



# 個人資料檔案盤點暨風險評鑑 教育訓練

2024.05.02

2024.05.08

# 大綱

2

- 執行個人資料管理制度的目的
- 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

# 執行個人資料管理制度的目的

# 執行個人資料管理制度的目的

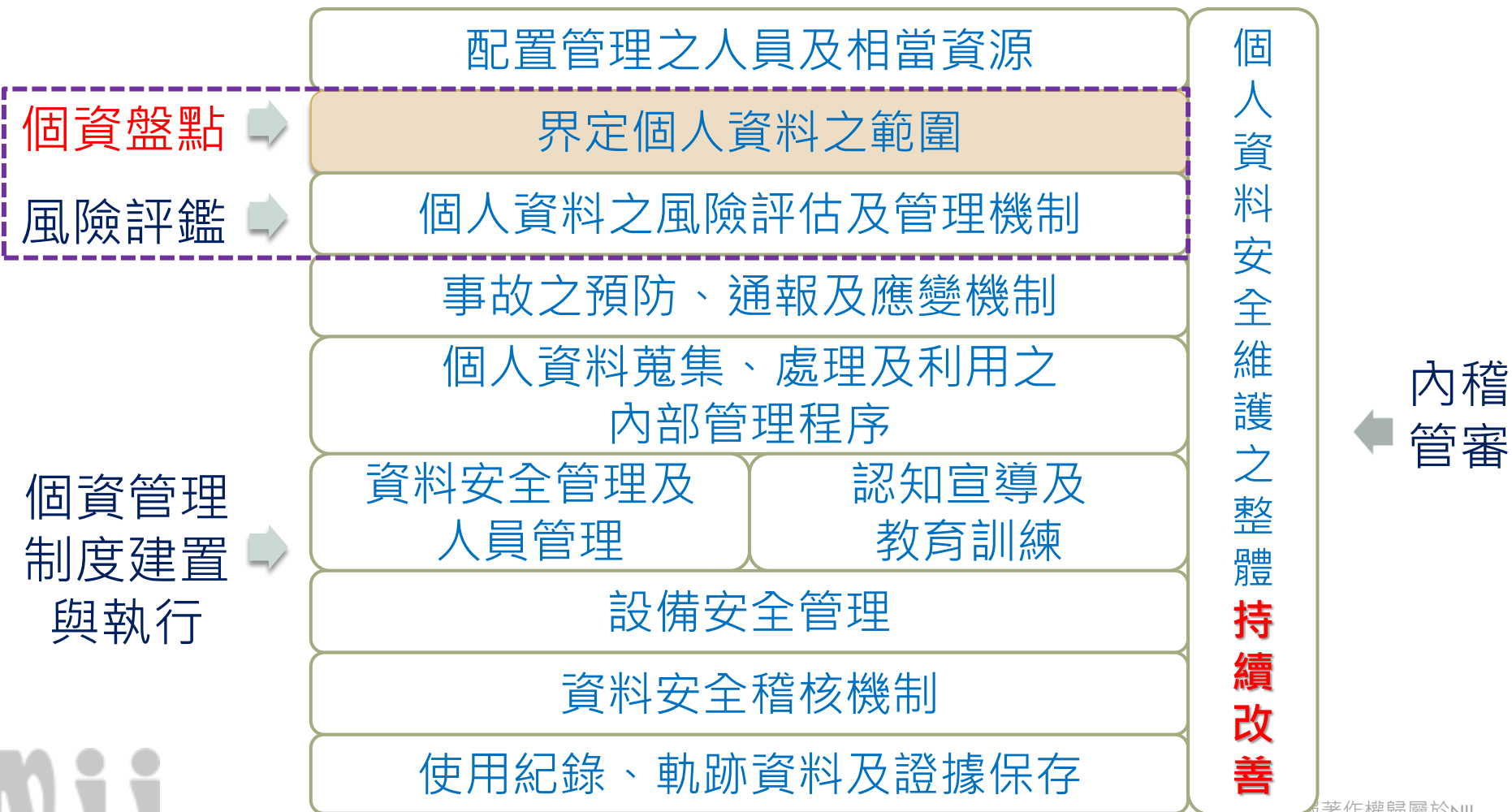
4

- 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。



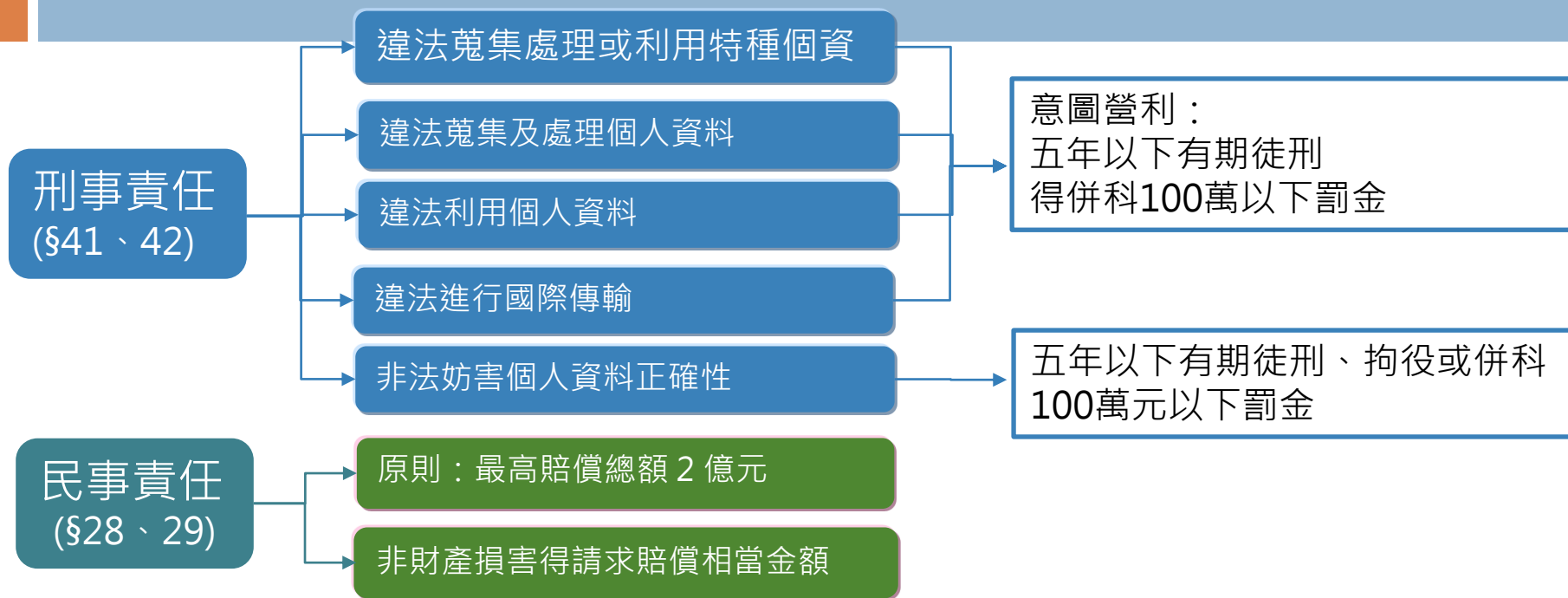
# 適當安全防護措施 (個資法施行細則§12)

