

個人資料鑑別與盤點課程



資深顧問師 彭至賢 (Sam Peng)

ISO27001/BS10012/ISO9001主導稽核員

PMP&APMP國際專案管理師

TTQS國家訓練品質計畫評核委員

Mobile: 0952-695460

E-mail: sam@safelink.com.tw

SafeLink 博創資訊科技股份有限公司



課程大綱

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



一、個人資料流之重要性



個人資料流之重要性

- 個資法第二條 用詞定義如下：
- 個人資料範圍：
 - 指自然人之姓名、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。
 - 細則第二條本法所稱個人，指現生存之自然人。



個人資料流之重要性

- 特種個人資料之定義
- 本法第二條第一款所稱**病歷**，應指下列各款資料：
 - 醫師依醫師法執行業務所製作之病歷。
 - 各項檢查、檢驗報告資料。
 - 其他各類醫事人員執行業務所製作之紀錄。
- **醫療**：
 - 指除前項病歷以外，其他以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為之診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術、或處置等行為全部或一部所產生之個人資料。
- **基因**：指由一段去氧核糖核酸構成，為生物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**：指對於無明顯疾病症狀，非出於對特定疾病診斷或治療之目的，以醫療行為所為診察行為之全部或一部之總稱。
- **犯罪前科**：指經緩起訴、職權不起訴或法院判決有罪確定之紀錄。



個人資料檔案

- 指依系統建立而得以自

動化

化方

人資

- 施行

條第

檔案

軌跡

- 注意

擊影響？

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。

網頁

資料表

Word

Excel

PDF

TXT

CSV

HTML

EML

PST

XML

資料庫

備份

電子檔案

磁帶

個人資料檔案的類型



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

金融帳號、
財務狀況



學籍、成績、
學籍資料、
教職員資料

教育



病歷、健康
檢查記錄

醫療健康



通訊、網路



電信帳單、
網路會員
資料

社會福利



身心障礙
別、醫療
證明

政府地政



戶政資料、
地政資料
財產狀況



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

- 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)。



二、個資法對蒐集階段之限制



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？
 - 病歷、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(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

• 有沒有不受個資法保護的資料？

1. 個人資料

§2現生存之自然人

例示

定義

得以直接或間接方式識別該個人之資料

非例示

間接識別

判斷標準

指保有該資料之公務或非公務機關僅以該資料不能識別，
須與其他資料對照、組合、連結等，始能識別該特定個人者

§51 不適用本法

自然人為單純個人或家庭活動之目的

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



個人資料體檢步驟一：清點個人資料

- 電子郵件

- 只有E-mail算不算是個人資料??

- 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

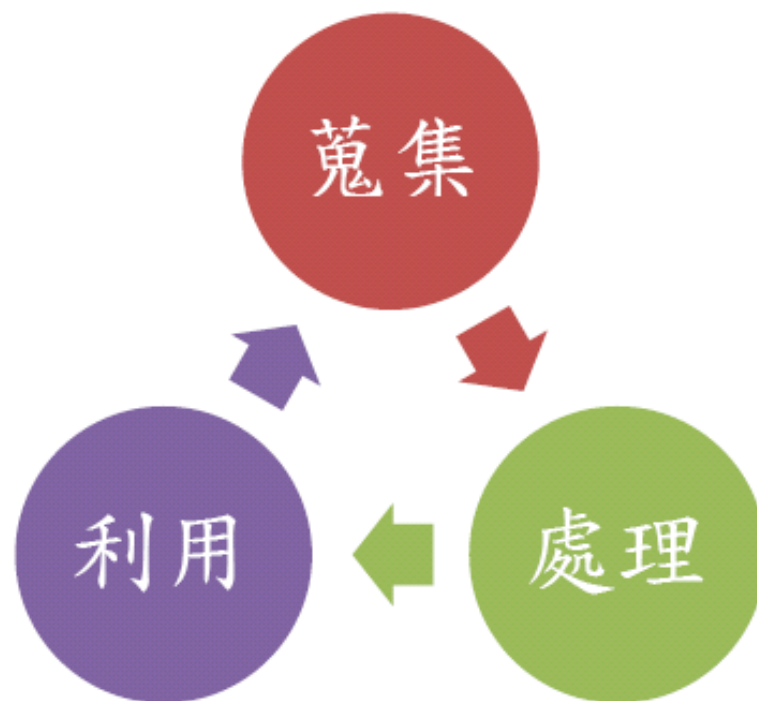
• 電話號碼

- 只有電話號碼算不算是個人資料??
- 電話門號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。
- 個人資料來源：
 - 員工、客戶、訪客、委外、其他……。



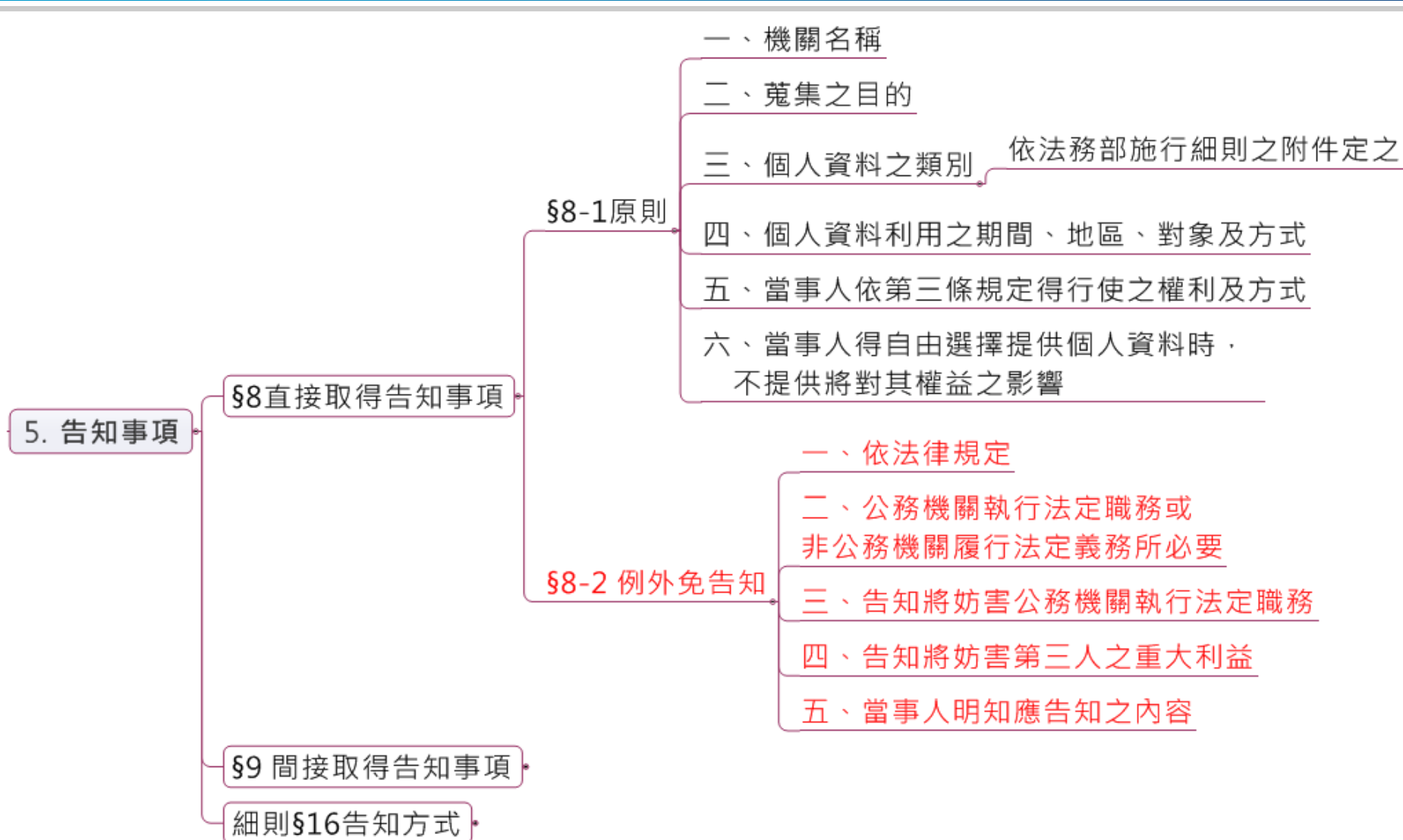


個人資料體檢步驟三：確認蒐集符合法定要件 (非特種資料)

- 個人資料之蒐集或處理，應有特定目的，並符合下列情形之一者：
 - 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。

