風險										

# 風險處理後

- 執行內部稽核，確保控制措施的有效性
- 當有下列情況時，執行風險評鑑作業
  - ▣ 每年定期執行
  - ▣ 營運組織變更
  - ▣ 作業流程改變
  - ▣ 資產新增或變更
  - ▣ 發生重大個資安全事件



# Q & A

72

- 個資清冊與風險評估表交付暨確認提醒：  
**111/05/13(五)前將「個人資料檔案清冊(含風險評估表)」上傳校務行政資訊系統。**
- 簡報完畢，謝謝聆聽