5

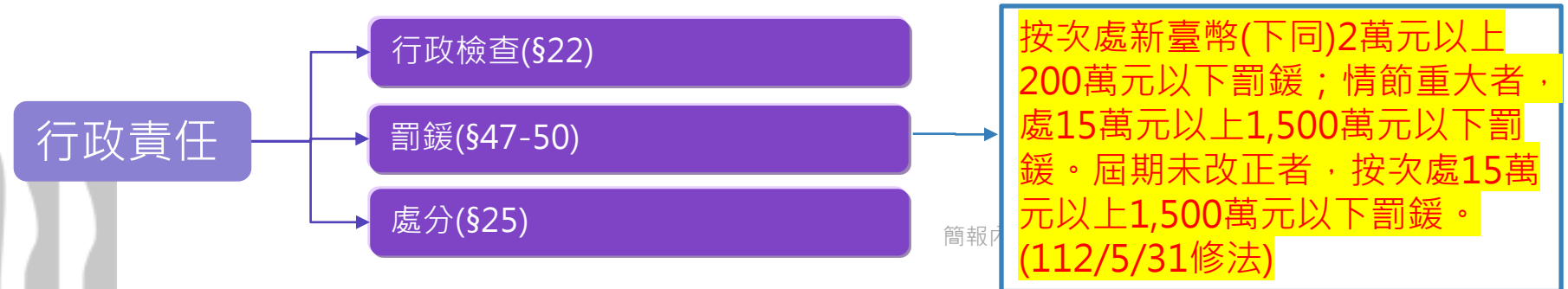


# 法律責任-非公務機關

6



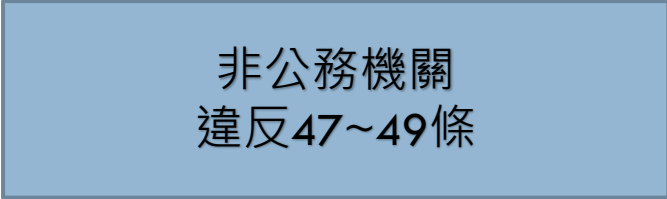
非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。(§29)



# 個資法罰則

7

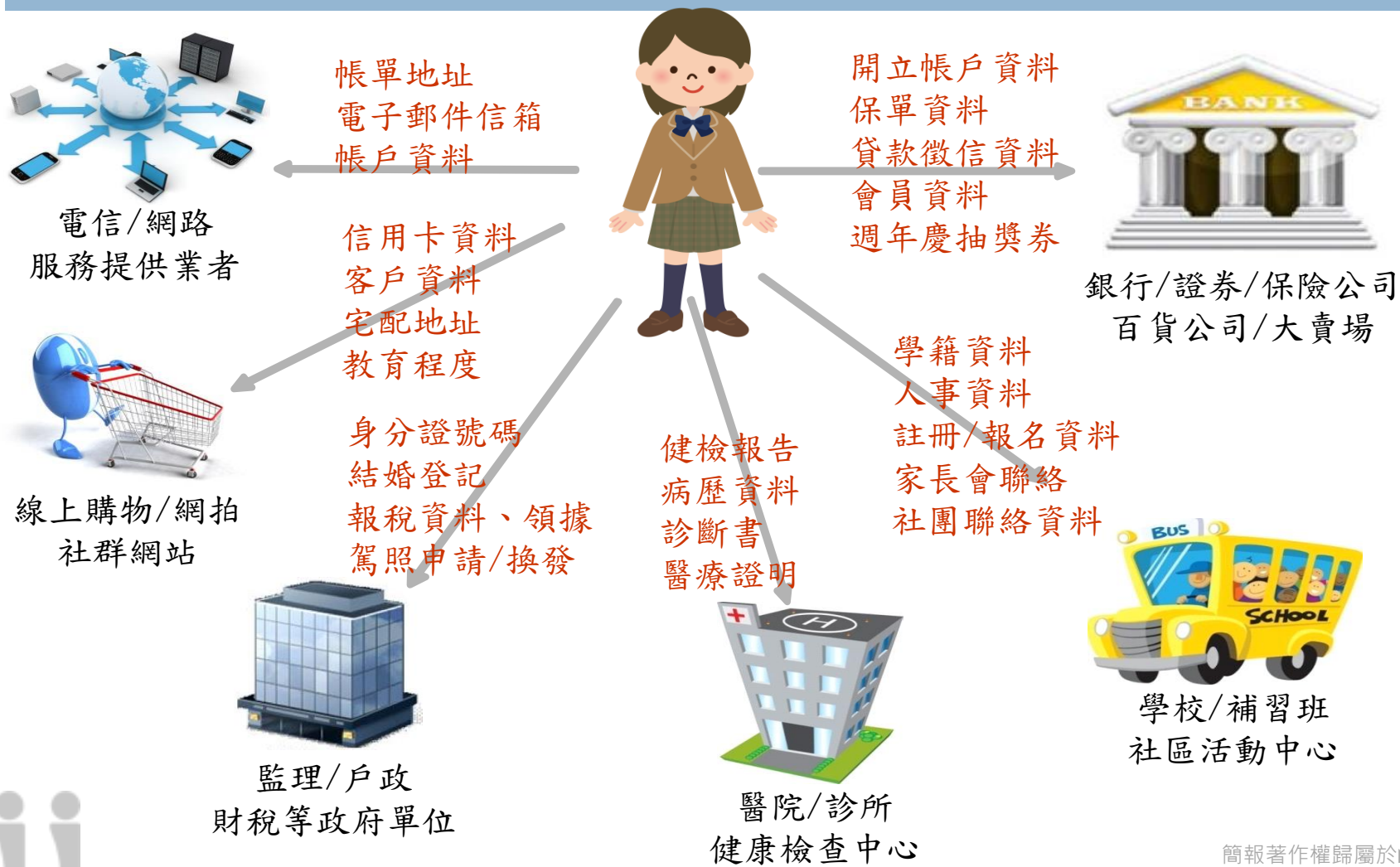
- 第 50 條
- 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。



非公務機關  
違反47~49條

# 個資.....在那裡？

8





# 可能的個資外洩管道

9

- ▶ 問卷、報名表 → 未妥善保護，造成個資外洩。
- ▶ 社群網站、網購 → 網站設計不良，導致APT、駭客攻擊，造成個資外洩。
- ▶ 內部人員、委外廠商 → 誤點釣魚網站，造成個資外洩。
- ▶ **人員 → 無個資保護認知**

# 華航今年又被駭！上百萬筆客戶個資流出 全被放上暗網出售

資料來源-聯合報 2024-03-26

10

駭客周日晚間在暗網放上華航會員資料，並宣稱這一次出售的會員資料為110萬筆，資料更新到2024年1月。華航會員也在近日收到重要通知，要求會員線上登入時，須透過手機或電子信箱接收一次性密碼（OTP），以提升資安安全性。

駭客這次在暗網上又放上110萬筆的華航會員資料，這一次被洩露的資訊，包含會員編號（ID）、中文名字、英文名字、性別、出生年月日、Email、國碼、手機號碼以及會員搭機的航空站。駭客也直接在暗網之中公開100名的華航會員資料內容細節。資安專家分析，造成個資外洩的原因很多，而且經常是一環扣著一環，駭客有可能是透過華航提供的服務系統入侵，也可能是透過社交郵件向華航的員工下手，透過這兩個管道進入華航內部環境，並取得機敏資料的權限和通道。



