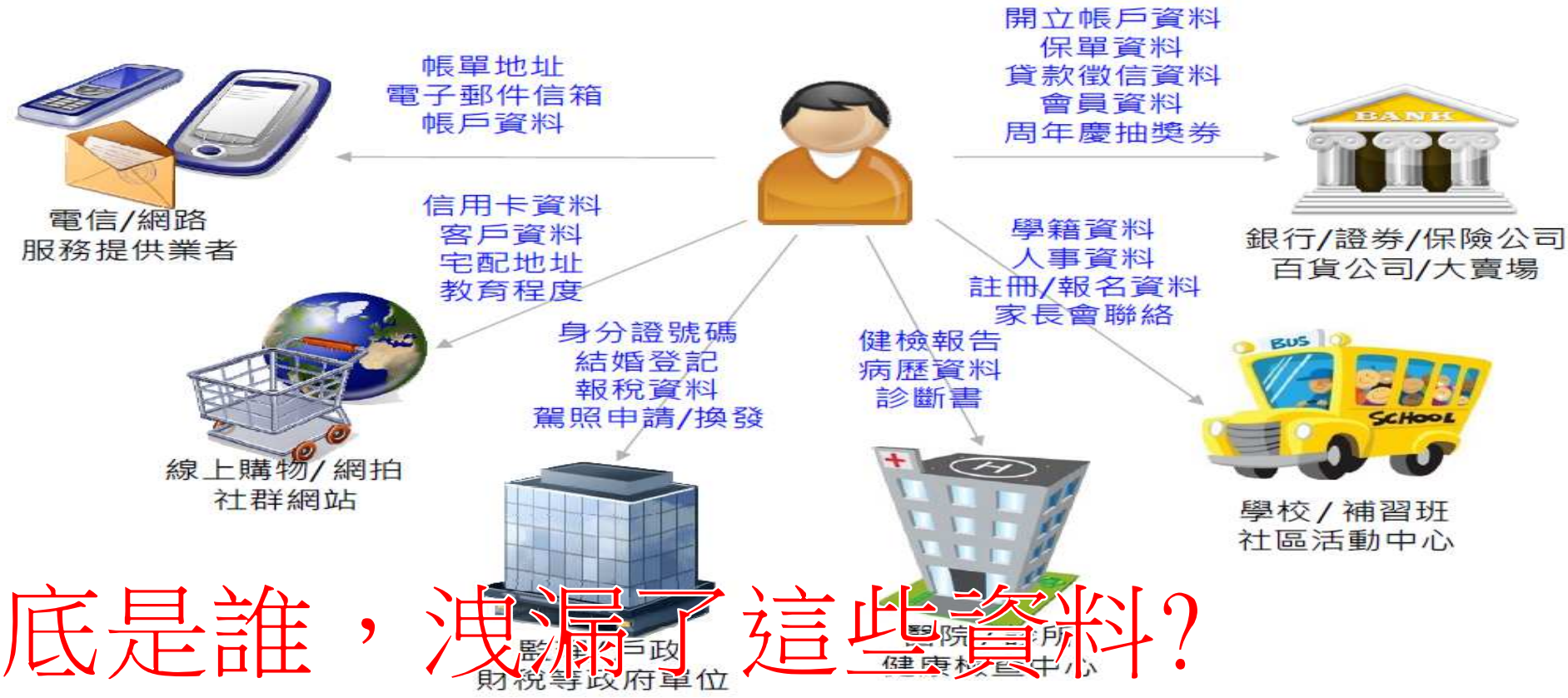
個資保護與隱私鑑別

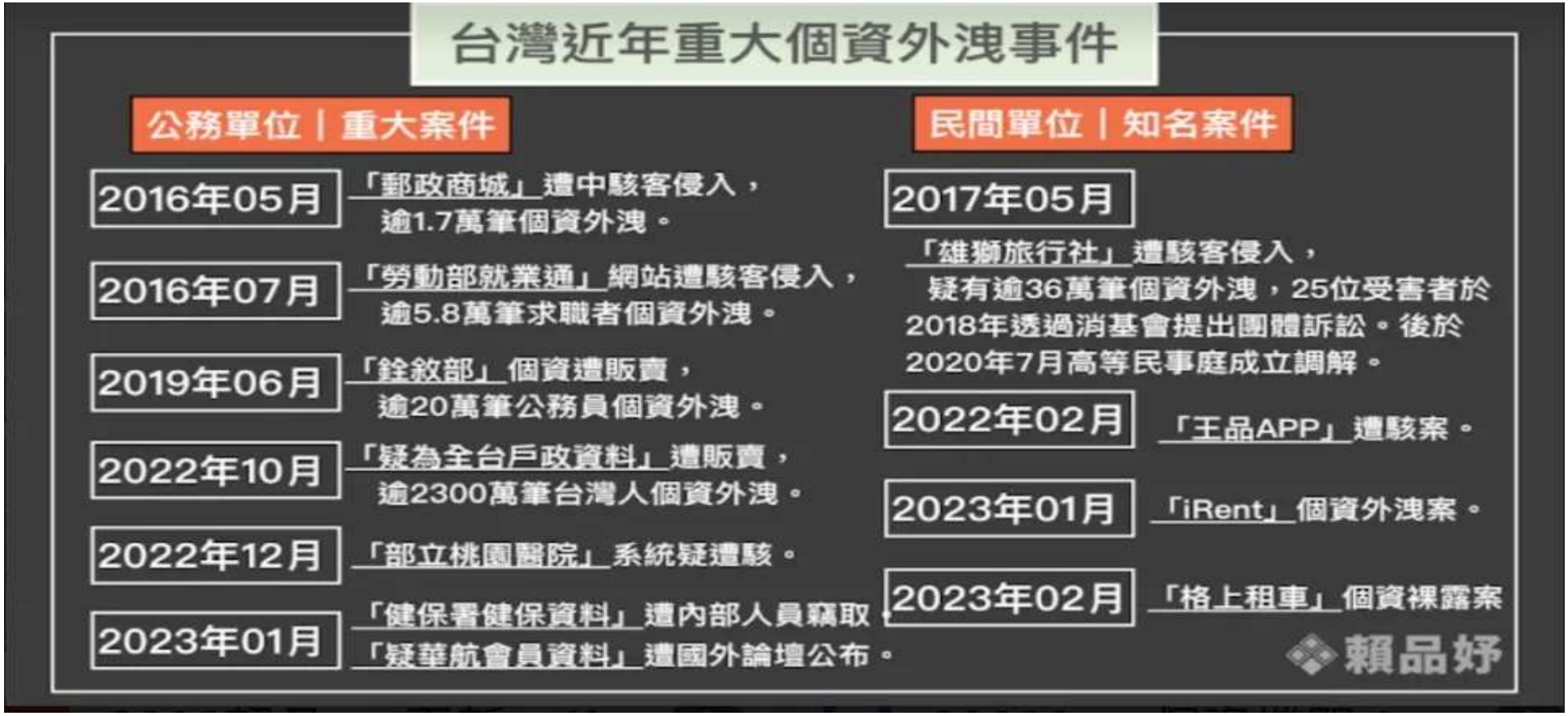
橙言有限公司 資安暨個資輔導顧問師 洪明賢 112.12.6

個人資料無所不在，個資事件層出不窮



到底是誰，洩漏了這些資料?