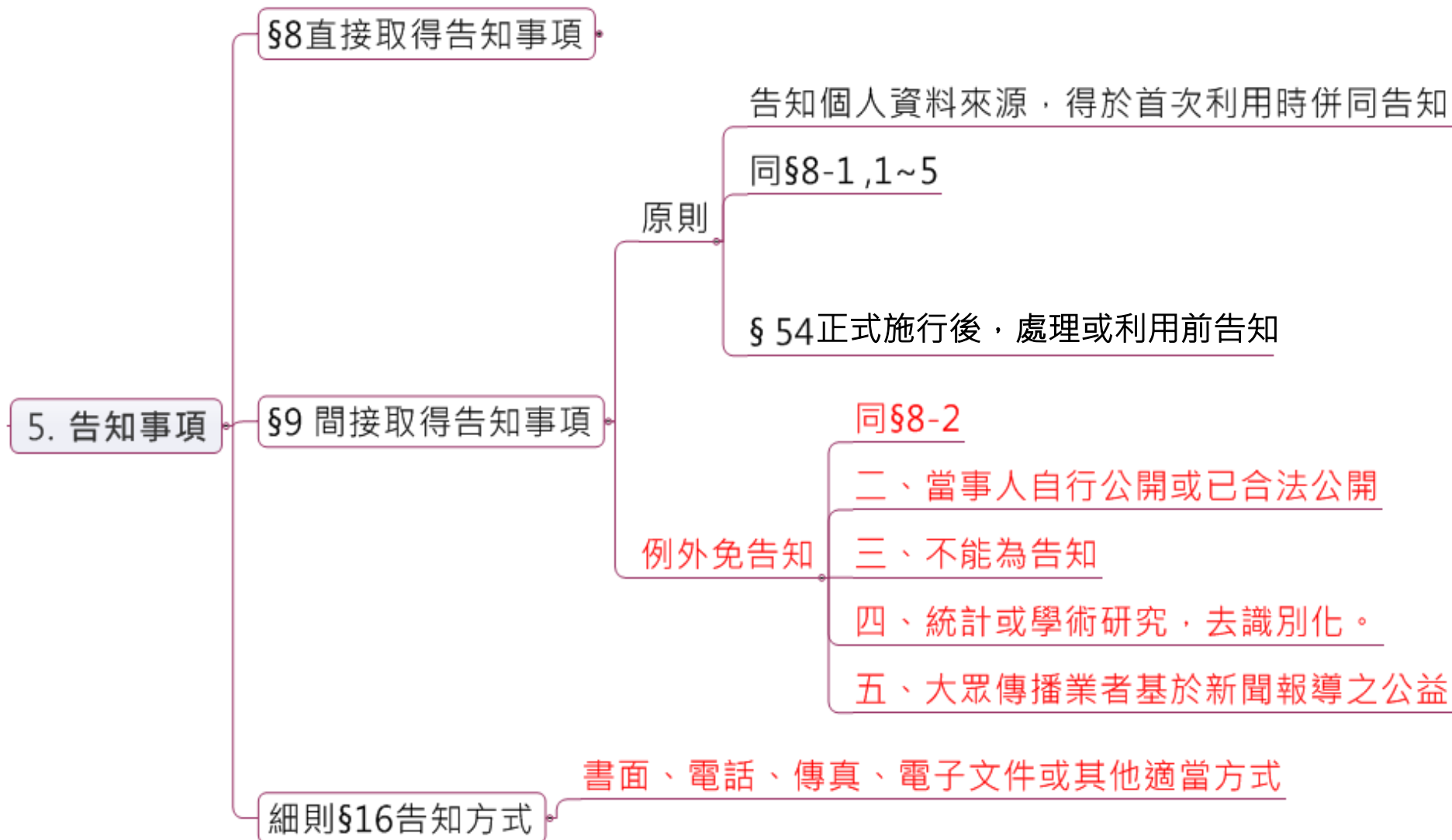


告知之義務-直接蒐集個資





告知之義務-間接蒐集個資



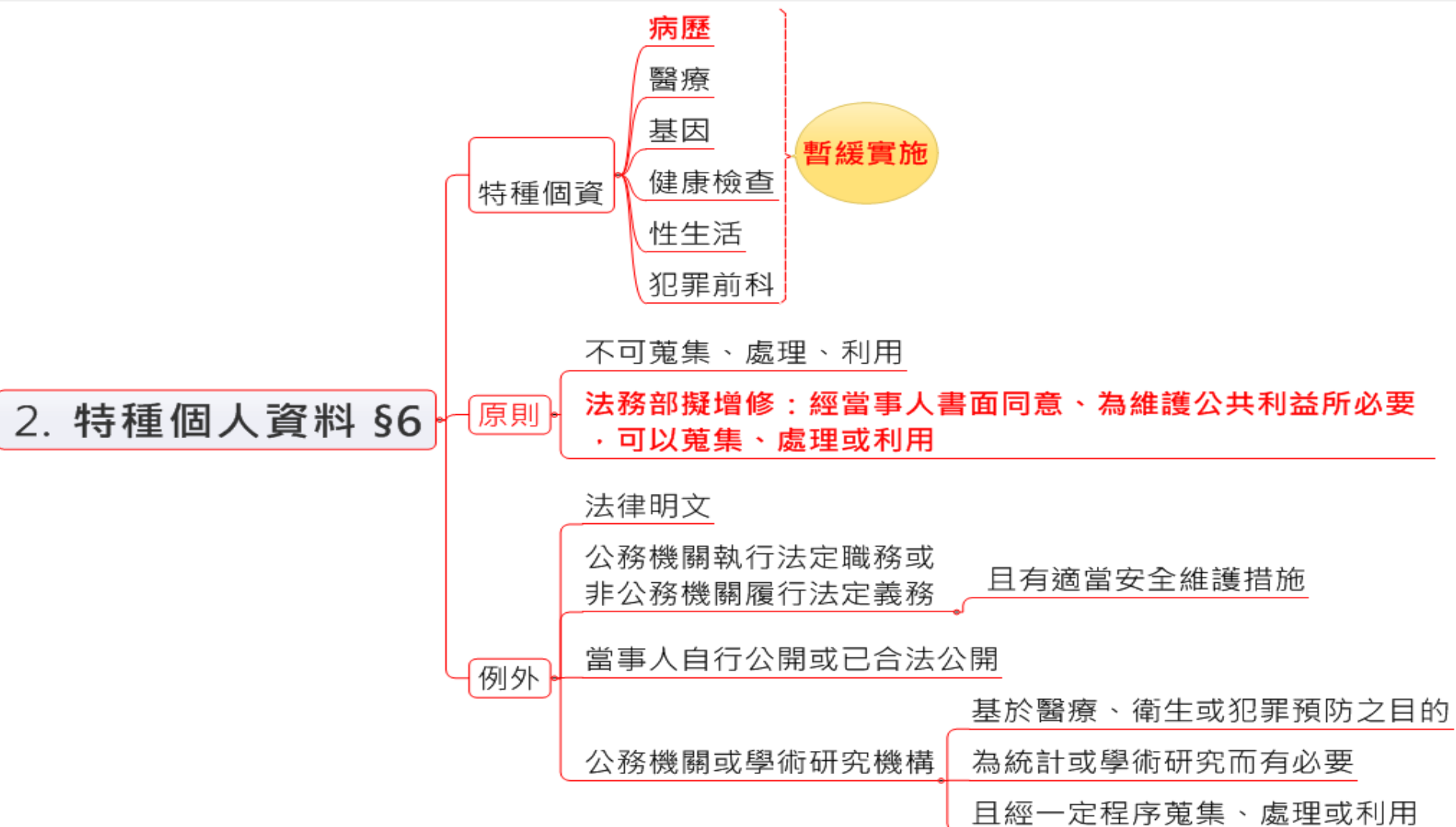


個人個人資料體檢步驟四：確認於期限內履行告知義務

- 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，應自本法修正施行後，應於處理或利用前告知，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：未違法蒐集、處理或利用特種資料