The image shows a screenshot of an email notification from China Airlines. At the top, it features the China Airlines logo and the text 'CHINA AIRLINES'. Below the logo, there are four small images of different airline loyalty cards. The main body of the email is in Chinese and reads: '親愛的會員 您好' (Dear member, hello). It then states: '為保障會員權益及資訊安全，自2024年4月2日起，華夏會員線上登入須透過手機或電子信箱接收一次性密碼(OTP)，同時取消社群登入機制；另，刪除會籍、新增/移除受讓人、網路酬賓獎項轉讓服務申請，以及酬賓獎項轉讓則無須再經OTP驗證流程。' (To protect member rights and information security, from April 2, 2024, China Airlines members logging in online must receive a one-time password (OTP) via mobile phone or email, and the social media login mechanism will be cancelled; additionally, account deletion, addition/removal of assignees, and online reward redemption service applications, as well as reward redemption, will no longer require OTP verification.) A red line of text follows: '\*\*\*提醒您\*\*\*再次至華夏會員專區確認或更新您的聯絡電話及電子信箱。' (\*\*\*Reminder\*\*\* Please confirm or update your contact phone number and email in the China Airlines member area again.) Below this, it says: '中華航空感謝您的支持與愛護，我們期待您再次搭乘中華航空，享受愉快的旅程。' (China Airlines thanks your support and love, we look forward to your next flight with China Airlines, enjoying a pleasant journey.) It then says: '祝福您 身體健康 萬事如意' (Wishing you good health and everything goes well) and '中華航空 敬上' (China Airlines, respectfully). At the bottom, there is a caption: '華航會員近日收到重要通知，要求會員線上登入時，須透過手機或電子信箱接收一次性密碼（OTP），以提升資安安全性。圖／擷取自華航會員重要通知函' (China Airlines members recently received an important notification, requiring members to receive a one-time password (OTP) via mobile phone or email when logging in online to enhance information security. Image taken from the China Airlines member important notification email.)

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

# 個資恐外洩...刑事局公布上季「高風險賣場」 健身、美容業都上榜

資料來源-聯合報 2024-01-18

11

警方統計，去年第四季「高風險賣場」前5名包含健身業「World Gym」218件、「健身工廠」134件、餐飲業「旭集」112件、電信業「台灣之星」106件、美容業「TKLAB」71件，相關賣場恐有個資外洩問題，常見詐團運用消費者個資假冒電商客服行騙民眾。

警方呼籲，民眾看見來電顯示開頭帶「+」號、「+21」、「+67」或「+87」等「境外」來電號碼，卻自稱「國內」電商或銀行業者，於通話過程聽到「解除分期付款設定」、「重複扣款」、「升級VIP」及「賣場認證」等關鍵字要求操作ATM、網路匯款時，請提高警覺，掛斷電話自行聯繫電商業者求證；必要時，可撥打165反詐騙諮詢專線協助。

## 112年第四季民眾通報高風險業者(賣場)排名

高風險業者(賣場)通報排名
World Gym : 218件
健身工廠 : 134件
旭集 : 112件
台灣之星 : 106件
TKLAB : 71件



簡報內容僅供參考，並非任何法律意見，請斟酌使用簡報

# 個資外洩遭詐騙！她告贏溫泉酒店 消基會：鼓舞民眾力爭權益

資料來源-ETtoday新聞雲 2024-02-17

12

消基會表示，去年1月中旬接獲趙姓消費者申訴，110年11月，透過北投麗禧溫泉酒店官網訂購溫泉券22張，花費數萬元，**訂購時填載姓名、電話、電子郵件、中信銀行刷卡帳號**等個人資料。之後因個資外洩遭訛詐近十萬元。北投麗禧酒店及建置系統的墨攻網路科技公司一再堅稱在安全防護措施上無過失，主張不用賠償，消費者一怒下狀告法院。

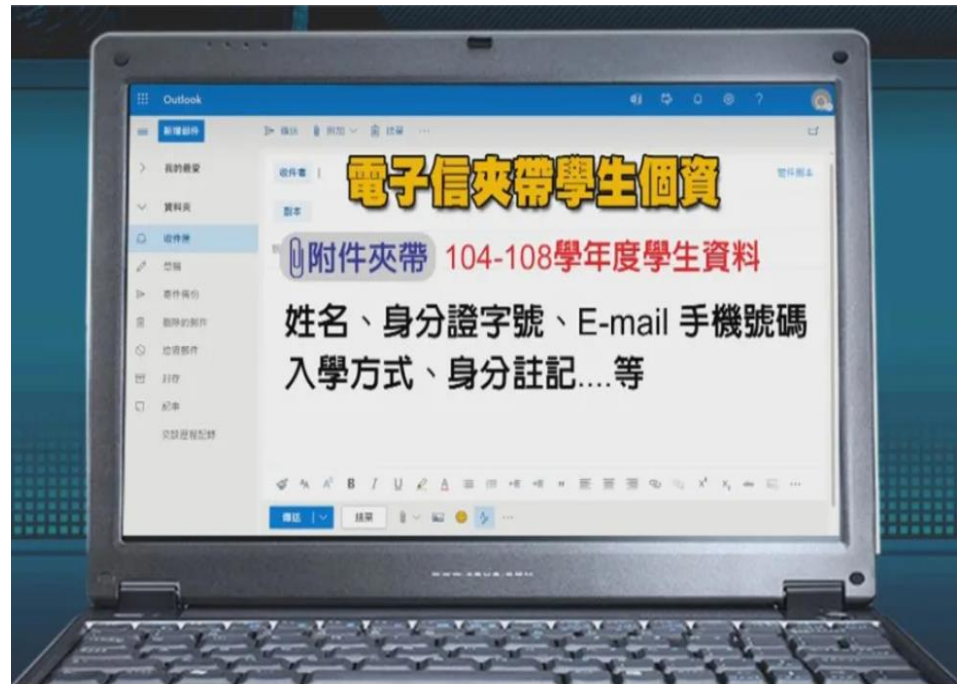
審理結論認定墨攻公司**無法證明就其管理維護的系爭訂購系統所保有消費者的個資，已盡採取適當安全措施責任**，並認定麗禧公司**無法證明消費者的個資遭外洩前，有適當監督墨攻公司管理維護系爭訂購系統行為**，故**判定麗禧公司、墨攻公司有過失**，均需對消費者個資的外洩負損害賠償責任，消費者可向業者請求賠償2萬元。



▲不少民眾因個資外洩遭到詐騙，消基會指出，趙女成功向廠商求償，是小蝦米力抗大鯨魚。(示意圖/ETtoday)

[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。



外洩筆數8,495筆，以每筆500元估算，合計4佰2拾4萬7千5百元!!!

