國立中興大學
National Chung Hsing University

個人資料盤點教育訓練

講師：NII產業發展協進會 專業講師群

財團法人中華民國國家資訊基本建設產業發展協進會

目錄

- 個人資料流之重要性
- 個資法對蒐集階段之限制
- 資訊資產分類原則
- 建立個資資產清冊
- 個資衝擊分析

個人資料流之重要性

◆個人資料範圍

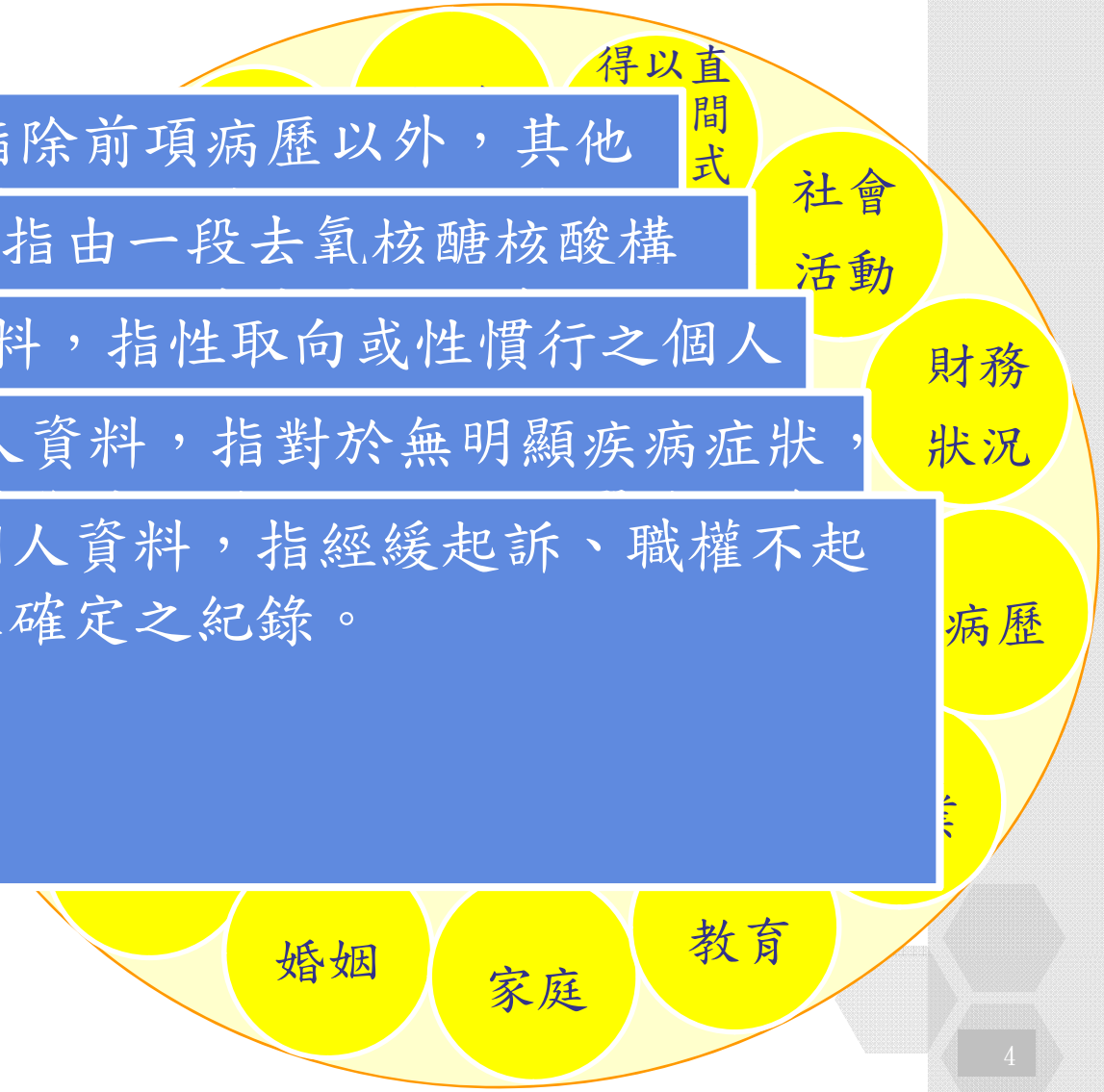
所稱醫療之個人資料，指除前項病歷以外，其他

所稱基因之個人資料，指由一段去氧核醣核酸構

所稱性生活之個人資料，指性取向或性慣行之個人

所稱健康檢查之個人資料，指對於無明顯疾病症狀，

所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定之紀錄。



醫
活、
罪前
財務
動及其他得以直接或間接方式識別該個人之資料。

個人資料流之重要性

個人資料無所不在

訂單、托運資料

金融帳號、財務狀況

學生學籍資料、成績、教職員資料

金融

商業行銷

育教

檢健療醫

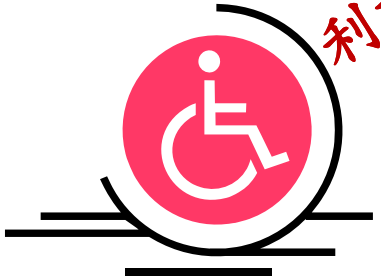
通訊、網路

病歷、健康檢查記錄

電信帳單、網路會員資料

利福會社

戶政地政

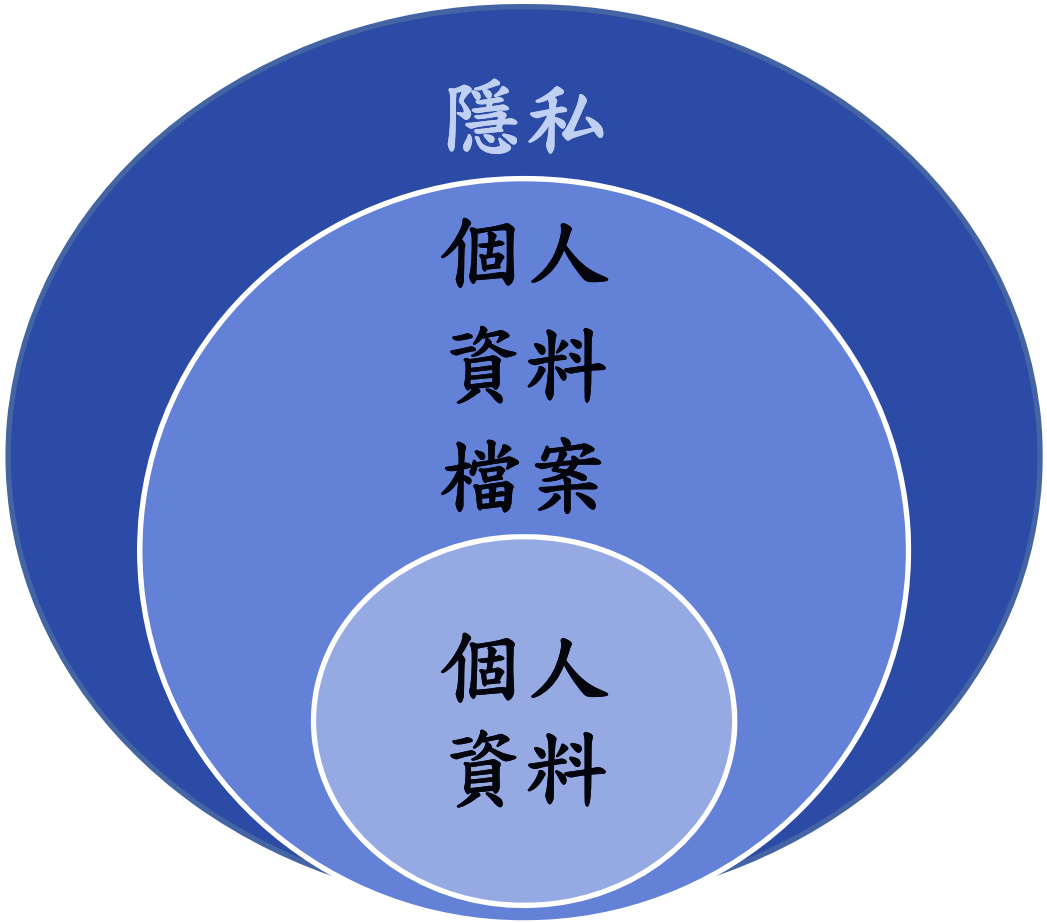


身心障礙別、醫療證明

戶政資料、地政資料財產狀況

個人資料流之重要性

- 隱私權與個人資料的關係



個人資料流之重要性

◆隱私權與個人資料的關係：

軌跡資料係指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（LOG FILES），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑…等，可用於比對、查證資料存取之適當性。因此，為符合本法個人資料保護與個人資料合理利用之立法意旨，個人資料檔案除備份檔案之外，亦應包括軌跡資料在內，爰增訂如上。