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

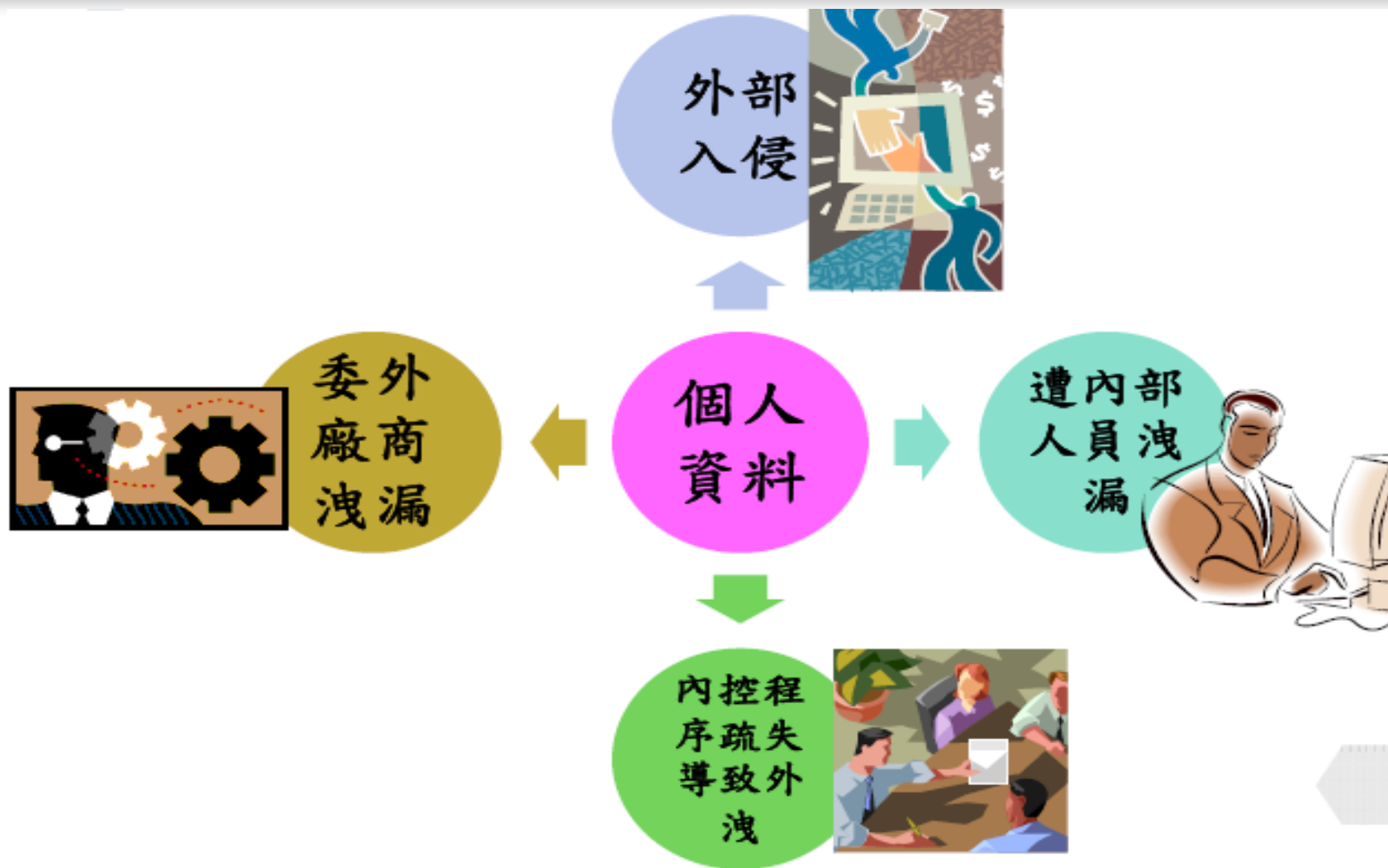
-應於蒐集之特定目的內使用
-特定目的外之使用應另外取得書面同意

-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



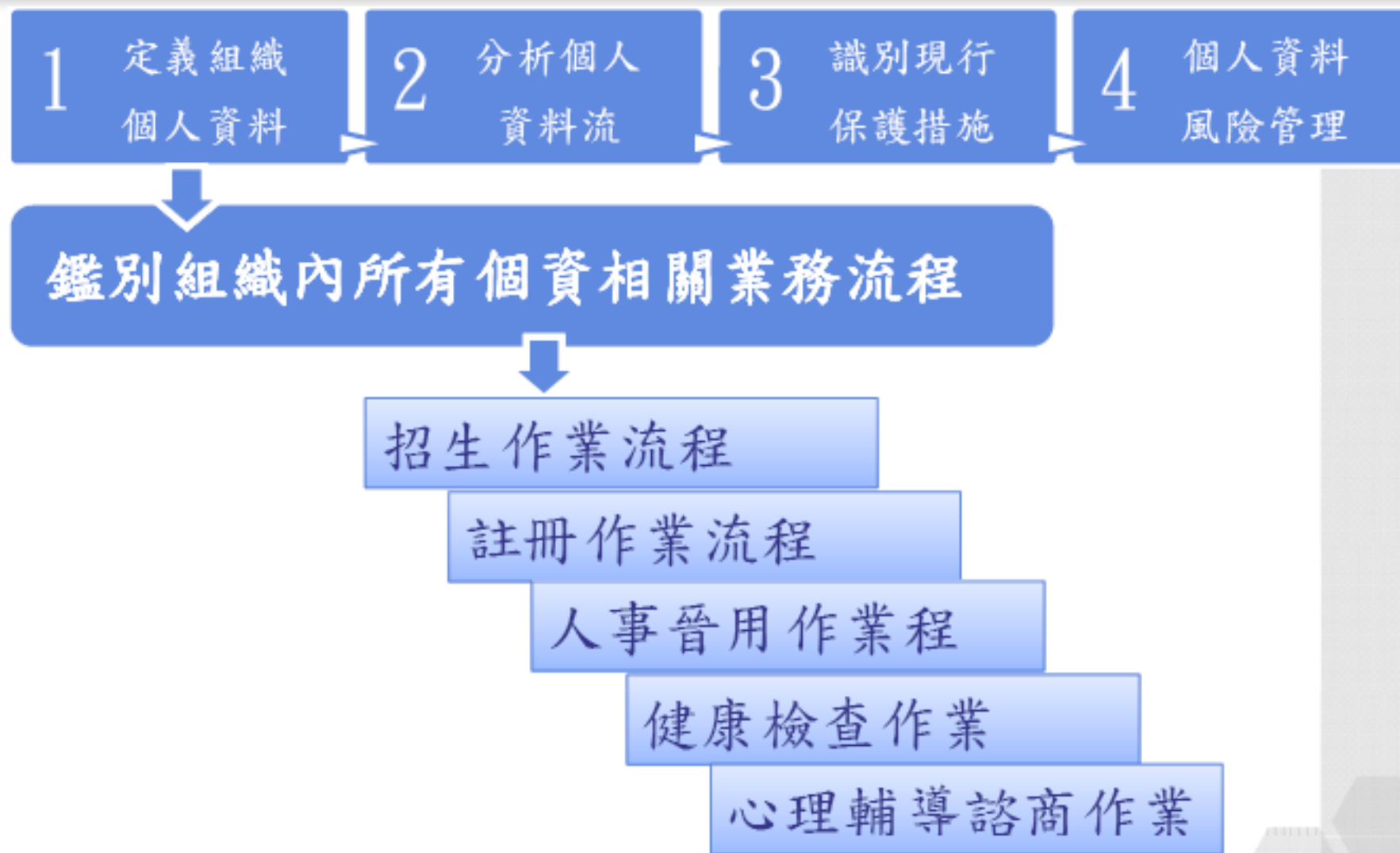


個人資料保護程序



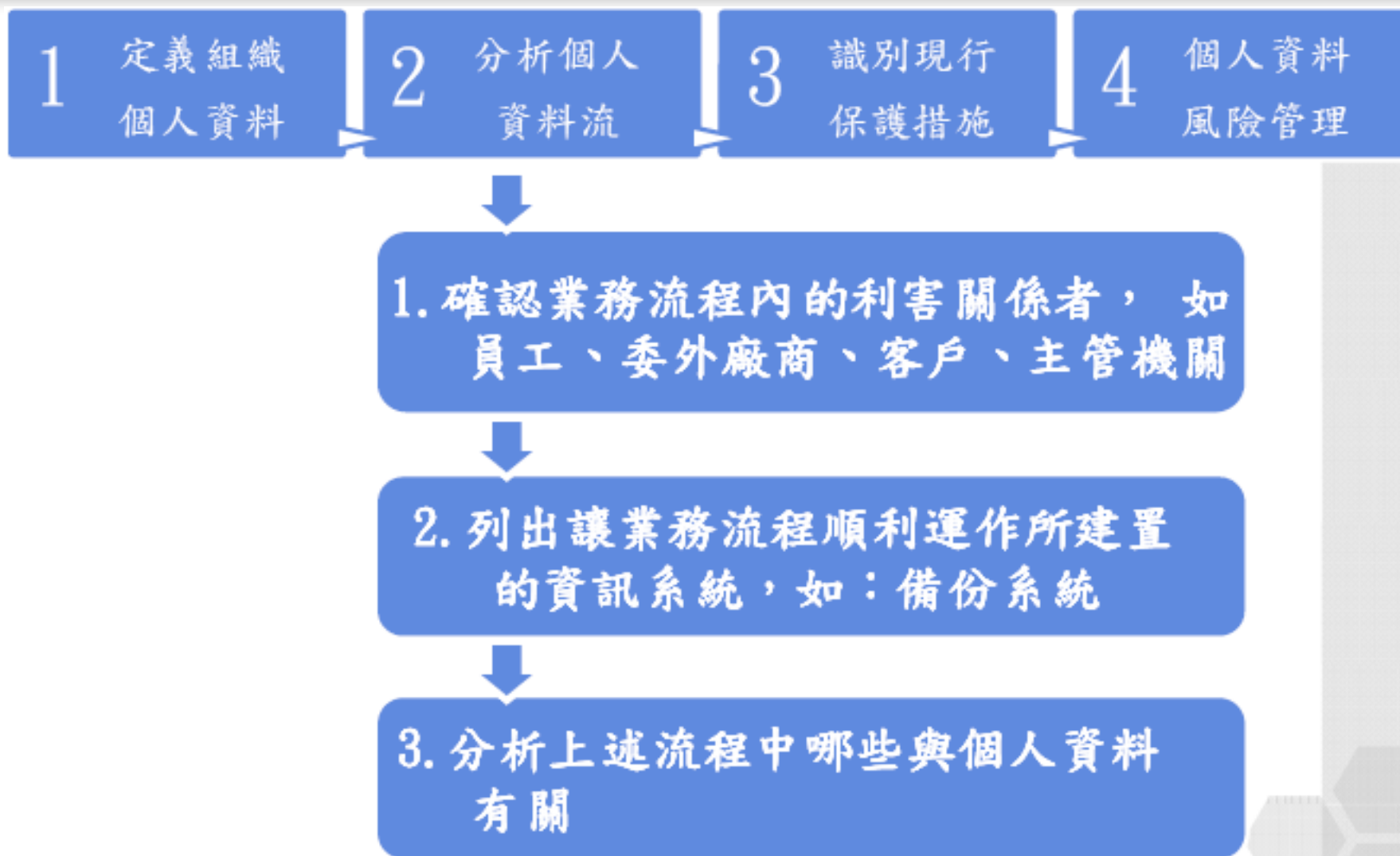


個人資料保護程序



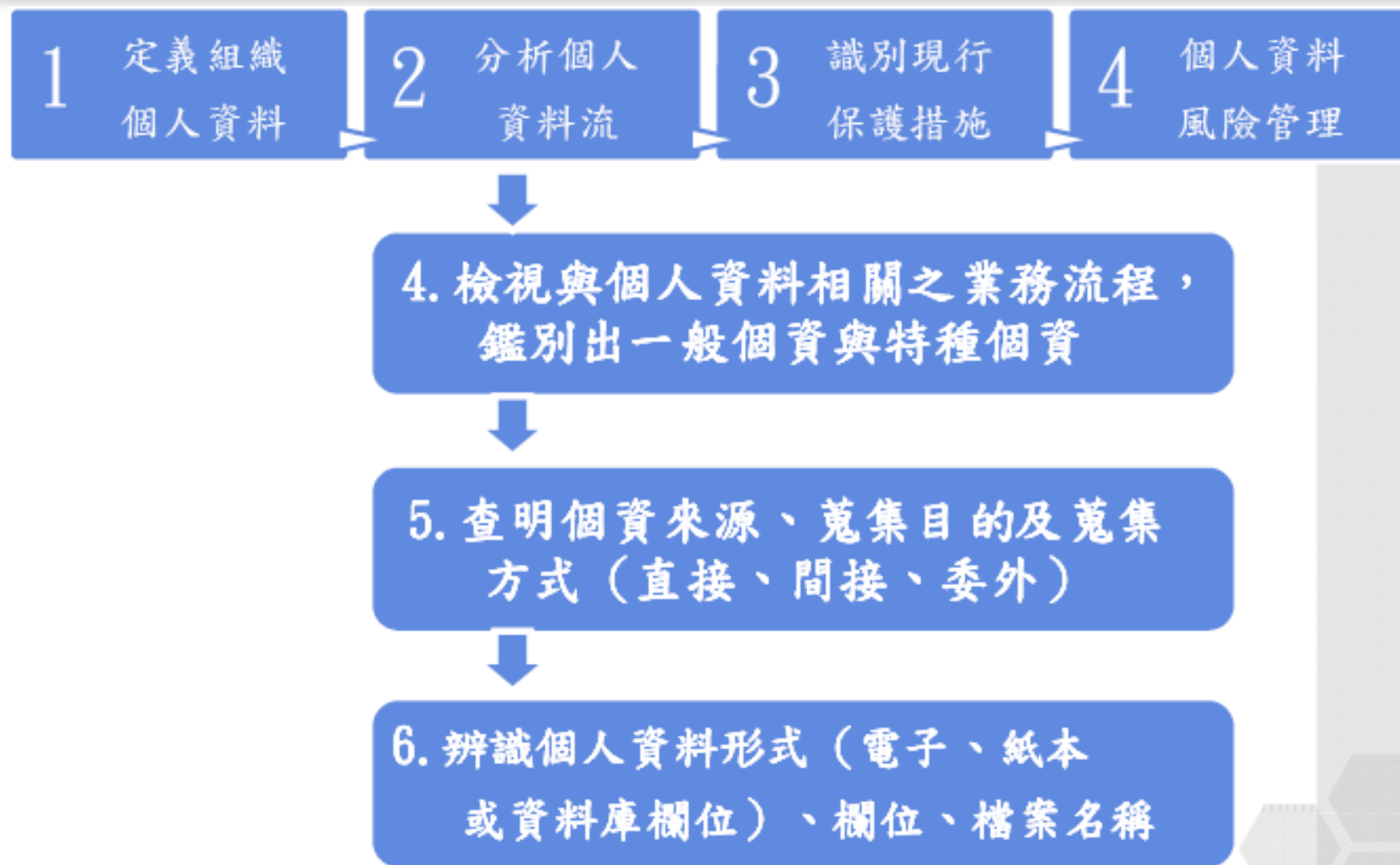


個人資料保護程序





個人資料保護程序

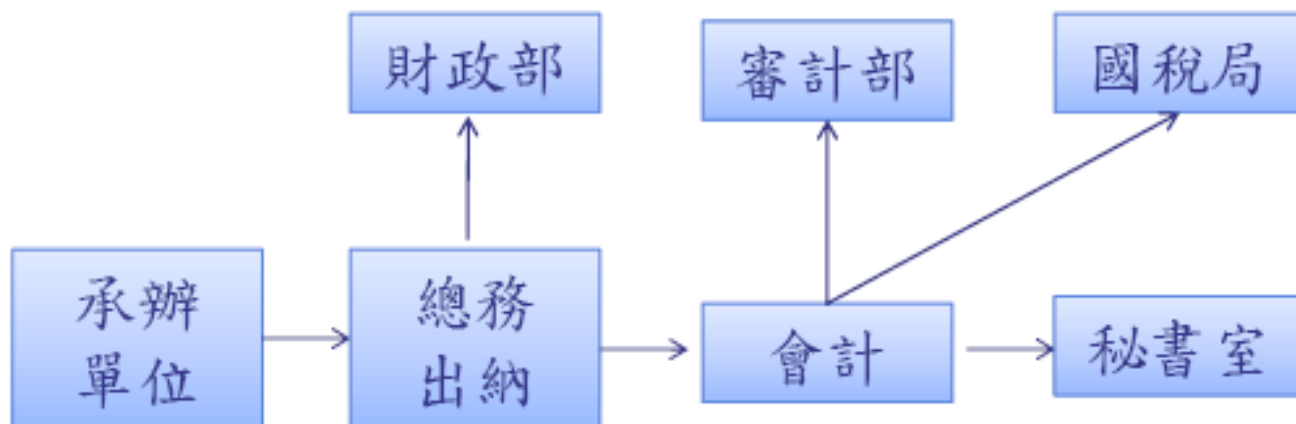




個人資料保護程序

- 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

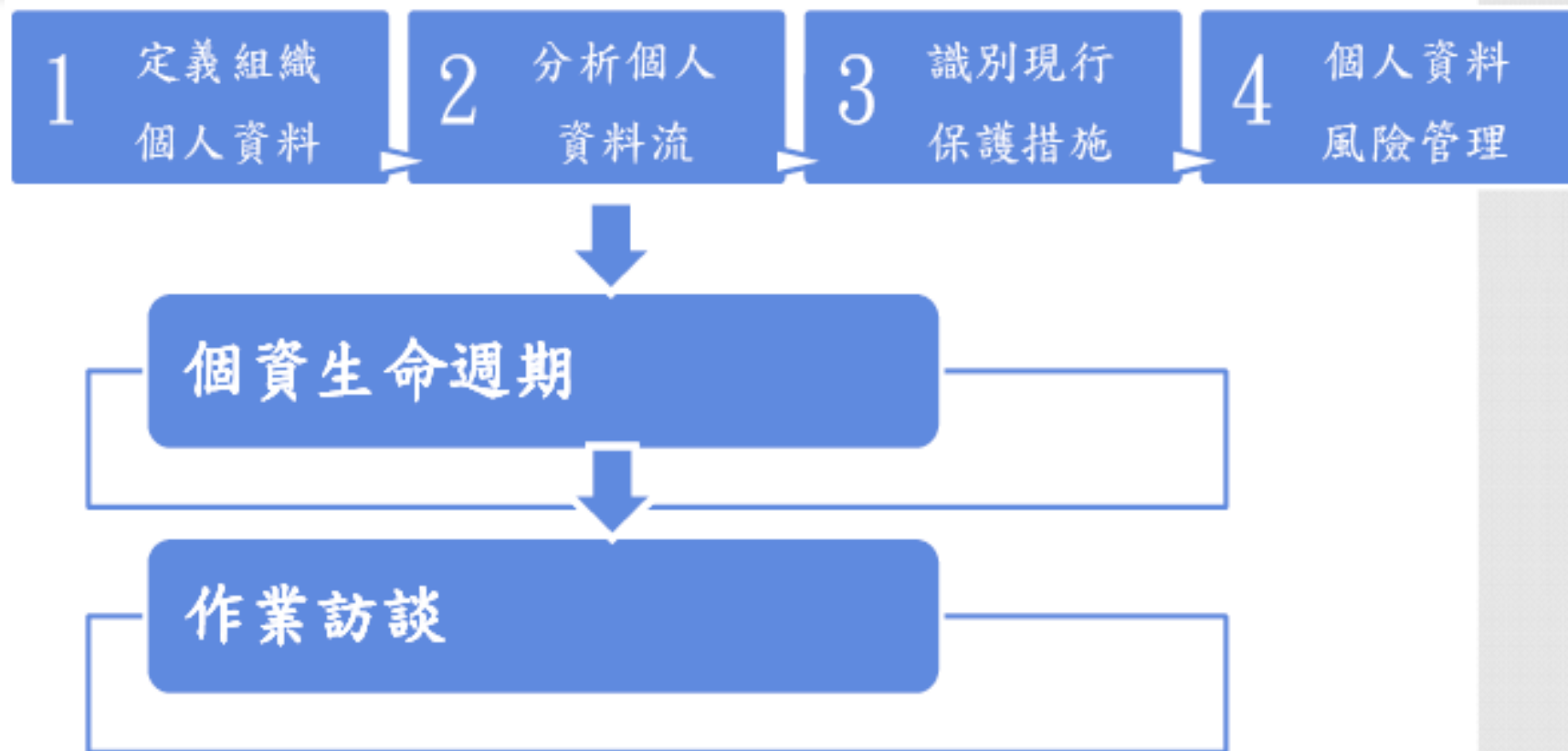
◆ 範例：公務機關「邀請專家學者出席會議請領車馬費作業」



- 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



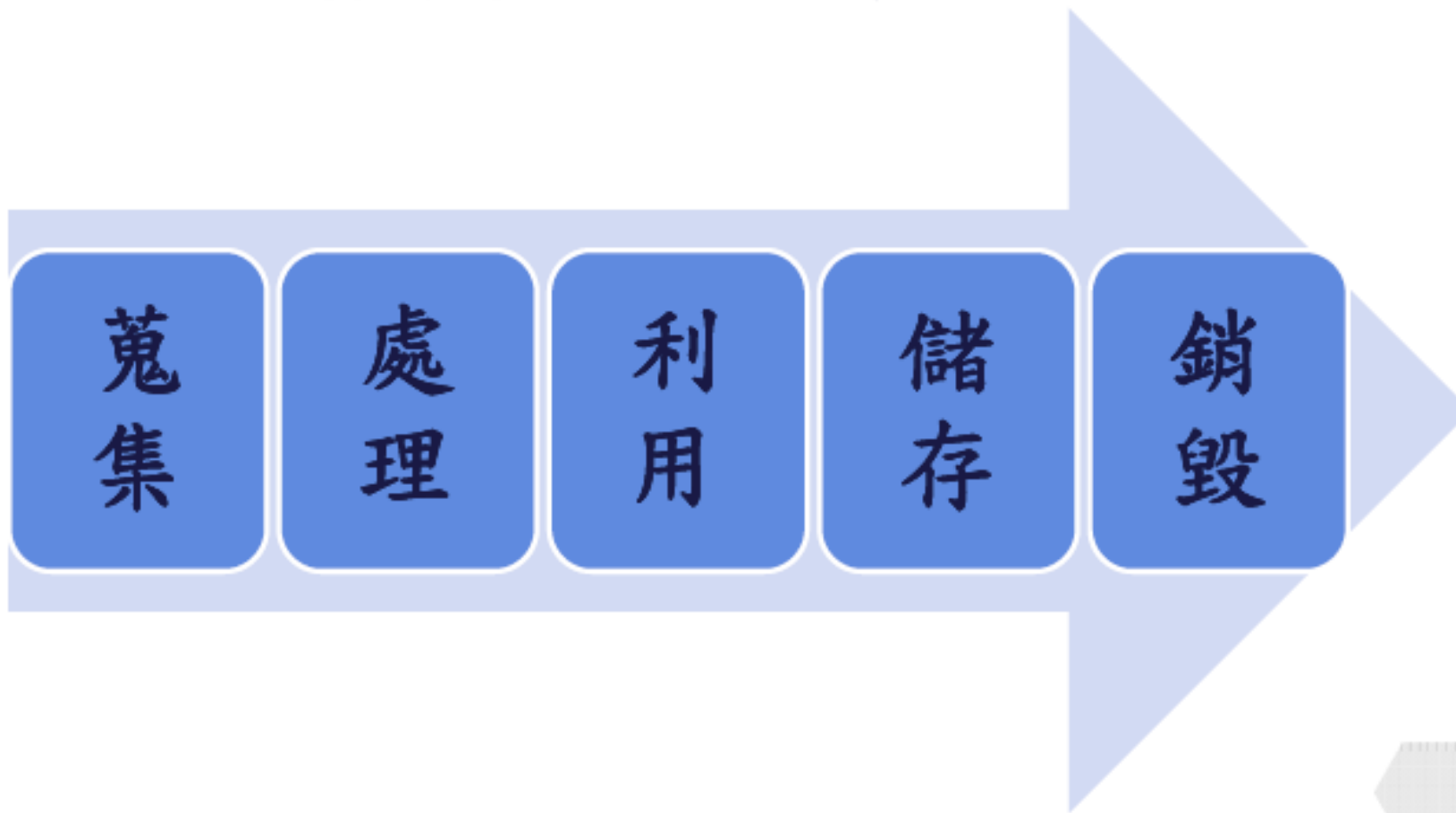
個人資料保護程序





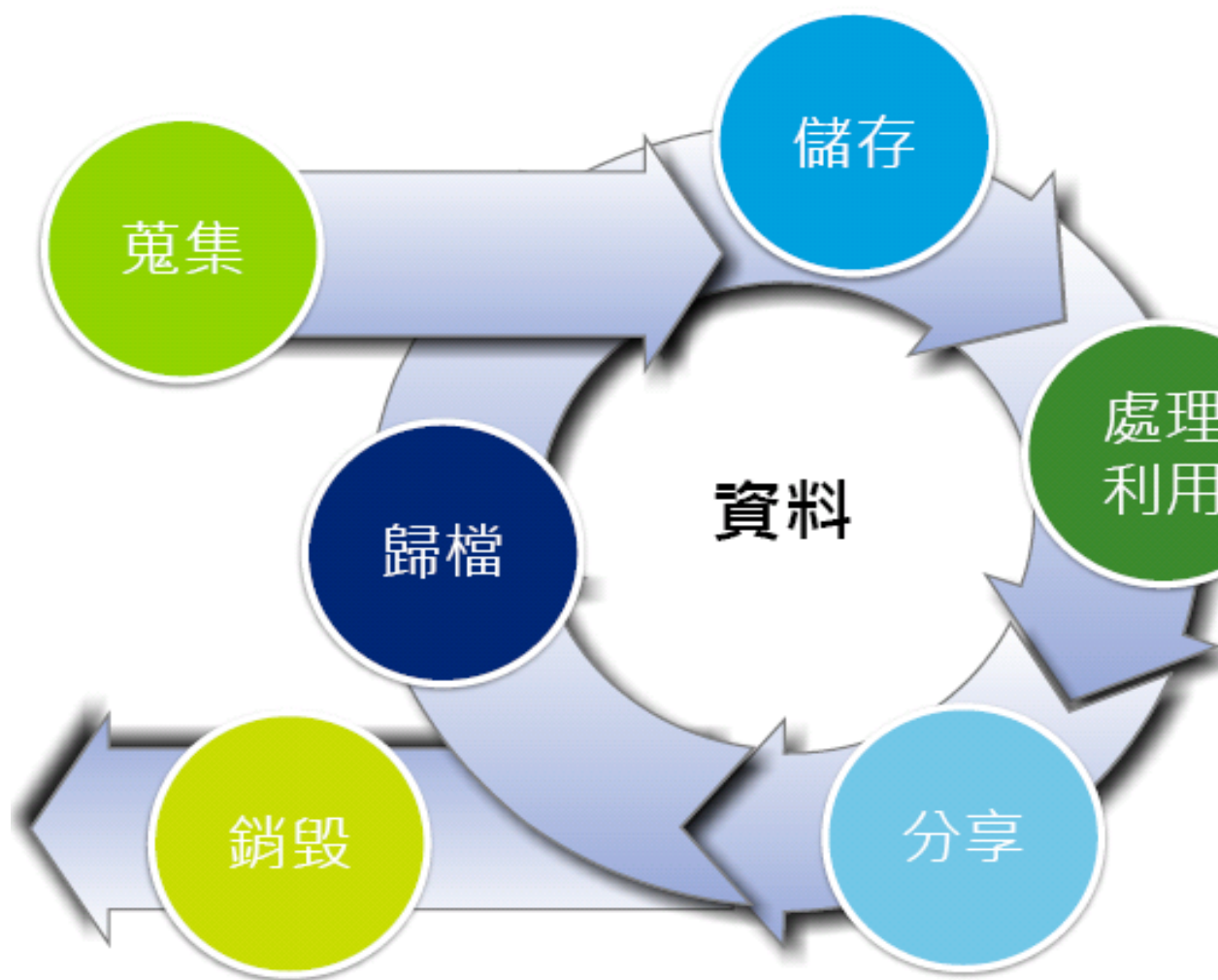
分析個人資料流

◆ 個人資料處理階段之生命週期：





分析個人資料流



蒐集

- 指以**任何方式取得**個人資料

處理/ 利用

- 處理：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：指將蒐集之個人資料為處理以外之使用。

分享

- 委託蒐集、處理或利用個人資料者，視同委託機構。
- 委託人**應對受託人為適當之監督**。

銷毀

- 個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。