# 正確面對「個資法」

14

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

15

# 個人資料的定義

# 何謂個人資料 (個資法§2、§6)

16

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

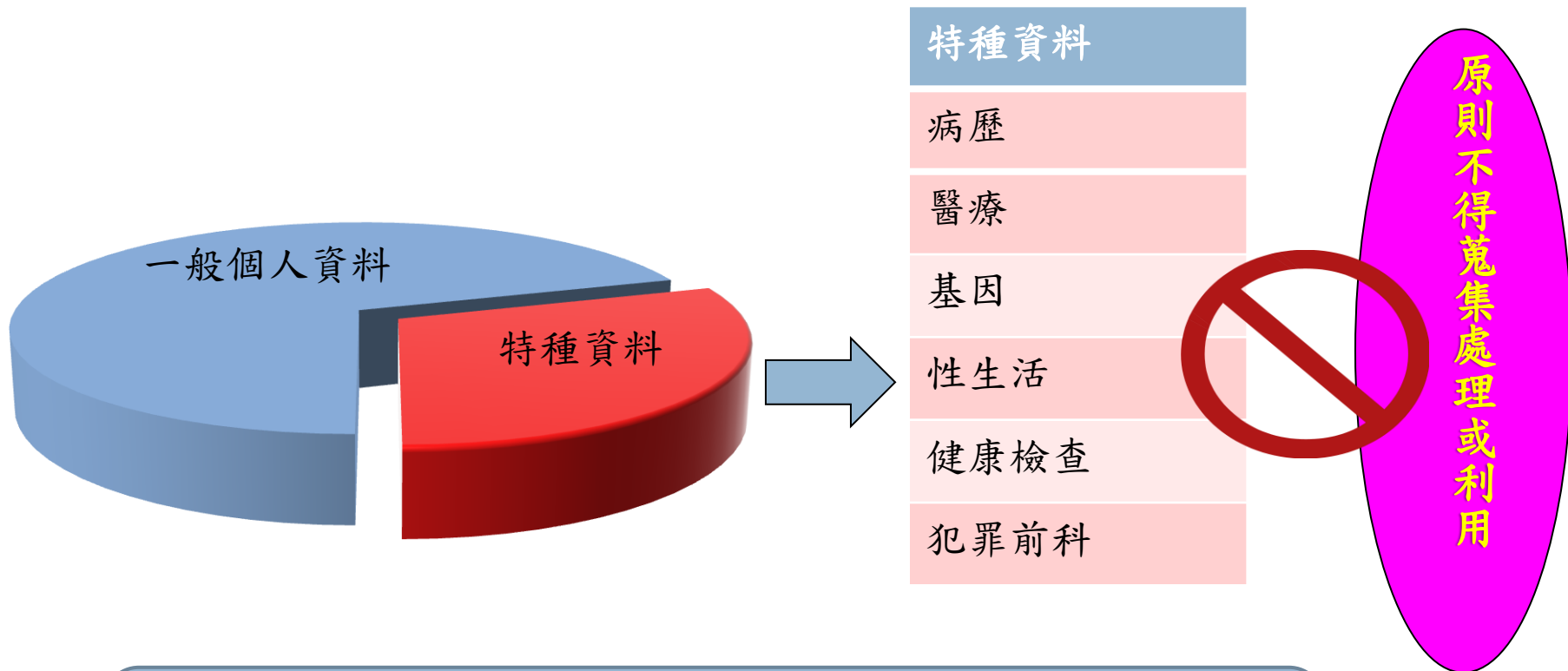
其他  
資料

- 得以直接或間接方式識別該個人之資料



# 特種資料

17



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)

# 特種個資 (個資法第6條/個資法施行細則第4條)

18

醫療法第10條所稱醫事人員，係指領有中央主管機關核發之**醫師、藥師、護理師**、物理治療師、職能治療師、醫事檢驗師、醫事放射師、營養師、助產師、**臨床心理師、諮商心理師**、呼吸治療師、語言治療師、聽力師、牙體技術師、驗光師、藥劑生、護士、助產士、物理治療生、職能治療生、醫事檢驗生、醫事放射士、牙體技術生、驗光生及其他醫事專門職業證書之人員。

類別	特種個資之意涵(細則)
病歷	醫療法第67條2項 病歷，應包括下列各款之資料： 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
醫療	指病歷及其他由醫師或其他之 <b>醫事人員</b> ，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 <b>診察及治療</b> ；或基於以上之診察結果，所為 <b>處方、用藥、施術或處置</b> 所產生之個人資料。
基因	由人體一段去氧核糖核酸構成，為人體控制特定功能之遺傳單位訊息。
性生活	指性取向或性慣行之個人資料。
健康檢查	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。
犯罪前科	指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