個人資料　・足以識別該個人之資料

個人資料流之重要性

- 隱私對組織而言是風險管理的議題，因個資外洩引起的威脅包括調查和訴訟、負面宣傳、運營中斷、計劃外預算的影響以及對企業信任產生懷疑。

- 企業/組織在個人資料保護的策略層應建立一個基於風險管理的資料保護策略方法，而非僅依賴周邊的安全。也就是將個人資料的安全保護直接加在資料本身。

個人資料流之重要性

- 前不久爆發的少將洩密案，政府的補救措施，除了徹底清查洩密案所帶來的損失外，還要追查資料外洩流向，調查該名少將在任職內還看過哪些檔案？以及這些機密檔案曾被哪些人閱覽過，是否還潛在著資料外洩的風險，或是有沒有任何管理流程上的漏洞。

- 唯有描繪出完整資料流，才能從中找出缺失及防堵方式，避免日後相同情況再度上演。

個人資料流之重要性

- **發生資料外洩後，第一件要做的就是描繪出完整的資料流向。**
  - 瞭解這份檔案日常的使用者、維護者及檔案使用狀況；
  - 清查檔案曾經被哪些員工閱覽過，這些員工又看過哪些其他的檔案；
  - 追查除了外洩檔案外，洩密者還看過哪些檔案。

個人資料流之重要性

- 描述和分析組織目前的業務流程架構，基本上，任何的業務活動都會牽涉到資訊的管理，並且包括四項元素，分別為：資訊收集、交易流程、交易結果和以上三者所留下的記錄。

個人資料流之重要性

- 在資料流分析過程中，至少要識別出業務流程主要的元件，如人員、設備及個人資料處理過程使用之相關紙本化表單或自動化方式等，以及個人資料如何透過業務流程被蒐集、處理、利用、揭露和保存，建議以清楚易懂的方式來呈現彼此的關聯(如圖形或簡易的表格方式)。

- 個人資料流之重要性
- **個資法對蒐集階段之限制**
- 資訊資產分類原則
- 建立個資資產清冊
- 個資衝擊分析

個資法草案通過，引起一陣恐慌

可能觸犯個資法的行為

事實	後果
將大甲媽祖遶境的照片，貼在個人部落格	入鏡的路人如果不同意被蒐集照片，都可提告求償
維基百科記錄個人教育、職業、婚姻等情形	如未取得當事人同意，都可能挨告
在Facebook上張貼同學會的照片	若未取得所有同學的同意，有觸法之虞
用群組式寄發電子郵件，顯露所有人的帳號	當事人必須同意，才能新增對方的聯絡資料，否則可能挨告求償
在MSN上詢問他人電話和個人資料	如未取得當事人同意，可能被視為非法蒐集
選舉期間提出競選對手的犯罪前科	對方可依個資法提告
媒體報導政治人物的密帳、婚外情、性傾向	必須先取得當事人同意才能公開報導
民代公布官員有雙重國籍或國外社會安全碼	要當事人同意才能公布

製表／蕭白雪

聯合報

來源：**2010.4.23**聯合報

99.4.27立法院復議後，三讀通過個資法

◆修正第9、19、20、51條

- 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料，不用告知。
- 非公務機關使用或處理個人資料，與公共利益有關，或個人資料取自一般可來源，且使用該資料有比保護資料更大利益。
- 單純的個人或家庭活動，及在公開場所和公開活動中，所蒐集、處理或利用之影音資料。

個人資料保護法之修法重點

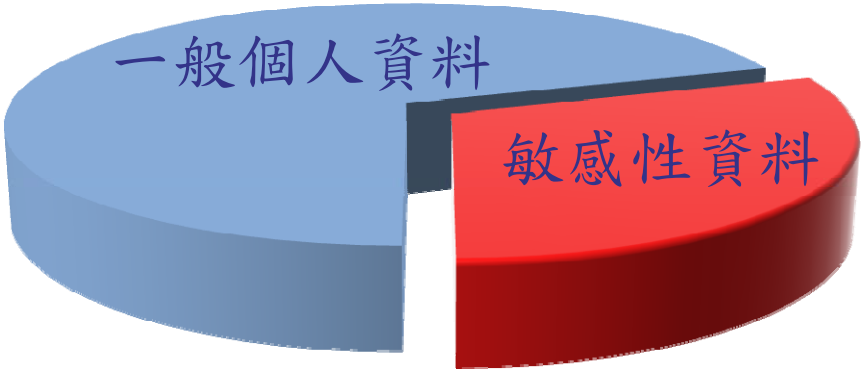
擴大適用主體	擴大保護客體	擴大適用地區	增加程序規定
• 適用所有行業機關及個人	• 包括人工處理資料 • 增加個人敏感性資料	• 在中華民國境外對中華民國人民個人資料蒐集、處理或適用亦有本法之適用	• 增加告知義務 • 直接蒐集 • 間接蒐集 • 特定目的外使用另行告知

排除個人或家庭活動，及公開場所或活動之影音資料

施行日起
一年內完成告知

個人資料保護法相關規定

◆確定蒐集客體



特種資料

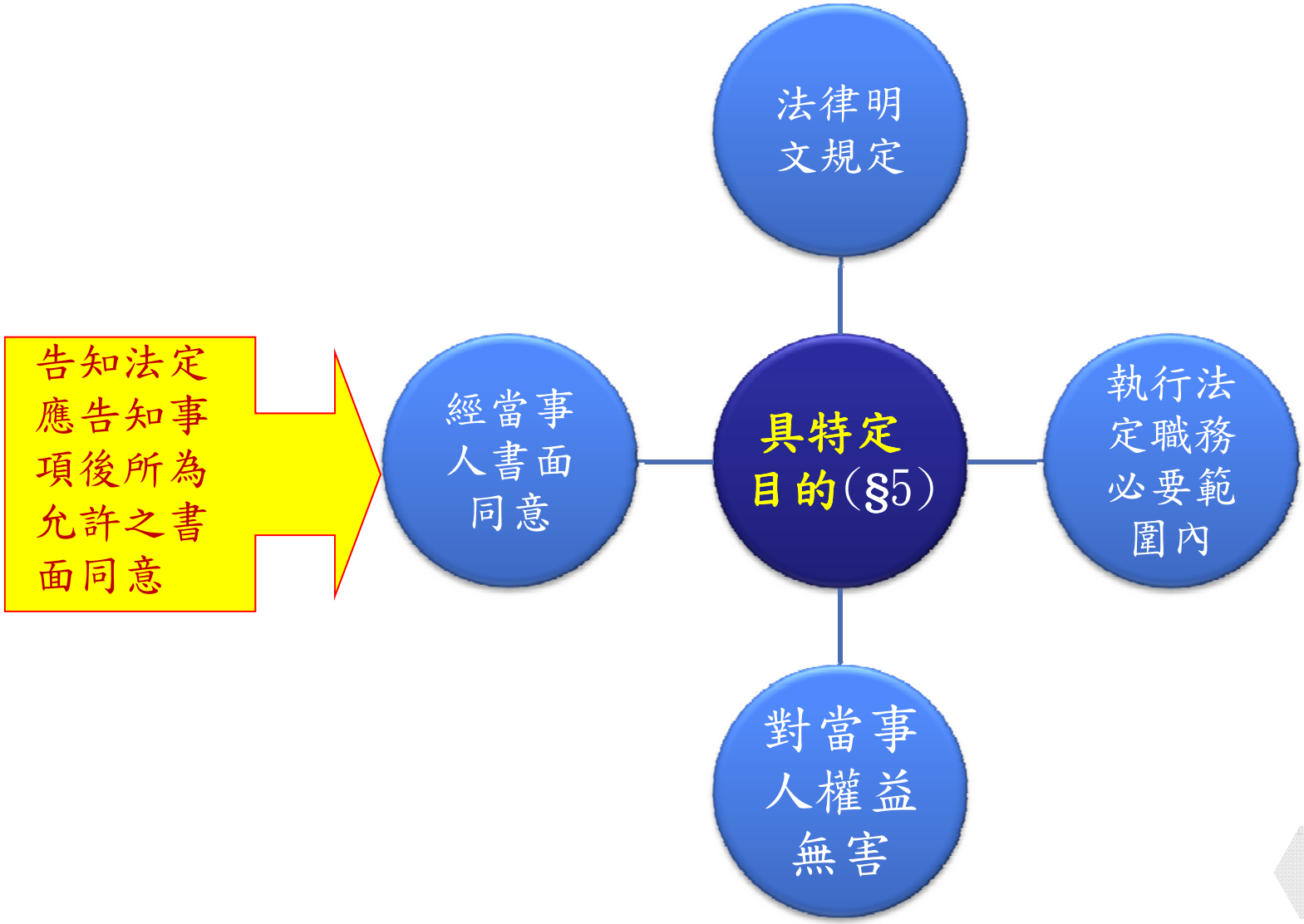
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