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？

單位名稱：

填表日期： 年 月 日

編號	業務流程	個人資料檔案名稱	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	個資存放位置	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		
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個資範圍
1	人事管理	約聘人員契約書	約聘人員考核及服務要點	002 人事管理	C001 C003 C031 C061 C068	姓名、地址、身分證統一編號、工作職稱、工作項目、契約期間、薪水	☒ 資料庫 ☐ 數位 ☒ 紙本	☐ 是 ☒ 否	辦公室 鐵櫃 承辦人 個人電腦	各單位核准公文、呈或續聘申請表	☐ 直接 ☒ 間接	人事室	建檔及異動維護管理	人事室	聘任期間	台灣	人事室	人員行政管理	人事室	業務存續期間	電子檔刪除、紙本碎紙	業務終止後銷毀	無	無	無



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？

單位名稱：

填表日期： 年 月 日

編號	業務流程	個人資料檔案名稱	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	個資存放位置	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			
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個資範圍
1	人事管理	約聘人員契約書	約聘人員考核及服務要點	002 人事管理	C001 C003 C031 C061 C068	姓名、地址、身分證統一編號、工作職稱、工作項目、契約期間、薪水	■資料庫 □數位 ■紙本	□是 ■否	辦公室 鐵櫃 承辦人 個人電腦	各單位核准公文、簽呈或續聘申請表	□直接 ■間接	人事室	建檔及異動維護管理	人事室	聘任期間	台灣	人事室	人員行政管理	人事室	業務存續期間	電子檔刪除、紙本碎紙	業務終止後銷毀	無	無	無