# 特種資料得蒐集、利用或處理之例外情況

19

□ 法律明文規定。

學校衛生法第8條第1項，學校應建立學生健康管理制度，定期辦理學生健康檢查。

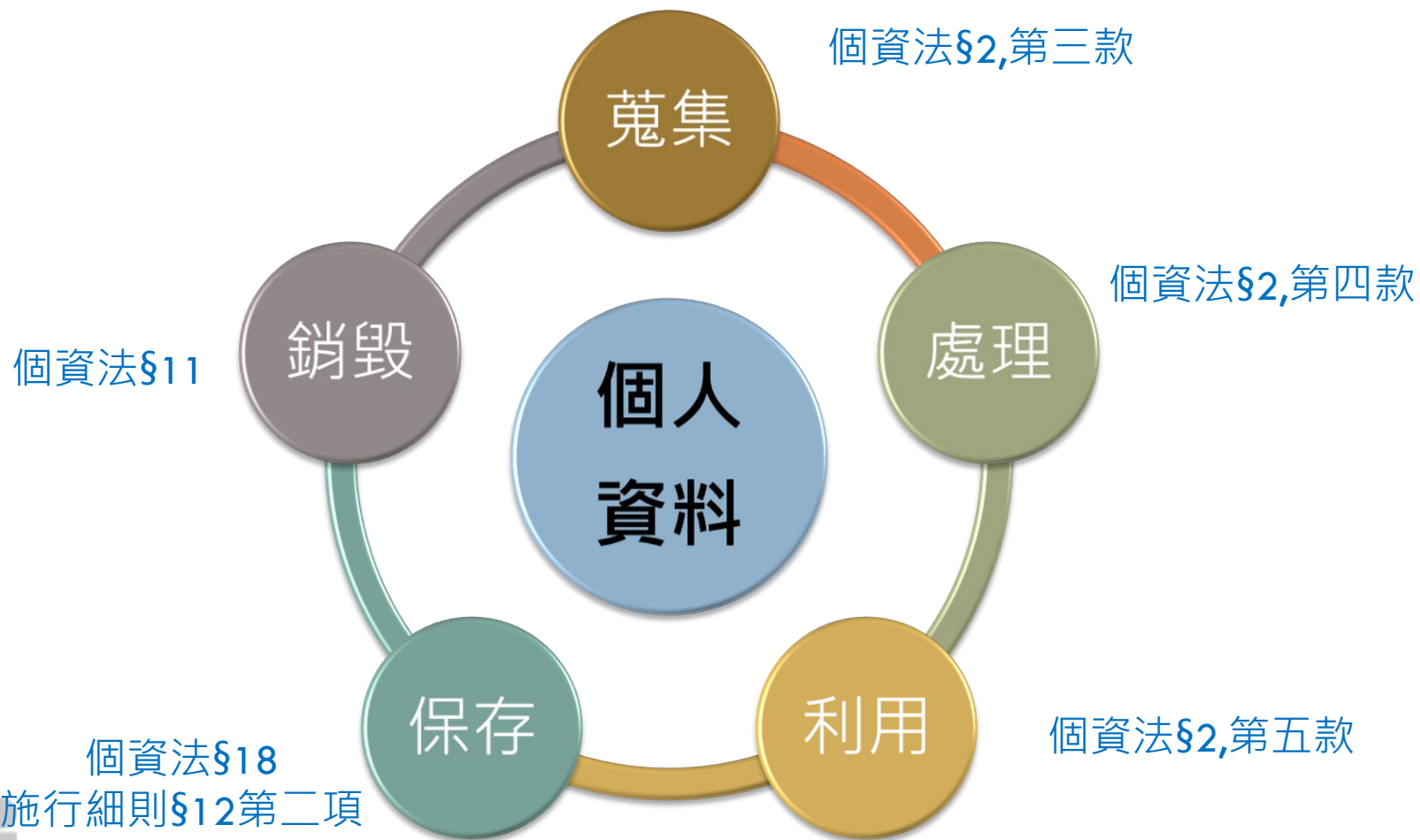
□ 公務機關執行法定職務或非公務機關執行法定義務所必要，且有適當安全維護措施。

□ 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。

# 個人資料生命週期

20



21

# 個資盤點實作說明

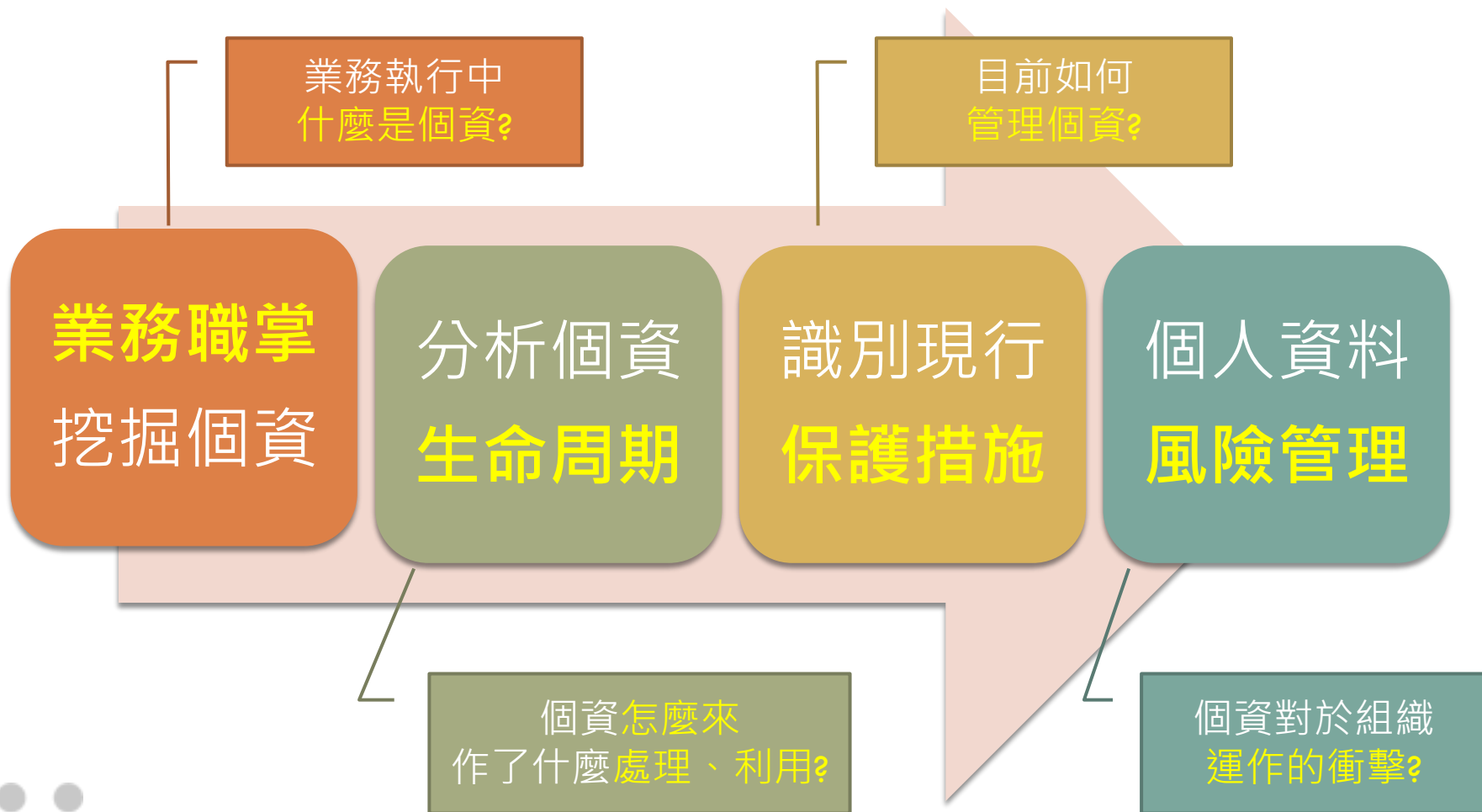
# 個資盤點注意事項

22

- 每年應至少執行一次個資檔案鑑別作業
- 得因應變動情況，調整個資清冊
  - 組織異動或作業流程改變
    - 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

23



# 個資盤點群組化觀念

- 相同屬性之紙本文件、電子檔案，且其生命週期(蒐集、處理、利用、儲存、銷毀...)活動均相同者，可將之群組化，列為同一筆個資資產

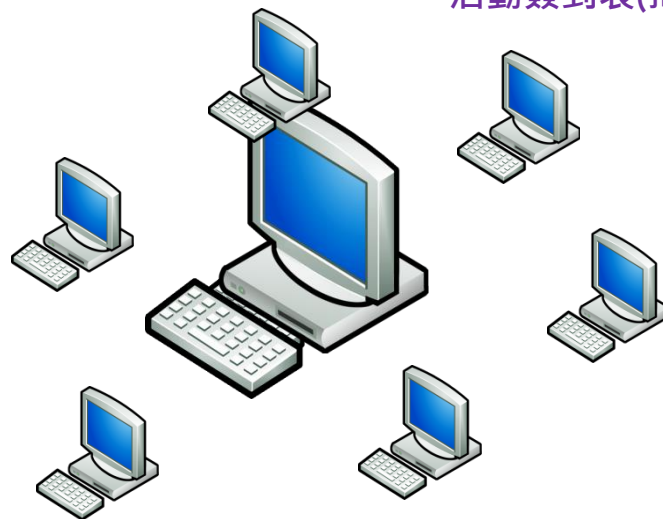
工讀生  
基本資  
料表



工讀生簽到表

服務時數統計表

活動簽到表(掃描)



活動報名清冊



# 個人資料檔案清冊說明

25

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)

26

- 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



# 個人資料檔案資料類型

27



紙本文件  
(Document)

- 以紙本形式存在之文書資料，包含公文、報表、表單、計畫書、合約、外來文件等

電子檔案  
(Data)

- 儲存於系統、硬碟、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔

同一個資檔案，同時  
存在紙本/電子形式，  
應**分開盤點**

# 個人資料範圍\_蒐集欄位

28

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
護照號碼	護照號碼 或 居留證號碼
特徵	年齡、性別、出生年月日、出生地、國籍、聲音、身高、體重、血型
指紋	指紋
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、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、E-mail、戶籍住址、住家住址、公司住址
財務情況	金融帳號、薪資
社會活動	旅行及其他遷徙細節、休閒活動及興趣

# 個資數量

29

## □ 每年

- ▣ 年度蒐集約略數量

## □ 總量

- ▣ 單位保存約略總數量

## □ 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

30



## 法律明文規定

EX. 大學法、學生輔導法、學校衛生法、勞基法、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

31

- 法務部於101/10/01修正公布
  - ▣ 182項特定目的；134項個人資料類別

國家發展委員會  
NATIONAL DEVELOPMENT COUNCIL

主管法規查詢系統  
Laws and Regulations Retrieving System

請輸入關鍵字 整合查詢

最新訊息 法規體系 法規檢索 草案預告 相關網站

現在位置：法規內容 友善列印

法規內容

法規名稱：	個人資料保護法之特定目的及個人資料之類別 <b>英</b>
公發布日：	民國 101 年 10 月 01 日
發文字號：	法務部法令字第10103107600號令會銜各中央目的事業主管機關修正發布
法規體系：	個人資料保護類
圖表附件：	<a href="#">立法總說明.pdf</a> <a href="#">條文對照表.pdf</a>