原則不得蒐集處理或利用

得蒐集、利用或處理敏感性資料之例外情況

- 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、利用或處理

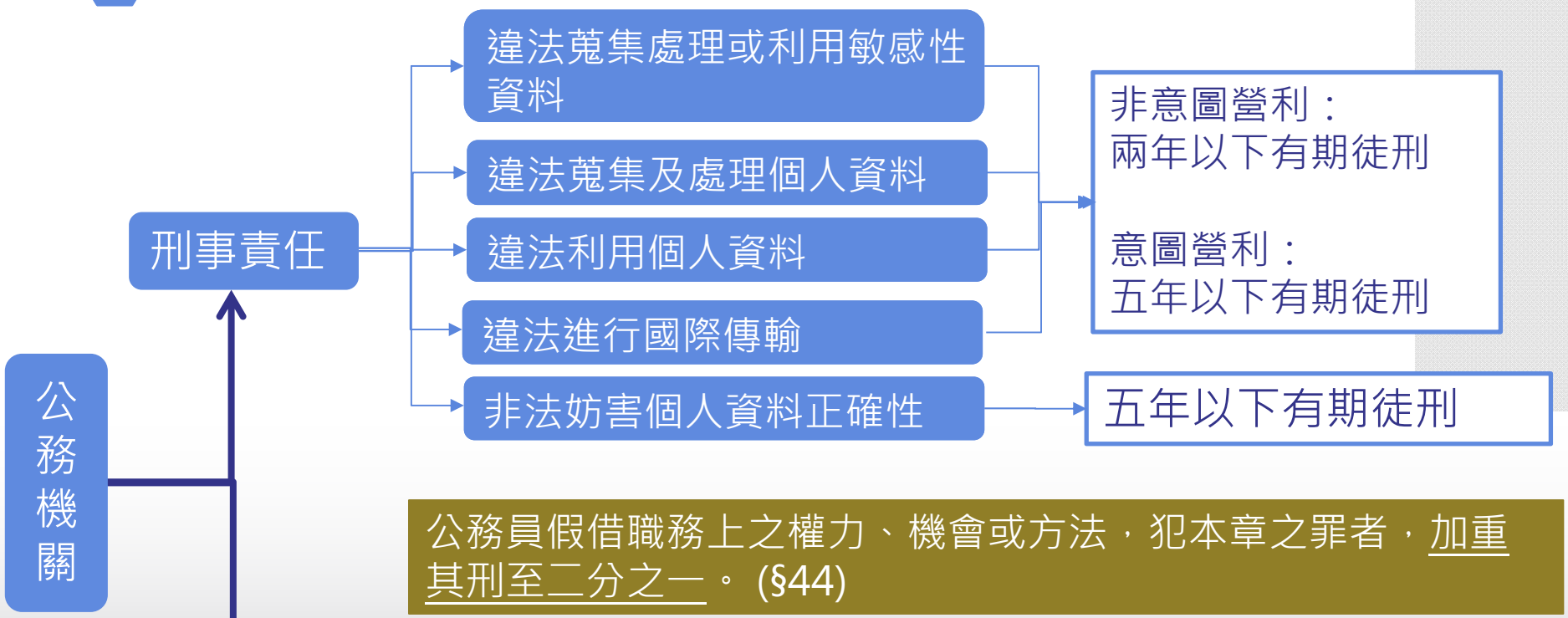
公務機關得蒐集資料之情況(§15)



維護個人資料正確性之義務

- 維護個人資料正確性，主動或依當事人請求更正或補充正確性有爭議時，應主動或依當事人之請求停止處理或利用
  - 因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。
- 當事人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料
  - 因執行職務或業務所必須或經當事人書面同意者，不在此限。
- 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料
- 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象

公務機關(公立學校)之法律責任



公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)

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。(§28)

個人資料體檢步驟一：清點個人資料

- 有沒有符合個資法定義的個人資料？
  - 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。
- 有沒有特種個人資料？
  - 醫療、基因、性生活、健康檢查、犯罪前科。

個人資料體檢步驟一：清點個人資料

◆有沒有下列不受個資法保護的資料？

- 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，如納 入個資法適用，恐造成民眾之不便亦無必要。
- 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。為解決合照或其他在合理範圍內之影音資料須經其他當事人書面同意始得蒐集、處理或利用之不便，且合照當事人彼此間均有同意之表示，其本身共同使用之合法目的亦相當清楚，因此排除個資法對上述影音資料的適用，回歸民法規定。

個人資料體檢步驟一：清點個人資料

◆電子郵件

- 機關將收集他人電子郵遞住址（E-MAIL）資料提供他人查詢服務，如其並未與自然人之姓名等相結合，尚不足以識別該個人者，則該資料即非上開規定所稱之個人資料，並無電腦處理個人資料保護法規定之適用。

（法務部94年05月06日法律決字第0940017397號）

個人資料體檢步驟一：清點個人資料

◆電話號碼

- 電話門號如未與申請人或使用人之姓名作連結，該門號僅係電話通訊線路之識別代碼，尚不足資識別該自然人為何人時，自不屬本法所稱之個人資料。
- 另如該電話門號係由公司或法人名義申請，由於非屬自然人之個人資料，則根本與本法無涉。
- 如電信公司僅提供電話門號資料，並未揭露該門號申請人或使用人之姓名，由於未達足資識別特定當事人之程度，自無本法之適用問題。

（法務部96年6月21日法律字第0960023899號）

個人資料體檢步驟二：清查取得個人資料的來源

- 直接蒐集
  - 由當事人提供
- 間接蒐集
  - 自第三人取得
  - 經由公開管道取得

個人資料體檢步驟三：確認蒐集符合法定要件（非特種資料）

- 應有特定目的。
- 應符合下列情形：
  - 執行法定職務必要範圍內。
  - 經當事人書面同意：
    - ✓ 當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。
  - 對當事人權益無侵害。

告知義務–直接蒐集

告知時點：向當事人蒐集前	
應告知事項	**得免為告知之情況**
公務機關名稱	依法免告知
蒐集之目的	履行法定義務所必要
個人資料之類別	告知將妨害公務機關執行法定職務
利用之期間、地區、對象及方式	告知將妨害第三人重大利益
當事人得行使之權利	當事人明知應告知內容
當事人得自由選擇提供個人資料時，不提供對其權益之影響	

告知義務–間接蒐集

告知時點：處理或利用前	
應告知事項	**得免為告知之情況**
公務機關名稱	依法免告知
蒐集之目的	履行法定義務所必要
個人資料之類別	告知將妨害公務機關執行法定職務
利用之期間、地區、對象及方式	告知將妨害第三人重大利益
當事人得行使之權利	當事人明知應告知內容
	當事人自行公開或其他已合法公開
	學術機構機於公益或學術研究之目的，且資料經處理或無從辨識當事人
	不能向當事人或其法定代理人告知
	大眾傳播業者基於新聞報導之公益目的

個人資料體檢步驟四-3：確認於期限內履行告知義務

- 直接**蒐集**：蒐集時告知
- 間接**蒐集**：處理或利用前告知
  - 本法修正施行前非由當事人提供之個人資料，應自本法修正施行之日起1年內完成告知，逾期未告知而處理或利用者，以違反個資法第9條規定論處。(§54)

個人資料體檢步驟五：確認未違法蒐集、處理或利用特種資料

醫療、基因、性生活、健康檢查及犯罪前科之個人資料，除有下列情形外，不得**蒐集**：

- 法律明文規定。
  - 僅限於法律規定，不包括行政命令。
- 公務機關執行法定職務所必要，且有適當安全維護措施。
  - 例如檢警偵辦犯罪，蒐集或利用涉嫌人的犯罪前科資料。
- 當事人自行公開或其他已合法公開之個人資料。
- 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、處理或利用之個人資料。
  - 蒐集、處理或利用之範圍、程序及其他應遵行事項（是否經匿名化處理、依揭露方式無從識別特定當事人、是否應得當事人明示之書面同意），授權中央目的事業主管機關會同法務部定之。