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

單位名稱：

填表日期： 年 月 日

編號	業務流程	個人資料檔案名稱	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	資料形式	有否將特殊資料？何種特殊資料？	個人資料位置	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					
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個人資料範圍
1	人事管理	約聘人員契約書	約聘人員考核及服務要點	002 人事管理	C001 C003 C031 C061 C068	姓名、地址、身分證統一編號、工作職稱、工作項目、契約期間、薪水	☒ 資料庫 ☐ 數位 ☒ 紙本	☐ 是 ☒ 否	辦公室 鐵櫃 承辦人 個人電腦	各單位核准公文、簽呈或續聘申請表	☐ 直接 ☒ 間接	人事室	建檔及異動維護管理	人事室	聘任期間	台灣	人事室	人員行政管理	人事室	業務存續期間	電子檔刪除、紙本碎紙	業務終止後銷毀	無	無	無



分析個人資料流

單位名稱：

填表日期： 年 月 日

編號	業務流程	個人資料檔案名稱	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	個資存放位置	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					
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個資範圍
1	人事管理	約聘人員契約書	約聘人員考核及服務要點	002 人事管理	C001 C003 C031 C061 C068	姓名、地址、身分證統一編號、工作職稱、工作項目、契約期間、薪水	☒ 資料庫 ☐ 數位 ☒ 紙本	☐ 是 ☒ 否	辦公室 鐵櫃 承辦人 個人電腦	各單位核准公文、簽呈或續聘申請表	☐ 直接 ☒ 間接	人事室	建檔及異動維護管理	人事室	聘任期間	台灣	人事室	人員行政管理	人事室	業務存續期間	電子檔刪除、紙本碎紙	業務終止後銷毀	無	無	無