法規內容 條文檢索

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

# 列舉-個人資料保護法之特定目的

32

## 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

33

## □ 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

34

- 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

# 個人資料檔案清冊說明

35

業務職掌  
挖掘個資



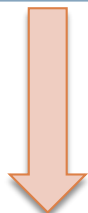
分析個資  
生命周期



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、處理或利用之定義

36

## 蒐集

- 指以任何方式取得個人資料。

## 處理

- 指為建立或利用個人資料檔案（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。）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

- 指將蒐集之個人資料為處理以外之使用。

# 蒐集

37

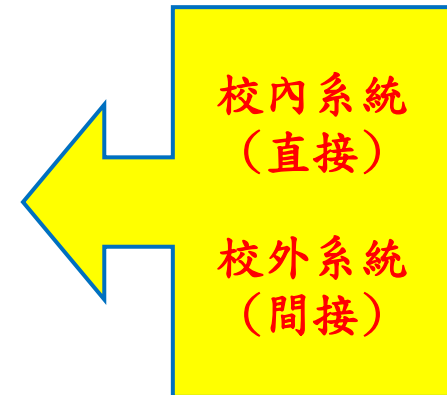
## □ 蒐集來源

- 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

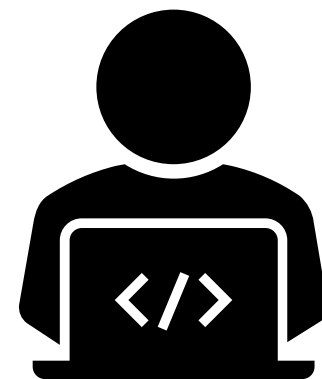
## □ 蒐集單位：對當事人蒐集之源頭單位



# 處理

38

- 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

39

- 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(以P.30「保有依據」為判斷基準)：
  - ▣ 法律 > 辦法 > 內規
  - ▣ 保存N年
  - ▣ 離職後保存N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

40

- 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

41

- 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

42

- 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

43

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						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

44



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.....

明確描述  
系統名稱

# 個人資料檔案清冊說明

45

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)

46

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

47

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

48



**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

49

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	各系辦	各系辦	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

50

## ◆ 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)

- 學校官網查詢到之同仁姓名、單位、分機等資訊不需列入個資清冊(**公開資訊不需列入盤點**)。
- 將校外系統列為盤點標的(個人資料檔案名稱)(**校外系統本校無資料之控制權**)。
- 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**。

# 個資盤點清冊諮詢常見問題(2/2)

- 保有依據不適切。(法律>執行法定職務或履行法定義務>當事人同意)。
- 不清楚特種個資之定義。(特種個資：病歷、醫療、基因、性生活、健康檢查及犯罪前科)
- 因未定義保存期限，所以目前資料都永久保存(應參考法令法規或內部規定，訂定適切之保存期限)。
- 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)。

# 個人資料盤點自我檢查步驟

53

Step1

- 確認**業務範圍**，清點所有個人資料

Step2

- 清查**蒐集**個人資料之**途徑與方式**

Step3

- 確認是否**須履行告知義務**並建立告知機制 (個資法§8)

Step4

- 確認**蒐集、處理、利用**之特定目的與保有依據

Step5

- 檢視**保存與利用**之範圍與方式

Step6

- 確認個人資料的**保存期限與銷毀方式**

54

# 風險評鑑作業說明

# 風險管理所帶來的效益

55

- 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



# 個資盤點及風險管理關聯(1/2)

56





# 個資盤點及風險管理關聯(2/2)

57

業務職掌  
挖掘個資



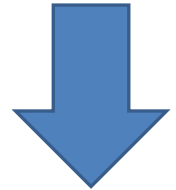
分析個資  
生命周期



識別現行  
保護措施



個人資料  
風險管理



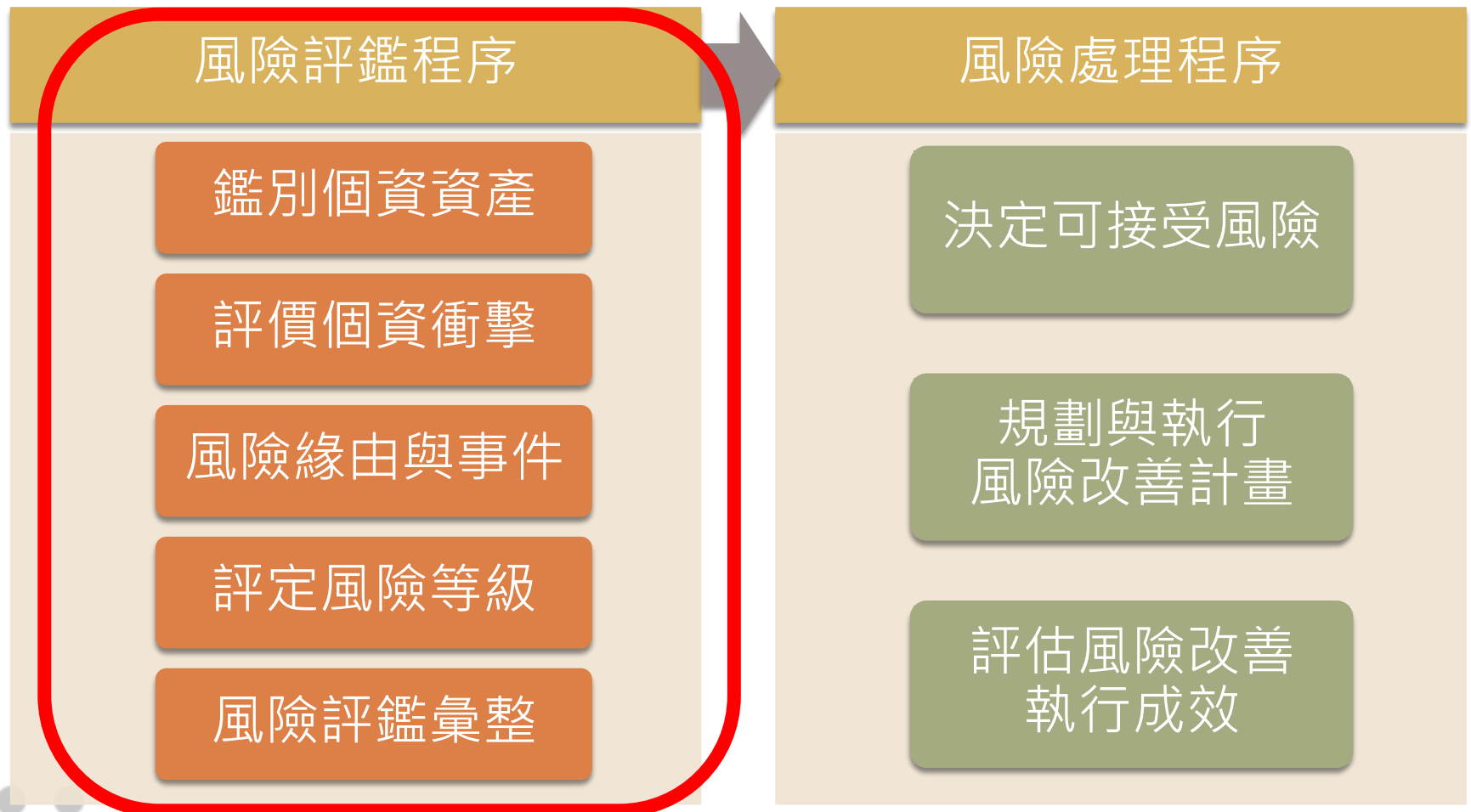
流程名稱	個人資料檔案名稱	資料類型	個人資料範圍	數量	保有依據	特定目的	個人資料類別	特種資料	蒐集			處理					利用					現有控制措施	個人資料範圍評估	檔案管理角色	
									來源	方式	單位	處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式				揭露對象