個人資料管理制度

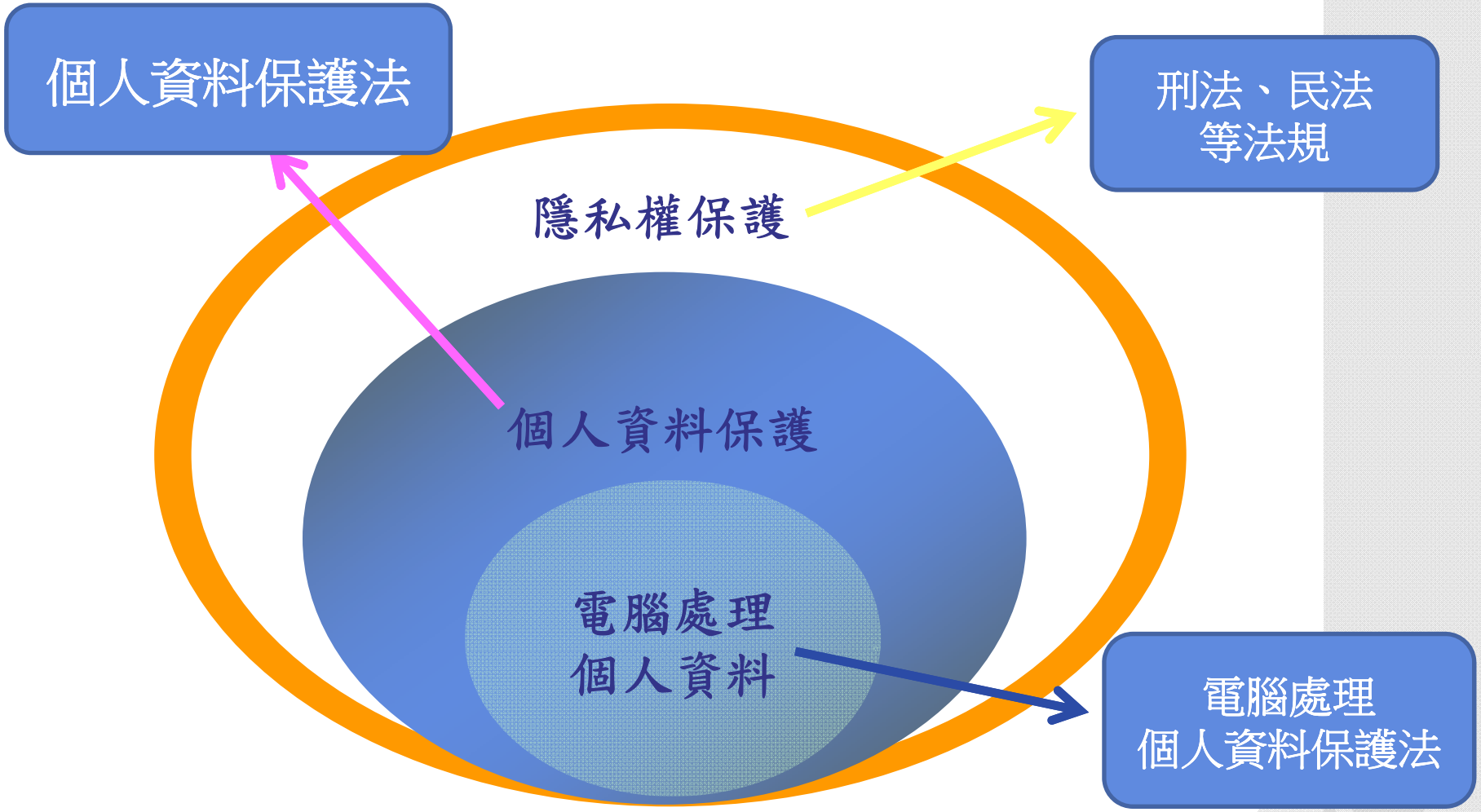




蒐集	處理	利用	儲存	銷毀
-依法進行告知義務 -取得書面同意	-採取適當保護措施，避免個人資料被竊取、竄改或毀損	-應於蒐集之特定目的內使用 -特定目的外之使用應另外取得書面同意	-採取適當保護措施，避免個人資料被竊取、竄改或毀損	-特定目的消失 -期限屆滿 -當事人要求