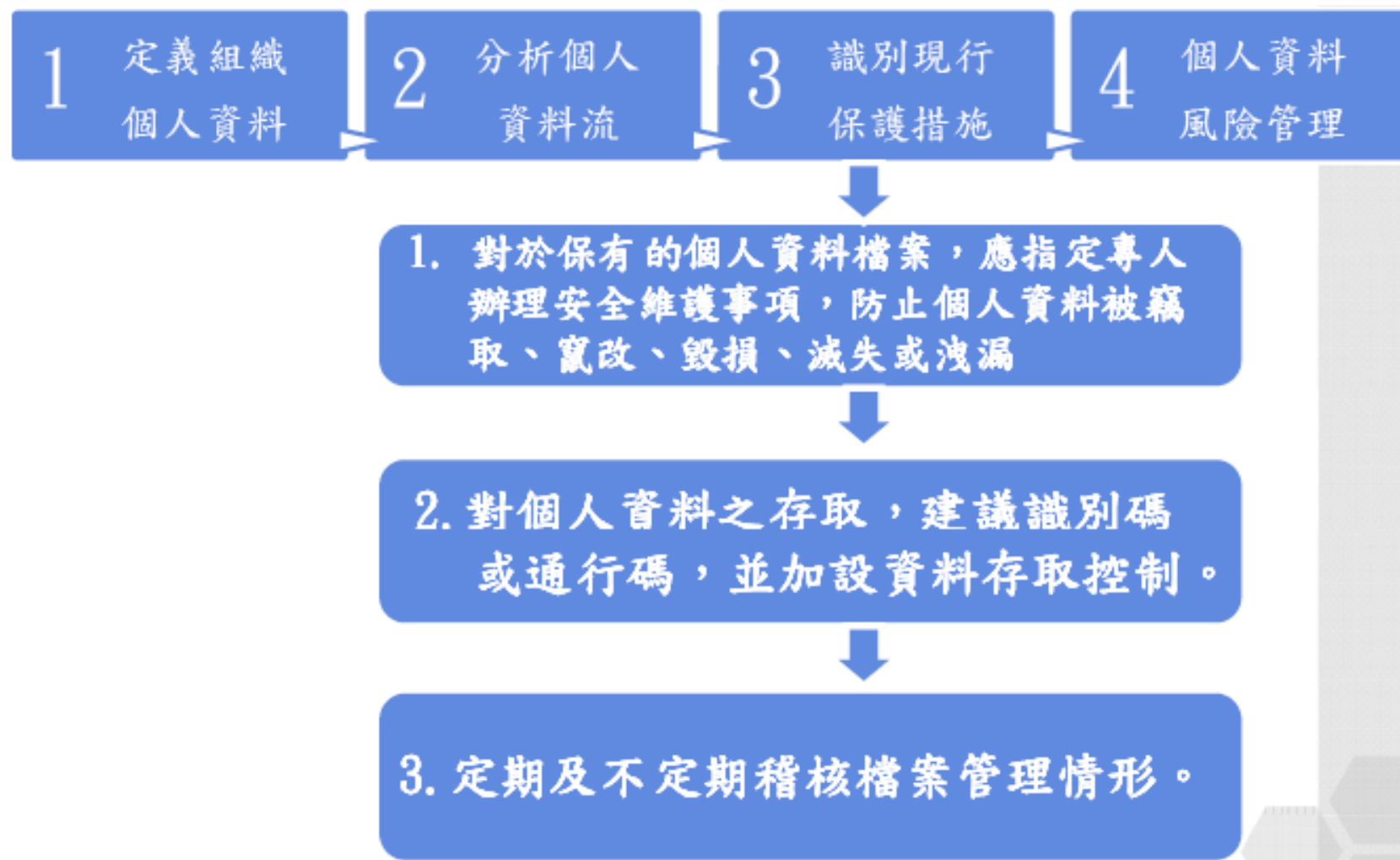
分析個人資料流

◆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

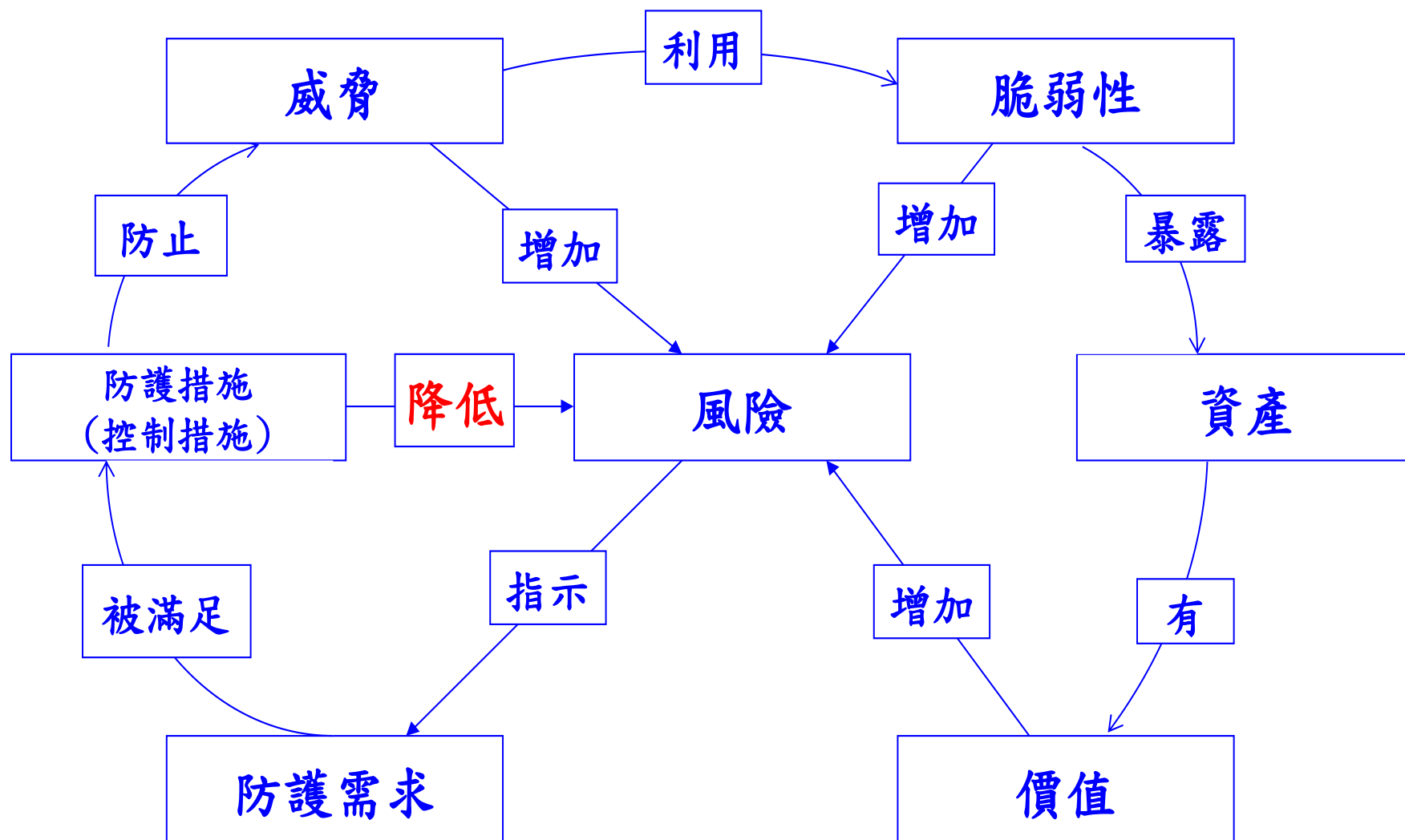




三、資訊資產分類原則

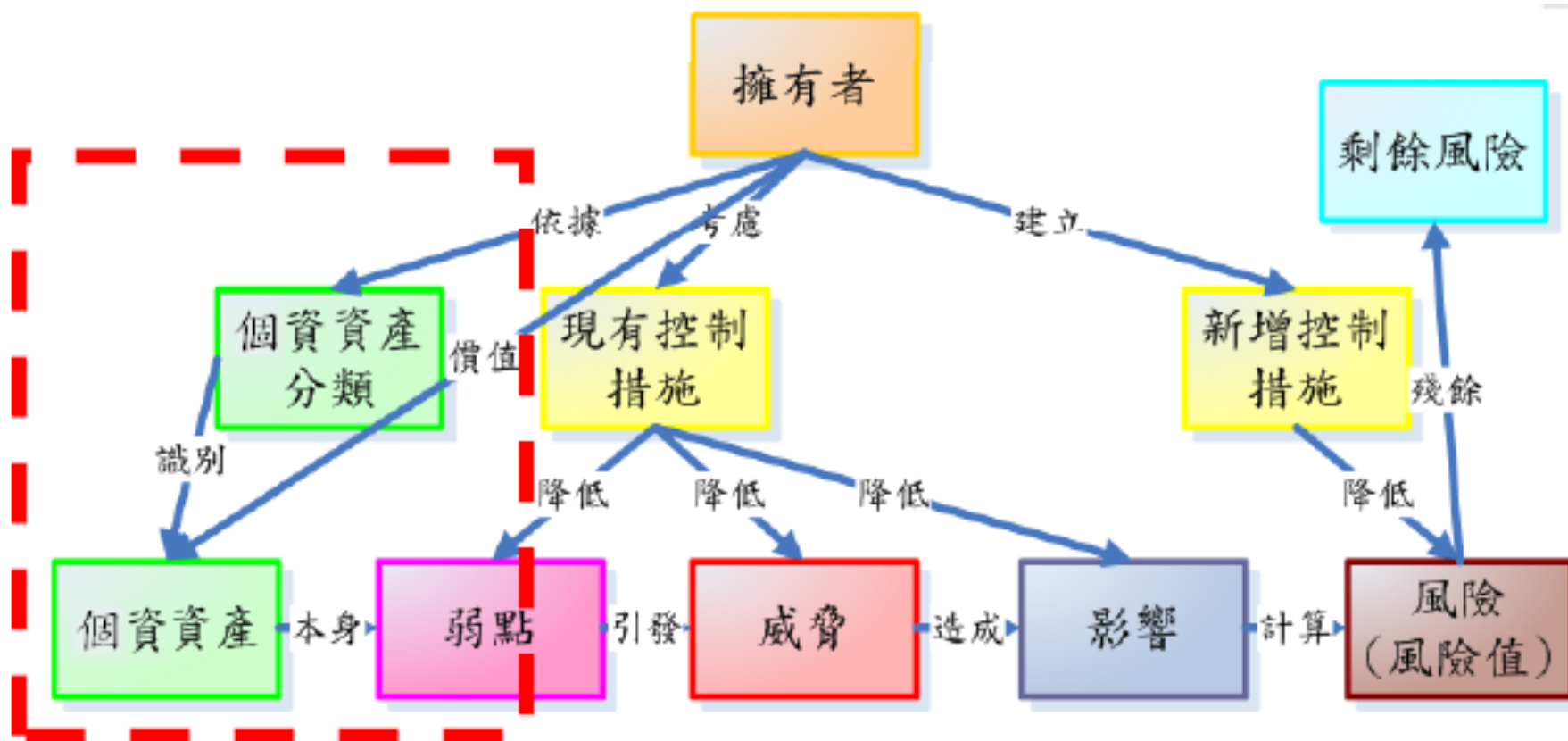


建立個資資產原則





建立個資資產原則





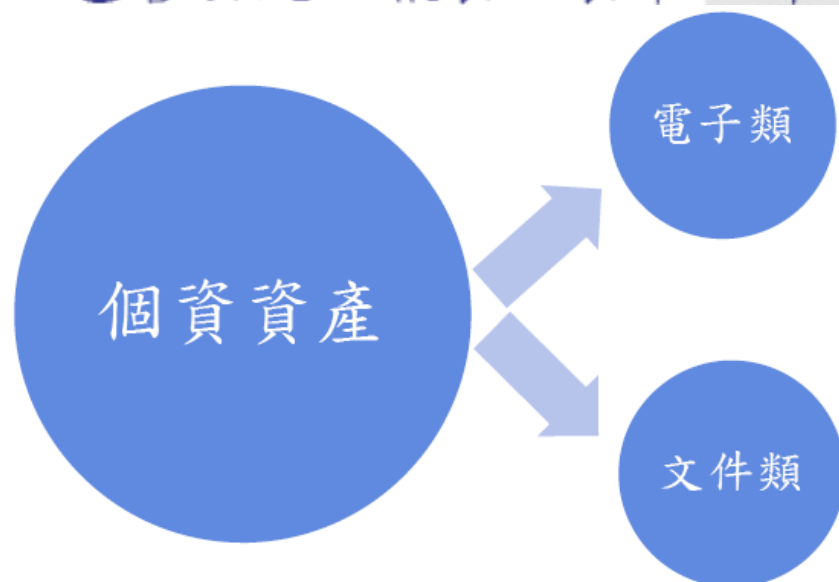
個資資產分類

◆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。





四、建立個資資產清冊



個人資料風險管理程序

作業流程	權責單位	相關文件
鑑別個資檔案	各單位個人資料保護專責人員	<u>個資項目盤點表</u>
鑑別個資檔案風險	各單位個人資料保護專責人員	<u>個資檔案風險評估彙整表</u>
撰寫風險評估報告	各單位個人資料保護專責人員	<u>個資檔案風險評估彙整表</u> <u>個資檔案風險評估報告</u>
確認核估結果	單位主管	<u>個資檔案風險評估報告</u>
個資風險處理	各單位個人資料保護專責人員	<u>個資檔案風險處理計畫</u>
確認處理結果	單位主管	<u>個資檔案風險處理計畫</u>
紀錄保存	各單位個人資料保護專責人員	



個人資料盤點

- ◆ 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

單位名稱：

填表日期： 年 月 日

編號	業務流程	個人資料檔案名稱	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	個資存放位置	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		
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	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	依據法令法規或內部規定	個資法特定目的之項目	個人資料類別之代號	個資表單或檔案之欄位	紙本或(及)數位或(及)資料庫	是否含有病歷、醫療、基因、性生活、健康檢查、犯罪前科	個人資料存放位置(數位及實體)	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	個資利用單位	個資利用之方式及目的	個資保存單位	個資保存期限	個資銷毀方式	個資銷毀頻率	個資揭露方式	個資揭露方式與目的	個資揭露的範圍



個資資產清冊

單位名稱：

填表日期： 年 月 日

編號	業務流程	個人資料檔案名稱	法律依據或內部規定	特定目的	個人資料類別	個人資料之範圍	資料形式	有否特種資料？何種特種資料？	個資存放位置	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		
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個資範圍
1	人事管理	約聘人員契約書	約聘人員考核及服務要點	002 人事管理	C001 C003 C031 C061 C068	姓名、地址、身分證統一編號、工作職稱、工作項目、契約期間、薪水	☒ 資料庫 ☐ 數位 ☒ 紙本	☐ 是 ☒ 否	辦公室 鐵櫃 承辦人 個人電腦	各單位核准公文、簽呈或續聘申請表	☐ 直接 ☒ 間接	人事室	建檔及異動維護管理	人事室	聘任期間	台灣	人事室	人員行政管理	人事室	業務存續期間	電子檔刪除、紙本碎紙	業務終止後銷毀	無	無	無



五、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

- 隱私權衝擊分析流程：
 - 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：