# 隱私衝擊分析(個資範圍評估值)

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。

# 風險評鑑與風險處理管理流程



# 風險評鑑工具

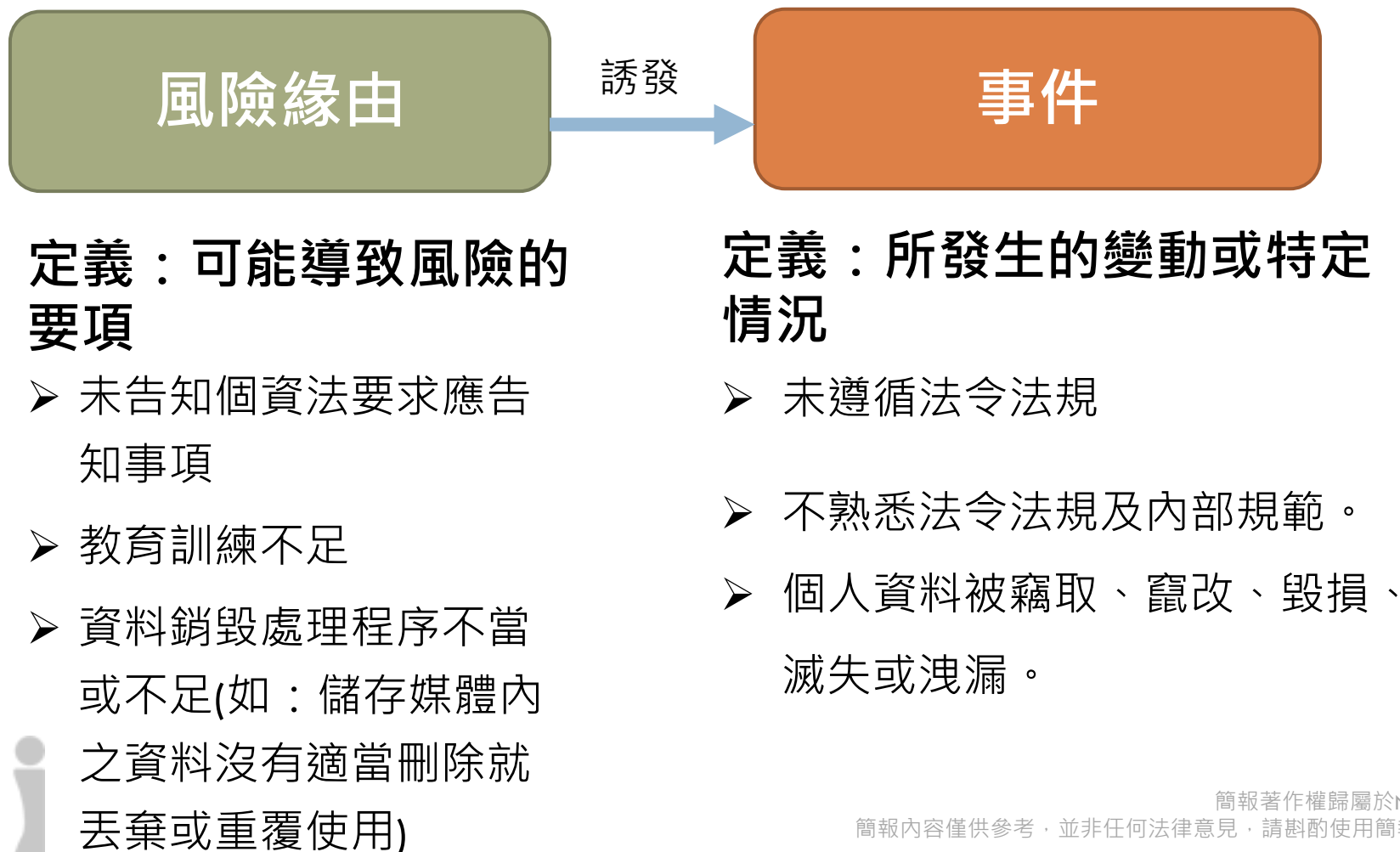
60

## FO-PIMS-2-03-02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

61



# 風險評估分析構面表-1-1

62

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

63

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

64

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

65

評估值	可能性	
4	該風險常導致此事件發生	<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	該風險曾導致此事件發生	<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	該風險可能導致此事件發生	<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	該風險導致此事件發生的機會極低	<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

66

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

67

□ 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

# 風險評估作業注意事項(1/2)

- 個資清冊欄位「個資資產編號」與「工作表名稱」不一致：

個資 資產編號	受訪單位
多媒體與遊戲發展系 001	多遊系
▶ 個人資料檔案清冊	多遊系-001   多遊系-002

- 風險值計算未套用公式：風險值 = 個資範圍評估值 X  
(衝擊影響 + 可能性)

# 風險評估作業注意事項(2/2)

- 風險值評分漏列，有利用行為(如聯絡當事人)，未評分或評分為不適用：

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
利用	未經授權下利用資料	個人資料被竊取、竄改、毀損、滅失或洩漏			0	0
利用	存取權限授與不當	個人資料被竊取、竄改、毀損、滅失或洩漏			0	0
利用	缺乏回收控管機制	個人資料被竊取、竄改、毀損、滅失或洩漏				0
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				0
利用	不了解個資法國際傳輸之要求	個人資料被竊取、竄改、毀損、滅失或洩漏				0