個人資料外洩管道

隱私權與個人資料保護差異



個人資料保護程序

1. 定義組織個人資料
2. 分析個人資料流
3. 識別現行保護措施
4. 個人資料風險管理

個人資料保護程序

1 定義組織個人資料

2 分析個人資料流

3 識別現行保護措施

4 個人資料風險管理

鑑別組織內所有個資相關業務流程

- 招生作業流程
- 註冊作業流程
- 人事晉用作業程
- 健康檢查作業
- 心理輔導諮商作業

個人資料保護程序

1 定義組織個人資料 → 2 分析個人資料流 → 3 識別現行保護措施 → 4 個人資料風險管理

1. 確認業務流程內的利害關係者， 如員工、委外廠商、客戶、主管機關

2. 列出讓業務流程順利運作所建置的資訊系統，如：備份系統

3. 分析上述流程中哪些與個人資料有關

個人資料保護程序

1 定義組織個人資料 → 2 分析個人資料流 → 3 識別現行保護措施 → 4 個人資料風險管理

4. 檢視與個人資料相關之業務流程，鑑別出一般個資與特種個資

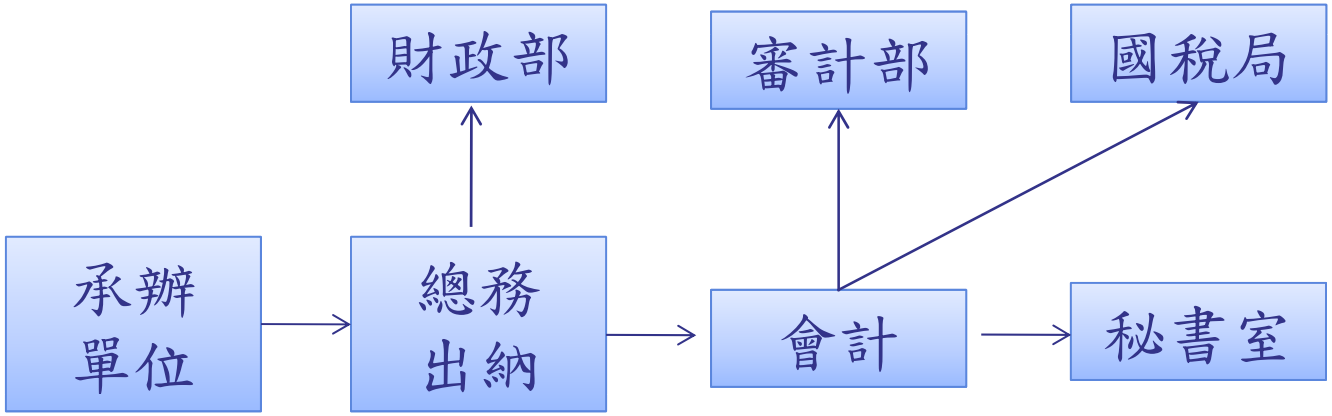
5. 查明個資來源、蒐集目的及蒐集方式（直接、間接、委外）

6. 辨識個人資料形式（電子、紙本或資料庫欄位）、欄位、檔案名稱

個人資料保護程序

1 定義組織個人資料 → 2 分析個人資料流 → 3 識別現行保護措施 → 4 個人資料風險管理

◆ **範例：公務機關「邀請專家學者出席會議請領車馬費作業」**



- 個資範圍：姓名、單位、身分證統一編號、戶籍地址、帳號、連絡電話等

個人資料保護程序

1 定義組織個人資料

2 分析個人資料流

3 識別現行保護措施

4 個人資料風險管理

個資生命週期

作業訪談

個人資料保護程序

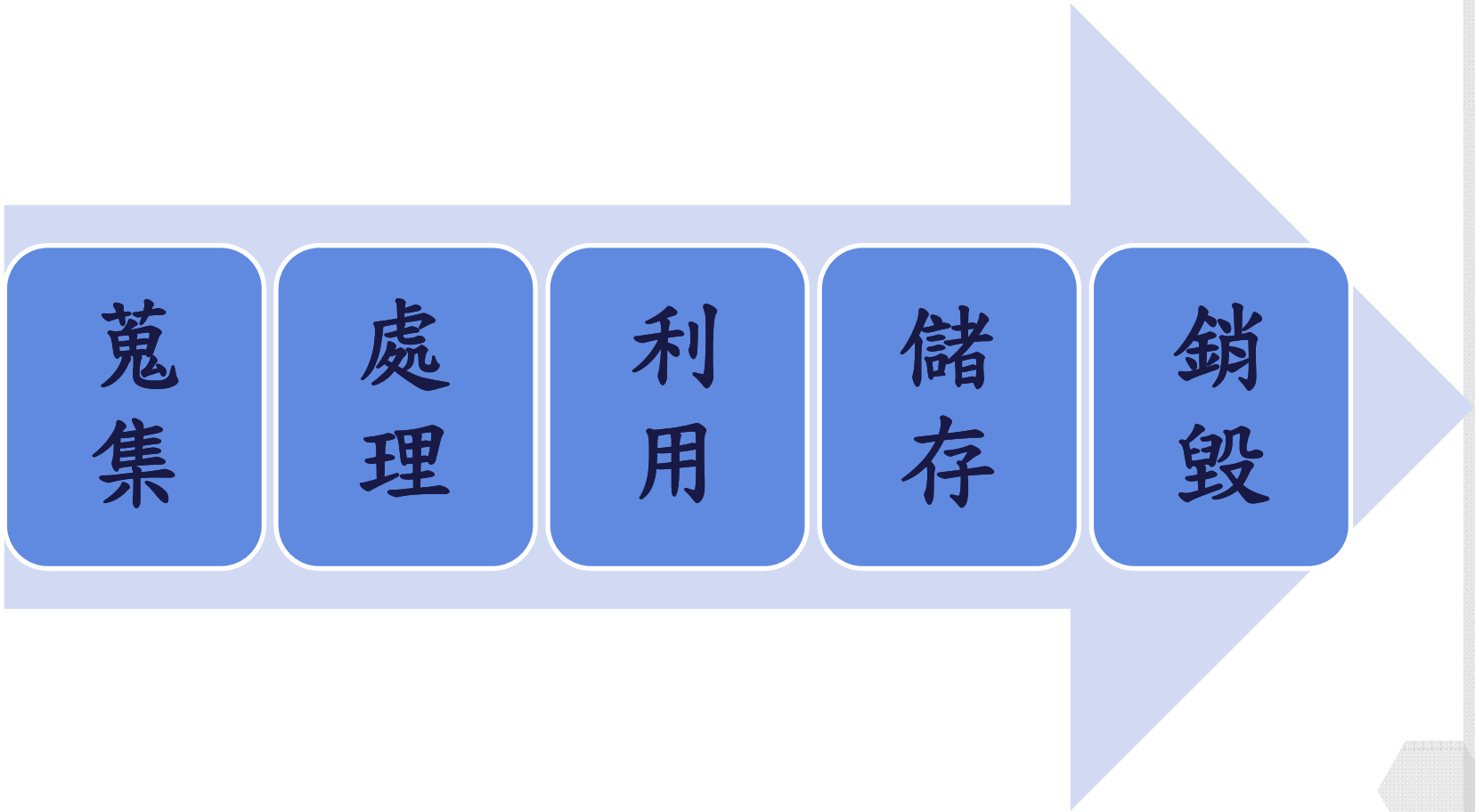
1 定義組織個人資料 → 2 分析個人資料流 → 3 識別現行保護措施 → 4 個人資料風險管理

個資生命週期

作業訪談

分析個人資料流

- 個人資料處理階段之生命週期：



分析個人資料流

何謂國外傳輸? 國內公司傳送Email至國外子公司，是否包含在內?

1. 依個資法第2條第6款之定義，國際傳輸指將個人資料作跨國（境）之處理或利用。

2. 個資法修正理由內進一步解釋國際傳輸之範圍：「不論是機關內部之資料傳送（屬資料處理），例如：總公司將資料傳送給分公司、公務機關將資料傳送給國外辦事處等；或將資料提供當事人以外第三人（屬資料利用），例如：母公司將資料提供給子公司或他公司、公務機關將資料傳送給他公務機關，只要該資料作跨國（境）之傳輸，不論是屬處理或利用行為，皆屬本法所稱之『國際傳輸』。」由此可知，國內公司傳送Email至國外子公司，自亦屬於國際傳輸。

此外，依照法務部94年8月26日法律字第0940029553號函之說明：「本法有關『國際傳遞』之規定，其立法目的係為落實個人資料保障之落實，避免跨境個人資料流通失控，故就我政府法權未及地域之跨境傳遞予以規範管理。準此，機關（公務或非公務）將個人資料傳輸至我國法權未及之地域，即屬本法所稱之『國際傳遞』，從而向大陸地區傳輸個人資料，自為本法所定之『國際傳遞』。」

依據上述定義、立法理由及函釋，國內公司傳送電子郵件至國外子公司或大陸地區子公司，構成跨國（境）之資料利用行為，自有個資法關於「國際傳輸」相關規定之適用。

方式
集
輸入、
結或
護措施？

分析個人資料流

◆各個階段的生命週期：

蒐集 → 處理 → 利用 → 儲存 → 銷毀

利用

- 指將蒐集之個人資料為處理以外之使用。

儲存

- 如何儲存個資？保存多久？

銷毀

- 如何銷毀個資？何時要銷毀？

分析個人資料流

注意

◆各個階段的生命週期：

- 組織內部資料傳送

處理

- 將個資提供第三人

利用

個人資料保護程序

1 定義組織個人資料

2 分析個人資料流

3 識別現行保護措施

4 個人資料風險管理

個資生命週期

作業訪談

分析個人資料流

- 作業訪談目的:
  - 在於瞭解每位同仁本身個資相關業務處理方式，及所使用之相關資訊(如紙本(電子)表單或系統等)。
- 訪談內容則參考適用之法令、法規或主管機關要求，以設計出可鑑別現行作業是否符合要求。

分析個人資料流

◆作業訪談內容範例：

- 請說明單位目前所負責之作業及業務流程？

流程名稱	檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料範圍	有否特種資料？	蒐集			處理		利用				保存		銷毀		揭露			現有控制
								來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍	
XX教育訓練報名作業	研討會廣宣名單	DA	合約	053教育或訓練行政	C001辨識個人者	姓名、單位、職稱、聯絡電話【或手機】、e-mail、傳真	否	寄送報名表請與會人員填寫資料	■直接 □間接	XX組	本機作業Excel表	XX組	無	台灣	XX組	報名通訊聯繫	XX組 X小姐 XXXX-XXXX # XXX	教育訓練執行期間	無	無	無	無	無	本機帳密保護

分析個人資料流

◆作業訪談內容範例：

- 請重點說明單位目前個資處理方式？

流程名稱	檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料範圍	有否特種資料？	蒐集			處理		利用				保存		銷毀		揭露			現有控制
								來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍	
XX教育訓練報名作業	研討會廣宣名單	DA	合約	053教育或訓練行政	C001辨識個人者	名、姓、單位、稱、職、絡、聯話電【或手機】、e-mail、傳真	否	寄送報名表請與會人員填寫資料	■直接 □間接	XX組	本機作業Excel表	X X組	無	台灣	XX組	報名通訊聯繫	XX組 X小姐 xxxx-xxxx # xxx	教育訓練執行期間	無	無	無	無	無	本機帳密保護

分析個人資料流

◆作業訪談內容範例：

- 組織於個資蒐集之初是否已主動告知當事人得利用個資之利害相關方與其個資利用方式等相關資訊？
- 遵循特定的紀錄保存規範？
- 個資使用及保存管理為何?
- 個人資料保存管控?用久或需銷毀

分析個人資料流

流程名稱	檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料範圍	有否特種資料？	蒐集			處理		利用				保存		銷毀		揭露			現有控制
								來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍	
XX教育訓練報名作業	研討會廣宣名單	DA	合約	053教育或訓練行政	C001辨識個人者	名、單位稱、職、聯絡電話【或手機】、e-mail、傳真	否	寄送報名表請與會人員填寫資料	■直接 □間接	XX組	本機作業Excel表	XX組	無	台灣	XX組	報名通訊聯繫	XX組 X小姐 xxxx-xxxx # xxx	教育訓練執行期間	無	無	無	無	無	本機帳密保護

分析個人資料流

流程名稱	檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料範圍	有否特種資料？	蒐集			處理		利用				保存		銷毀		揭露			現有控制
								來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍	
XX教育訓練報名作業	研討會廣宣名單	DA	合約	053教育或訓練行政	C001辨識個人者	名稱、單位、職稱、聯絡電話【或手機】、e-mail、傳真、姓	否	寄送報名表請與會人員填寫資料	■直接 □間接	XX組	本機作業Excel表	XX組	無	台灣	XX組	報名通訊聯繫	XX組 X小姐 xxxx-xxxx # xxx	教育訓練執行期間	無	無	無	無	無	本機帳密保護

分析個人資料流

◆作業訪談所得資料彙整於個人資料清冊：

單位	流程	個資檔案	格式	個人資料流				
				蒐集	處理	利用	儲存與銷毀	揭露
業務單位	員工聯絡資料維護作業	員工聯絡資料名冊	DA	業務單位	業務單位	業務單位	業務單位	無
總務	採購作業	採購案契約書數份	DA	業務單位	業務單位	總務	總務	無
會計	付款作業	憑證用紙（出差費、講師鐘點費）	DC	會計	會計	會計	會計	查帳主管機關
政風	檢舉作業	檢舉人資料	DC	政風	政風	主管機關	政風	主管機關