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	個人資料查詢困難，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 <u>直接</u> 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21~2,000筆	一般個資20,001筆以上 特種個資2,001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)	除識別資料外，還含有個人活動資料或財務金融資料	含有特種個人資料 (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資	有特定目的外利用個資，但符合例外條款	有特定目的外利用個資，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，等級判定依據個資法之相關要求訂定，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。



- 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「風險發生可能性等級」評估標準，如：

等級	可能性	發生機率	描述
3(高)	幾乎確定	61-100%	在大部分的情況下會發生
2(中)	有可能	41-60%	有些情況下會發生
1(低)	幾乎不可能	0-40%	只會在特殊的情況下發生



個資隱私衝擊分析(續)

- 以個資法之要求對組織個資作業之衝擊進行評估分析
 – 對應「風險分布矩陣」判斷風險分布情況：

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)



個資隱私衝擊分析(續)

- 以個資法之要求對組織個資作業之衝擊進行評估分析
– 決定可接受風險值：

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



個資隱私衝擊分析-範例

個資盤點表

盤點列表

• 106年度

105年度

104年度

新增盤點表

風險等級判定

風險等級判定列表

• 106年度

105年度

104年度

新增盤點表

風險評估表列印

個資項目盤點表

首頁 > 個資盤點表 > 個資項目盤點表

編號	個資檔案名稱	保有依據	特定目的	個資類別	個人資料範圍	資料形式	風險評估	刪除
1	人事基本資料	人事資料管理要點	002 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)	CO00-三 CO03-三 CO31-三 CO六八 CO六八	姓名 職稱 地址 身分證字號 學歷 服務單位/機關 其他	紙本 資料庫	評估	刪除

個資風險評估彙整表

首頁 > 個資風險等級判定

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	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	人事基本資料	第一次評鑑	3	2	2	2	1	1	3	2	6	3	存取權限控管/實體安全控管(存放於鐵櫃中)
		風險再評鑑											



個資隱私衝擊分析-範例(續)

風險處理計畫

處理計畫列表

• 106年度

105年度

104年度

新增盤點表

處理計畫列印

匯出資料

個資風險處理計畫

首頁 > 個資風險處理計畫 > 列表

資產識別風險說明					風險處理措施		風險進度追蹤							
編號	個資檔案名稱	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	實際完成日	覆核人員	處理結果	未完成原因	編輯	評鑑
1	人事基本資料	1.未落實鐵櫃上鎖控管機制，造成資料外洩。 2.未定期執行權限審查，易發生非授權存取。	6	3	降低風險	1.每年定期執行存取權限審查，確保非授權存取。2.落實鐵櫃上鎖，保護資料安全。	Chen	2016-06-30	2016-06-30	project	已完成		編輯	再評估

風險等級判定

風險等級判定列表

• 106年度

105年度

104年度

新增盤點表

風險評估表列印

匯出資料

個資風險評估彙整表

首頁 > 個資風險等級判定

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	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	人事基本資料	第一次評鑑	3	2	2	2	1	1	3	2	6	3	存取權限控管/實體安全控管(存放於鐵櫃中)
		風險再評鑑	3	2	2	1	1	1	3	1	3	2	存取權限控管/實體安全控管(存放於鐵櫃中)



範例-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權衝擊分析
- ◆ 作業流程：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：_____