# 風險評估範例

70

## 學生保險清冊

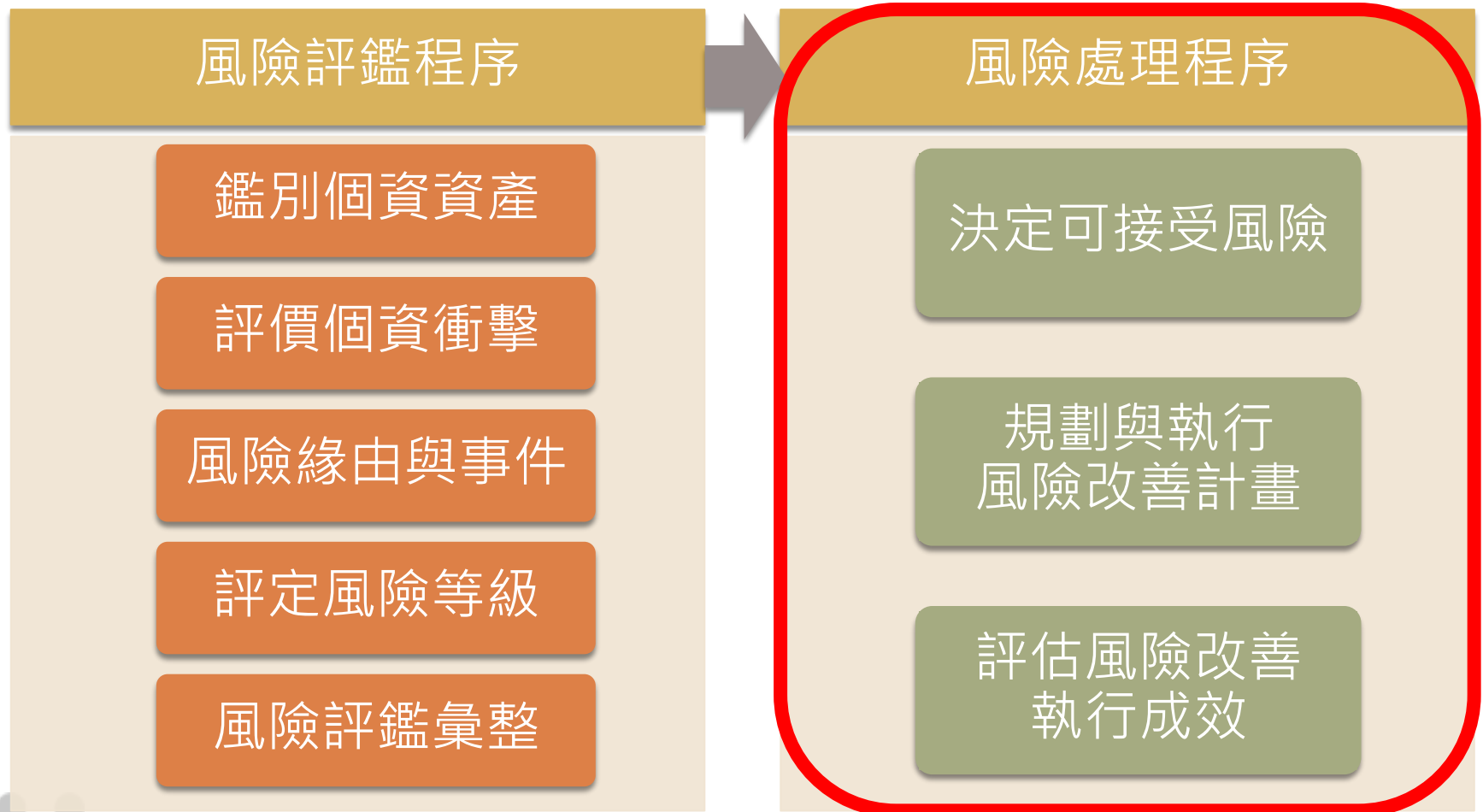
- 個資範圍評估值=3

## 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管理流程



# 風險控管原則

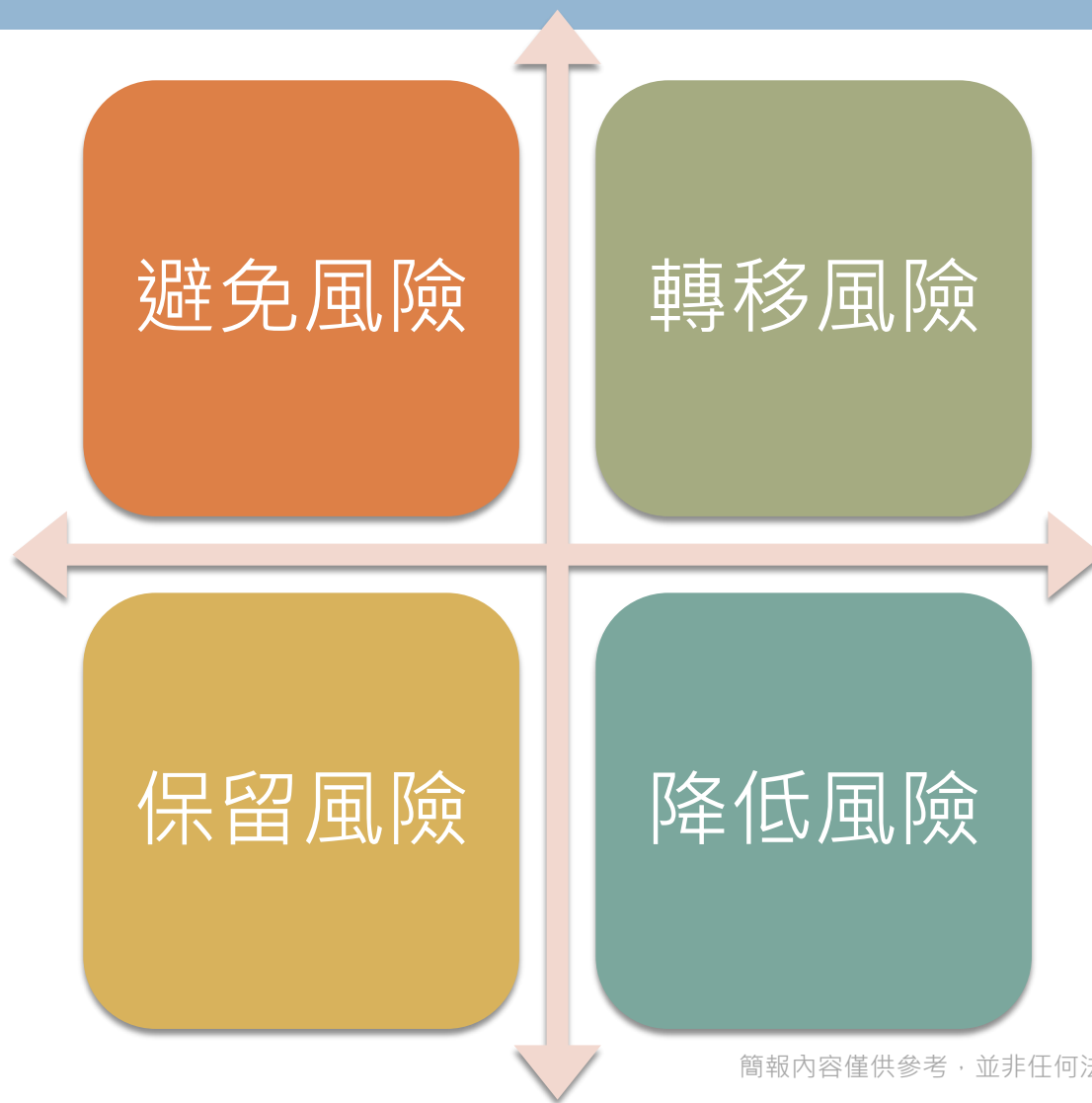
72

- 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

## □ 個人資料檔案風險處理計畫

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

78

## □ 追蹤處理現況

- 建立評量指標(例如：KPI指標)，協助控制目標達成
- 執行內部稽核，確保控制措施的有效性

## □ 除每年執行一次外，當有下列情況時，應執行風險評鑑作業

- 營運組織變更
- 作業流程改變
- 個人資料檔案新增或變更
- 發生個資安全事件



# 專案時程提醒：

79

- 「個人資料檔案清冊(含風險評估表)」上傳校務行政資訊系統：**5/17(五)前**
- 內部稽核：8/21(三)、8/22(四)
- 外部稽核：11/28(四)、11/29(五)



# Q & A

80

□ 簡報完畢，謝謝聆聽



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