個人資料保護程序

1 定義組織個人資料 → 2 分析個人資料流 → 3 識別現行保護措施 → 4 個人資料風險管理

1. 對於保有的個人資料檔案，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏

2. 對個人資料之存取，建議識別碼或通行碼，並加設資料存取控制。

3. 定期及不定期稽核檔案管理情形。

個人資料管理具體行動通知當事人以預防損害

- 違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。(§12)
  - 通知方式：人數不多時，得以電話或信函通知；人數眾多時，得以公告請當事人上網或電話查詢。
  - 隱匿不為通知者，上級機關應查明後令機關改正，並依法懲處失職人員。

個人資料的生命週期管理

- 個人資料**蒐集**之特定目的消失或期限屆滿：應刪除、停止處理或利用該個人資料。
  - 例外情形：因執行職務或業務所必須，或經當事人書面同意。(§11)
- 違反個資法規定**蒐集**、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。(§11)

關於蒐集部份，律師回覆說明

◆無特定目的，僅蒐集個人資料，是否違法？

- 依個資法第19條第1項前段之規定，**非公務機關對個人資料之蒐集或處理，應有特定目的，並符合該條所列之法定事由**。同法第8條第1項及第9條第1項亦規定，公務機關或非公務機關依第15條或第19條規**定向當事人蒐集個人資料時，應明確告知當事人蒐集之目的**；公務機關或非公務機關依第15條或第19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第8條第1項第1款至第5款所列事項**。由此可知，**學校單位蒐集個人資料除了應符合第19條所列之法定事由，並應明確說明其特定目的。**

關於蒐集部份，律師回覆說明

- 告知之方式，只有個別告知嗎？網站統一告知是否可行？
  - 依法務部預告之個資法施行細則修正草案第13條規定：「依本法第八條、第九條及第五十四條所**定告知之方式，得以書面、電話、傳真、電子文件或其他適當方式為之。**」該條修正理由說明：「**蒐集者應以個別通知之方式讓當事人知悉。」是於直接蒐集、間接蒐集或個資法施行前已為間接蒐集個人資料而應踐行或補行告知程序者，應以分別通知之方式使當事人知悉，不得逕經由網站統一公告。**

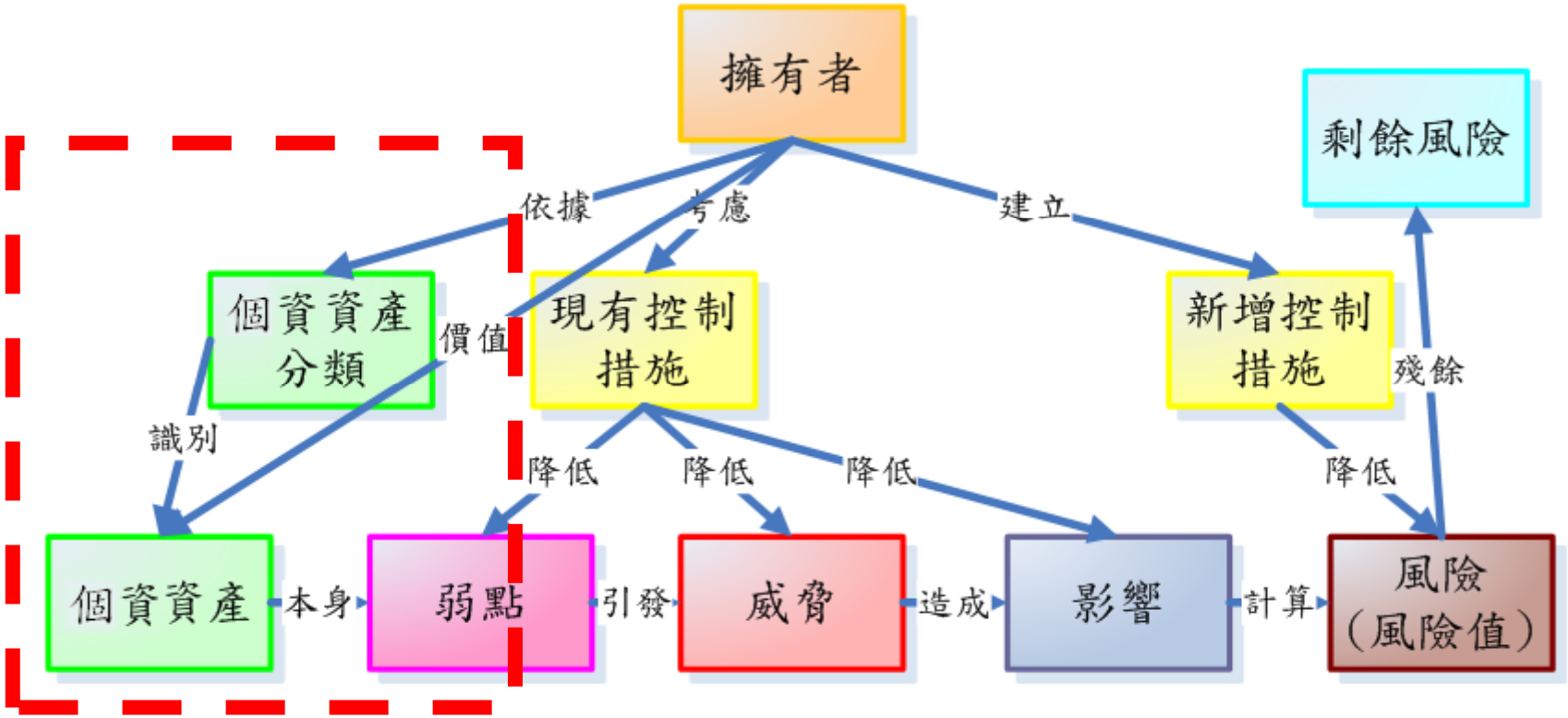
關於蒐集部份，律師回覆說明

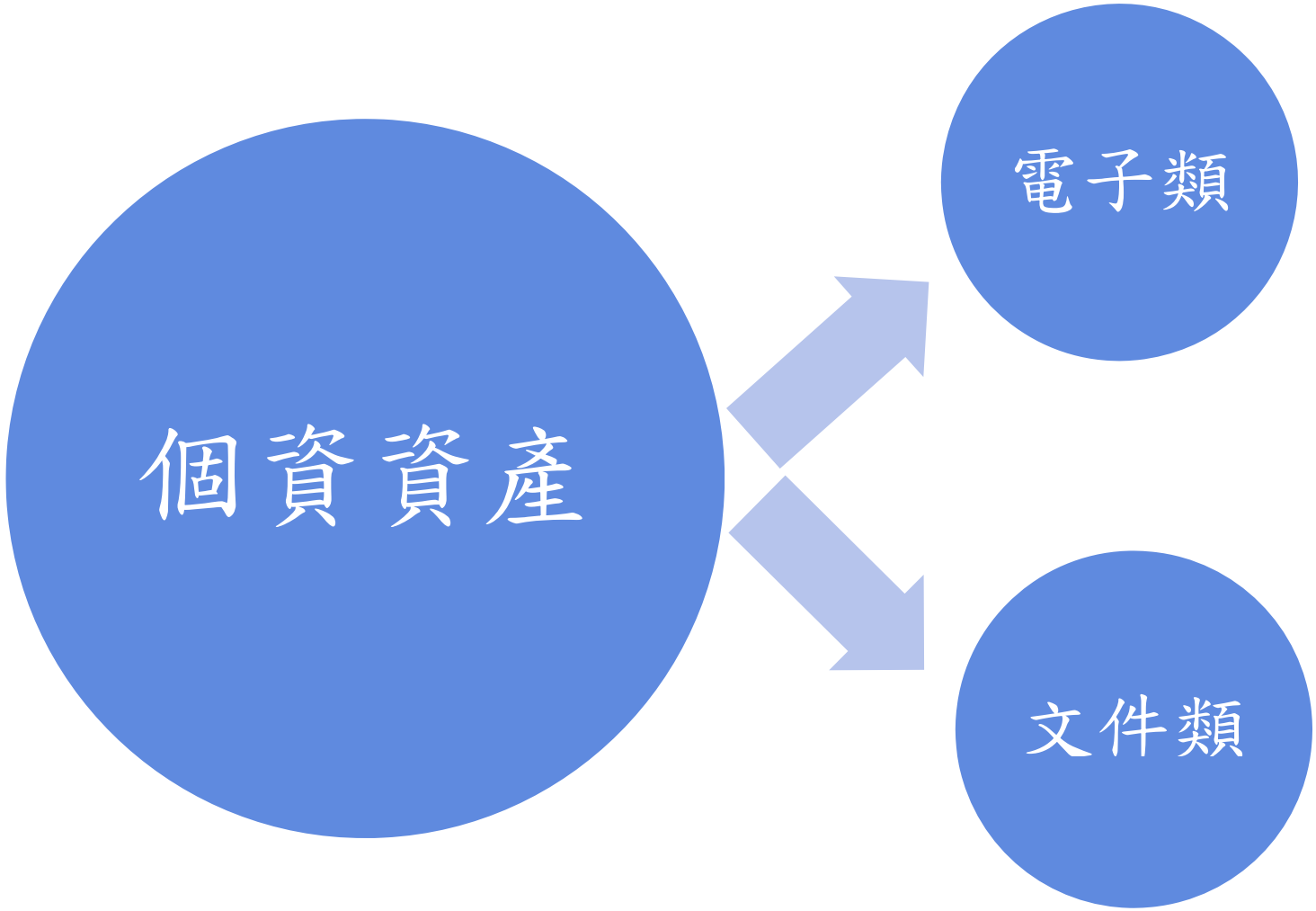
- 此外，共同行銷管理辦法第13條第5項規定，**關於「客戶資料變更修改方式」及「選擇退出方式」等措施，除公告外，應另以書面或電子郵件方式為之，以達到個別通知之效果。**