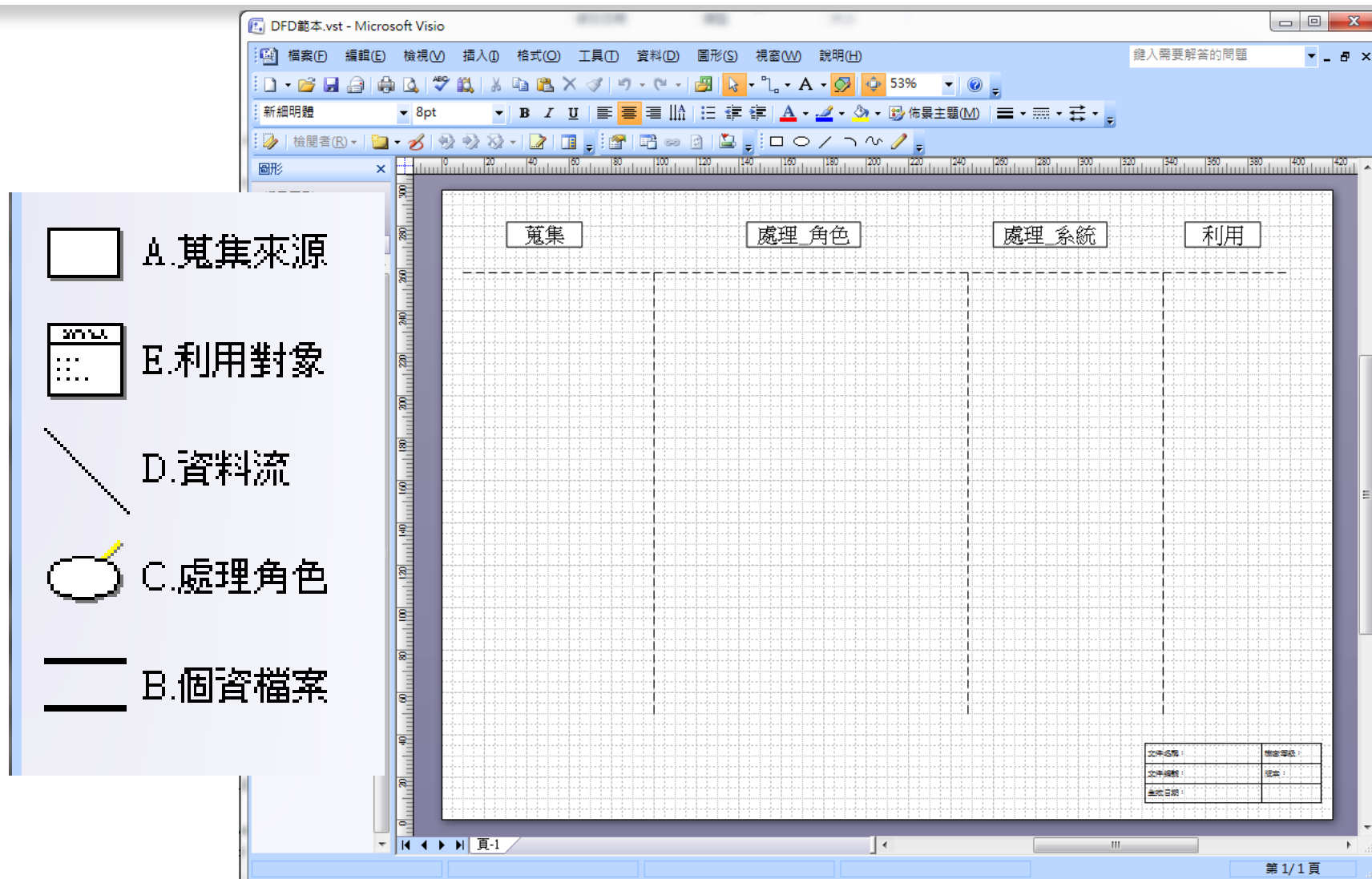
身分證字號：_____

研討會簽到表

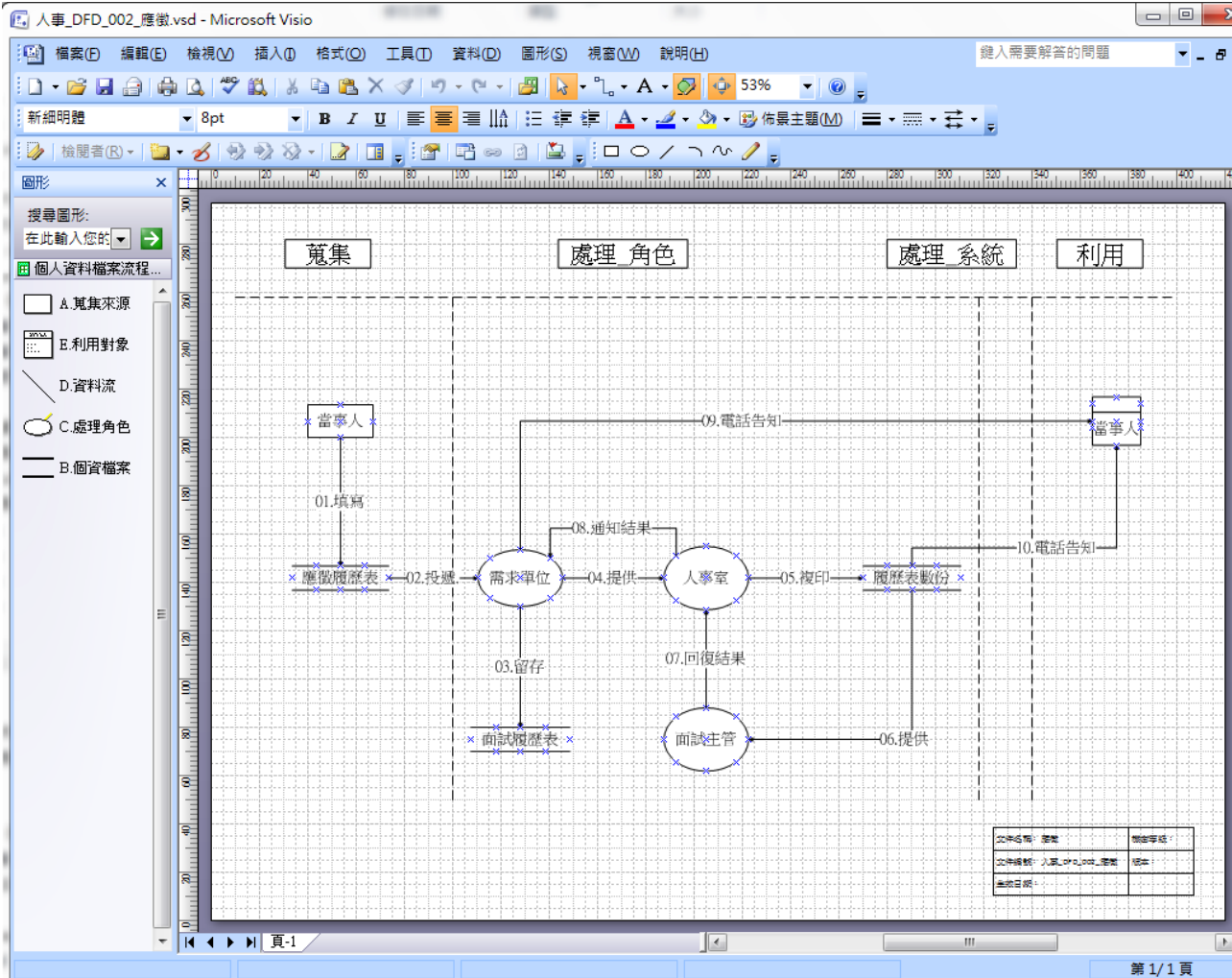
姓名	部門	職稱



資料流程圖樣板



繪圖結合匯出報告功能



	A.蒐集來源	當事人
總數	1	
	B.個資檔案	面試履歷表
	B.個資檔案	履歷表數份
	B.個資檔案	應徵履歷表
總數	3	
	C.處理角色	人事室
	C.處理角色	面試主管
	C.處理角色	需求單位
總數	3	
	D.資料流	01.填寫
	D.資料流	02.投遞
	D.資料流	03.留存
	D.資料流	04.提供
	D.資料流	05.複印
	D.資料流	06.提供
	D.資料流	07.回復結果
	D.資料流	08.通知結果
	D.資料流	09.電話告知
	D.資料流	10.電話告知
總數	10	
	E.利用對象	當事人
總數	1	



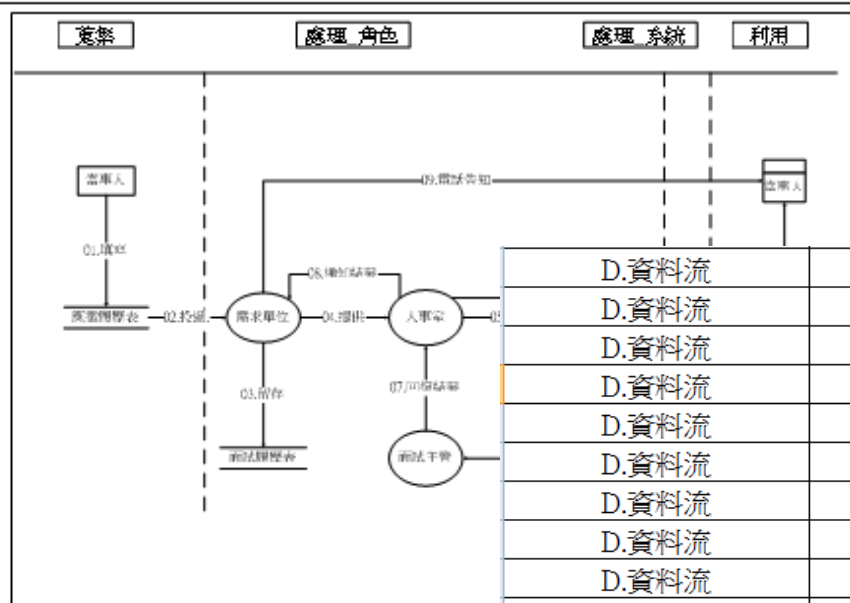
產製個人資料流程表

中國科技大學

個人資料流程表

單位名稱：	人事	組別名稱：	
流程名稱：	應徵	序號：	DFD_002
版本：		機密等級：	
資料時間：		生效日期：	
填表人：		連絡電話：	
E-mail：			

資料流程圖



D.資料流	01.填寫	當事人填寫履歷表	
D.資料流	02.投遞	由當事人投遞給需求單位	
D.資料流	03.留存	需求單位留存副本	
D.資料流	04.提供	需求單位將履歷表提供給人事室	
D.資料流	05.複印	人事室複印履歷表數份	
D.資料流	06.提供	提供給面試主管	
D.資料流	07.回復結果	面試主管回復審核結果給人事室	
D.資料流	08.通知結果	人事室通知結果給需求單位	
D.資料流	09.電話告知	需求單位電話通知當事人	
D.資料流	10.電話告知	人事室亦會電話通知當事人	
10			小計



Q&A 問題與討論

～如有任何問題・歡迎隨時來電詢問～

SafeLink

博創資訊科技股份有限公司

臺中市西屯區國安一路208巷6號

TEL : 886-4-25250535

FAX : 886-4-24615268

<http://www.safelink.com.tw/>

E-mail: sam@safelink.com.tw