- 另一方面，個資法第12條規定，**公務機關或非公務機關違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應於查明後以適當方式通知當事人。**依法務部預告之個資法施行細則修正草案第18條規定：「**本法第十二條所稱適當方式通知，係指即時以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但耗費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他足以使公眾得知之方式為之。」是於個人資料被竊取、洩漏、竄改或其他侵害而須通知當事人之情形，原則上仍應分別通知當事人，但如個別通知當事人所需耗費之成本過鉅，得例外以網站統一公告，惟應兼顧當事人隱私之保護。**

- 個人資料流之重要性
- 個資法對蒐集階段之限制
- **資訊資產分類原則**
- 建立個資資產清冊
- 個資衝擊分析

建立個資資產原則


擁有者
剩餘風險
依據
考慮
建立
個資資產分類
價值
現有控制措施
新增控制措施
殘餘
識別
降低
降低
降低
降低
個資資產
本身
弱點
引發
威脅
造成
影響
計算
風險（風險值）

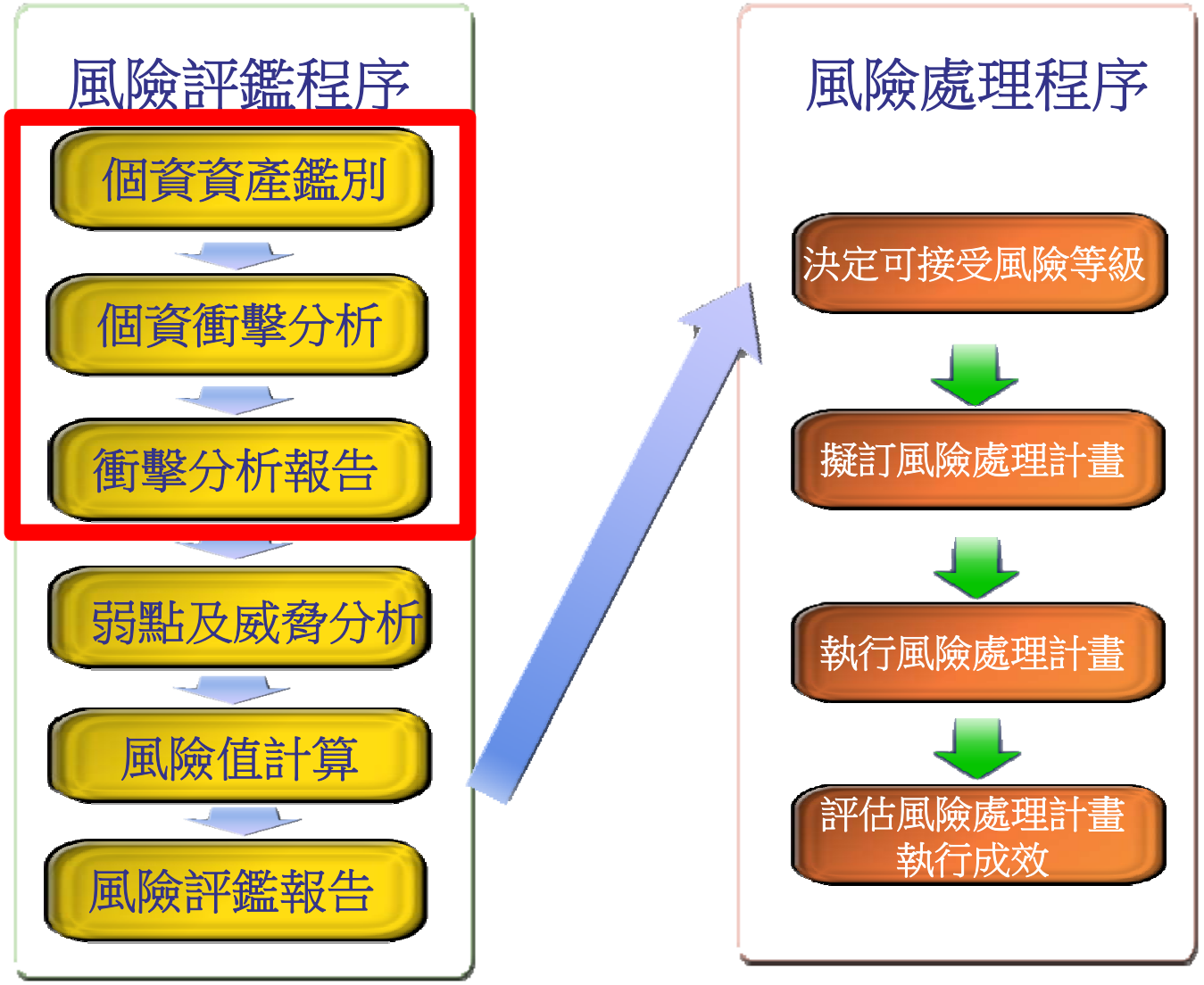

個資資產
電子類
文件類

個資資產分類

- **電子 (Data)**
  - 儲存於硬碟、磁帶、光碟、唯讀記憶體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。
- **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。

- 個人資料流之重要性
- 個資法對蒐集階段之限制
- 資訊資產分類原則
- **建立個資資產清冊**
- 個資衝擊分析

個人資料風險管理程序


風險評鑑程序
個資資產鑑別
個資衝擊分析
衝擊分析報告
弱點及威脅分析
風險值計算
風險評鑑報告
風險處理程序
決定可接受風險等級
擬訂風險處理計畫
執行風險處理計畫
評估風險處理計畫
執行成效

個資盤點

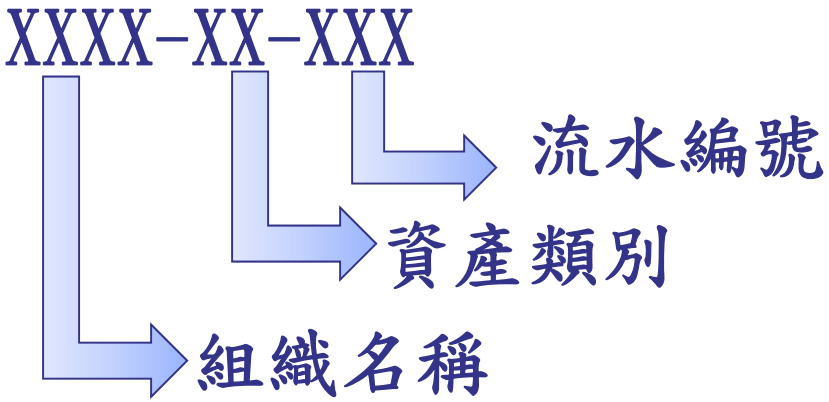
- 個資盤點是管理制度中相當重要的作業，唯有全面性進行清查，才能了解相對應之風險，並施以適切的控制措施。
- 根據法規要求個資之定義，重新檢視所有已蒐集之資訊。
- 鑑別出所有與個人資料相關之營運流程。
- 針對各個流程細項了解其流程架構。
  - 各個活動執行時，資料輸入輸出之說明。
  - 資料流向。

個資資產清冊欄位

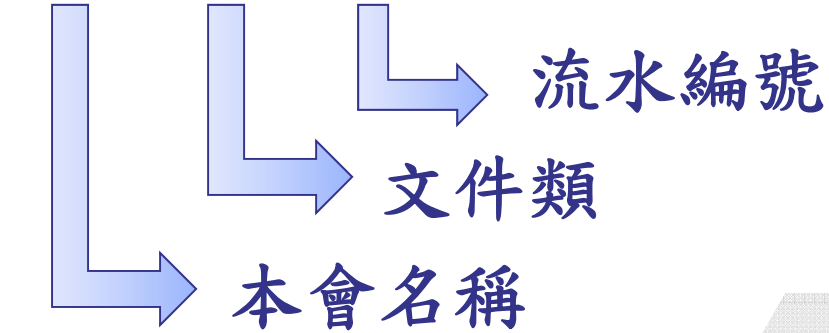
資產編號	流程名稱	個人資料檔案名稱	資料形式	法律依據	個人資料之範圍	有否特種資料？何種特種資料？	蒐集			處理 (指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送)		利用 (將蒐集之個人資料為處理以外之使用)				保存		銷毀		揭露			現有控制	衝擊值
							來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍		
個人資料資產編號	業務流程名稱	個人資料表單或檔案名稱	電子或文件	依據法令法規或內部規定	個資表單或檔案之欄位	是否含有療因生健康查罪科檢犯前科	個資蒐集來源（網站或問卷）	個資蒐集方式（直接、間接）	個資蒐集單位	個資處理方式	個資處理單位	個資利用的期間	台灣地區或是國外	個資利用對象	個資利用之方式及目的	資存位其絡式個保單及連方	個資保存期限	個資銷毀方式	個資銷毀頻率	個資揭露對象	個資揭露方式與目地	個資揭露的範圍	對個資之現有保護	個資價值（衝擊值）

資產編碼方式

- 資產編號之編碼方式，如右圖
  - 1～4 碼為組織名稱
  - 5、6 碼為資產類別
  - 7～9 碼為資產流水編號



例如：



個資資產清冊

資產編號	流程名稱	個人資料檔案名稱	資料形式	法律依據	個人資料之範圍	有否特種資料？何種？	蒐集			處理		利用				保存		銷毀		揭露			現有控制	衝擊值
							來源	方式	單位	方式	單位	期間	地區	對象	方式目的	單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍		
NCHU-DA-001	學籍系統作業	學籍系統資料	DA	053 079 C001	名民分統編、業絡式（地址、話絡真司址、電連傳公地址姓國身證一號職聯方	否	學生提供	■直接 □間接	教務處	建檔	教務處	校務行政系統	台灣	本校各處室	學生事務管理	教務處XX小姐	永久保存	紙本銷毀，電子永久保存	學生畢業後半年進行銷毀	無	無	無	權限控管	

個資資產群組化

- 好處
  - 降低風險評鑑負擔，減少弱點、威脅的重複識別。
- 群組原因
  - 先依據識別出之個資資產進行分類，再從分類中群組化資產避免遺漏重要資產。
  - **針對群組資訊資產進行風險評鑑。**
- 原則
  - 個資資產價值相同。
  - 個資資產性質、欄位相同，且資產數量較多。
  - 不需知道細部作業，即可進行風險鑑別。
    - 個資欄位要相同。

- 個人資料流之重要性
- 個資法對蒐集階段之限制
- 資訊資產分類原則
- 建立個資資產清冊
- 隱私衝擊分析

隱私衝擊分析（PIA）

- 個資資產權責單位應依據個資資產清冊之評估標準，確認個資流程衝擊價值。
- 以保護隱私為核心考量。
- 識別並制定隱私的可歸責性，清楚呈現管理者及任何其他參與者的責任。
- 提供決策者必要資訊，以利投入資源。

隱私衝擊分析

- 隱私衝擊分析中重要活動有：
  - 流程／活動列表分析。
  - 識別各項流程/活動之負責部門。
  - 各活動存取個資之範圍。
  - 各活動存取個資之存取方式。
  - 各活動安全性之控制目標。
  - 各活動現行控制措施之有效性。

隱私衝擊分析

- 隱私衝擊分析流程：
  - PIA計畫。
  - 評鑑（組織流程差異分析）。
  - PIA報告。
  - 技術專家／法律顧問。
  - 可使用在相關系統之決策。

個資隱私衝擊分析

以個資法之要求對組織個資作業之衝擊進行評估分析

◆ 設定評估等級標準，如：

衝擊影響程度	個人資料範圍
極高(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**。
高度(3)	1. 含自然人之**姓名**及**國民身分證統一編號**（或護照號碼），但不含特種個人資料。 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：卡號、帳號）**，但不含特種個人資料。
中度(2)	含自然人之**姓名**，但不包含**身分證**或特種資料。
一般(1)	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

個資隱私衝擊分析

資產編號	流程名稱	個人資料檔案名稱	資料形式	法律依據	個人資料之範圍	有否特種資料？何種？	蒐集			處理		利用				保存		銷毀		揭露			現有控制	衝擊值
							來源	方式	單位	方式	單位	期間	地區	對象	方式目的	單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍		
NCHU-DA-001	學籍系統作業	學籍系統資料	DA	053 079 C001	姓名、國民身分證統一編號、職業、聯絡方式（地址、電話、傳真、公司地址	否	學生提供	■直接 □間接	教務處	建檔	教務處	校務行政系統	台灣	本校各處室	學生事務管理	教務處XX小姐	永久保存	紙本銷毀，電子永久保存	學生畢業後半年進行銷毀	無	無	無	權限控管	3

個資隱私衝擊分析-範例

個人資料檔案名稱	資料形式	個人資料之範圍	衝擊值
人事扣款清冊	DA	姓名、身分證	3
中央銀行國庫局匯出匯款證明書	DA	姓名、匯款帳戶	3
薪資表	DA	姓名、身分證統一編號、職稱、住址、住家電話號碼、銀行帳戶之號碼、離職之日期、貸款餘額	3

衝擊影響程度	個人資料範圍
極高(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**。
高度(3)	1. 含自然人之**姓名及國民身分證統一編號**（或護照號碼），但不含特種個人資料。 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：卡號、帳號）**，但不含特種個人資料。
中度(2)	含自然人之**姓名**，但不包含**身分證**或特種資料。
一般(1)	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

個資隱私衝擊分析-範例

檔案名稱	資料形式	個人資料之範圍	衝擊值
生活津貼資料	DA	姓名、身分證、職稱、官職等、俸點、俸額、戶籍地址、眷屬人事資料、就學資料（結婚補助、生育補助、子女教育補助、眷屬喪葬補助之當事人）。	3
人事資料	DC	姓名、身分證、性別、出生日期、通訊處及電話、學歷、考試、外國語文、訓練進修、家屬、兵役、教師資格、身心障礙及原住民註記、經歷及現職、獎懲、考績	4
健保名冊	DA	姓名、身分證、性別、出生日期、俸級、家屬、身心障礙及原住民註記	4

衝擊影響程度	個人資料範圍
極高(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**。
高度(3)	1. 含自然人之**姓名及國民身分證統一編號**（或護照號碼），但不含特種個人資料。 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：卡號、帳號）**，但不含特種個人資料。
中度(2)	含自然人之**姓名**，但不包含**身分證**或特種資料。
一般(1)	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

範例-隱私衝擊分析

- 流程名稱：辦理各項審查會議
- 流程：上網搜尋委員的聯絡資料，建立審查委員聯絡表（姓名、任職單位、專長、e-mail、地址、電話）→逐一聯繫邀約，直至委員名單確認（每案約3位）→召開會議或採書面審查→發給委員出席費或審查費（付款時需蒐集受款人的姓名、身分證字號、戶籍地址、聯絡電話）

表單或檔案名稱	數量
審查委員名單	約30筆
簽到表_xx審查會議	約3筆
出席費領據	約3筆
審查費領據	約3筆

個人資料檔案名稱	資料形式	個人資料之範圍	衝擊值
審查委員名單	紙本	姓名、任職單位、專長、e-mail、地址、電話	2
簽到表_xx審查會議	紙本	姓名、任職單位	2
出席費領據	紙本	姓名、身分證字號、戶籍地址、聯絡電話	3
審查費領據	紙本	姓名、身分證字號、戶籍地址、聯絡電話	3

練習-隱私衝擊分析

- 請針對人資部辦理教育訓練課程之流程進行隱私衝擊分析。
- 流程：人資部於報名網站放置報名表→各部門同仁上網進行線上報名→人資部e-mail發出上課通知→報名同仁上課報到→課程結束後由人資部進行學習時數統計。

網站報名表

姓名：_____

任職單位：_____

部門：_____ 職稱：_____

公務e-mail：_____

手機：_____

身分證字號：_____

研討會簽到表		
姓名	部門	職稱

問題與討論