層出不窮的個資外洩事件(I)



層出不窮的個資外洩事件(II)

歷年公務機關個資外洩事件表

時間	事件內容
2023年1月	華航會員資料庫遭駭，國外論壇公布會員資料，包含賴清德、張忠謀、林志玲等人。
2023年1月	健保署前主秘葉逢明、現任承保組科長謝玉蓮、職員李仁輝三人，疑竊取民眾及11情治單位健保資料長達13年，遭調查局偵訊。
2022年12月	部立桃園醫院遭爆採用中國醫療資訊系統(內有簡體中文附註的程式碼)，自2020年8月起遭駭，竊取個資與醫護資料，部桃新聞稿稱案發後即請資安公司鑑識，僅有一台主機資料遭竊，且內無個資。
2022年10月	戶政資料遭駭，並在外國論壇公開兜售，疑為2,357萬餘筆。
2020年5月	美國資安公司Cyble 在暗網發現外洩資料庫，內容稱是全臺戶籍資料，包含超過2千萬筆民眾個資，資料庫來源是內政部戶政司。
2019年6月	銓敘部爆發公務人員個資被置於國外論壇販賣案，外洩資料內含國安局等機敏機關，超過20萬筆公務員資料。
2016年7月	勞動部勞發署發現所屬之「台灣就業通」網站，遭民間債務催收公司駭入，竊取5萬8千多筆求職民眾個資，以賺取催收債務傭金。
2016年5月	中華郵政商城因網站漏洞遭中國駭客侵入，逾1.7萬筆的交易資料遭竊

近年民間公司團體個資外洩案例

公司	時間	事件	後續	主管機關
和雲(iRent)	2023年2月	外媒報導國外資安人員在和泰雲端伺服器發現資料庫，內有iRent 約14萬會員全名、手機號碼、Email、信用卡等訊息	● 2/1，和泰車發布重大訊息 ● 2/1，公路總局調查 ● 2/4，和雲聲明會員資料未遭盜用並提出慰問方案	交通部公路總局
博客來	2022年第二季	刑事局統計博客來個資外洩，接獲民眾通報遭詐騙全年達3,773件。	● 官網加註反詐騙宣導警語、發送反詐騙宣導簡訊	經濟部商業司
網軟	2021年7月	至少 35 個愛心協會及社福團體，因委託之資訊服務商網軟遭駭，導致大批捐款個資外洩	刑事局接獲捐款民眾報案，調查後披露此事。	衛福部
誠品生活	2021年4月	「誠品線上」會員個資外洩，遭詐騙集團假冒誠品解除分期付款，刑事局統計全年反詐通報達940件。	● 未發布重大訊息	經濟部商業司
人力銀行	2020年10月	104約592萬筆、1111約有335萬筆求職者個資被放在中國暗網論壇販售。	104：報調查局偵查 1111：報刑事局偵查	勞動部

整理自媒體報導

個資外洩事件根因-I

■對網路高依賴性

- 社群軟體好友聯繫
- 通訊軟體公務私訊
- 影音下載收看
- 生活資訊查詢

個資外洩事件根因-II

- 惡意/山寨APP
- 誤入釣魚網站及金融詐騙陷阱
- 社群隱私缺乏防護
- 單一密碼走天下
- 個資網路大公開

個資外洩事件根因-III

- **無心之過更加難以防範：**
  - 資料外洩的因素，超過一半來自外部的攻擊，然而，企業員工因操作不當、採用錯誤設定等因素，無意間產生的意外事件數量，也創下最近5年來的新高，占所有事件的34%。
  - 由於這樣的失誤，不像刻意發動攻擊的資料竊取事件，可能會出現某些徵兆，尚且有跡可循，相較之下，意外事件更加難以預防。

個資外洩對全球造成的衝擊

2018 是人類歷史上資料外洩最嚴重的一年，全球遭外洩個資已高達 17 億筆，造成的損失金額約台幣 1.2 億起跳
造成個資外洩的手法以帳密填充、帳密竊取以及網路釣魚大宗。除此之外，針對路由器漏洞的攻擊、跨平台惡意程式攻擊、 API 濫用，以及假冒行動應用程式也助長個資外洩。」

個人資料鑑別

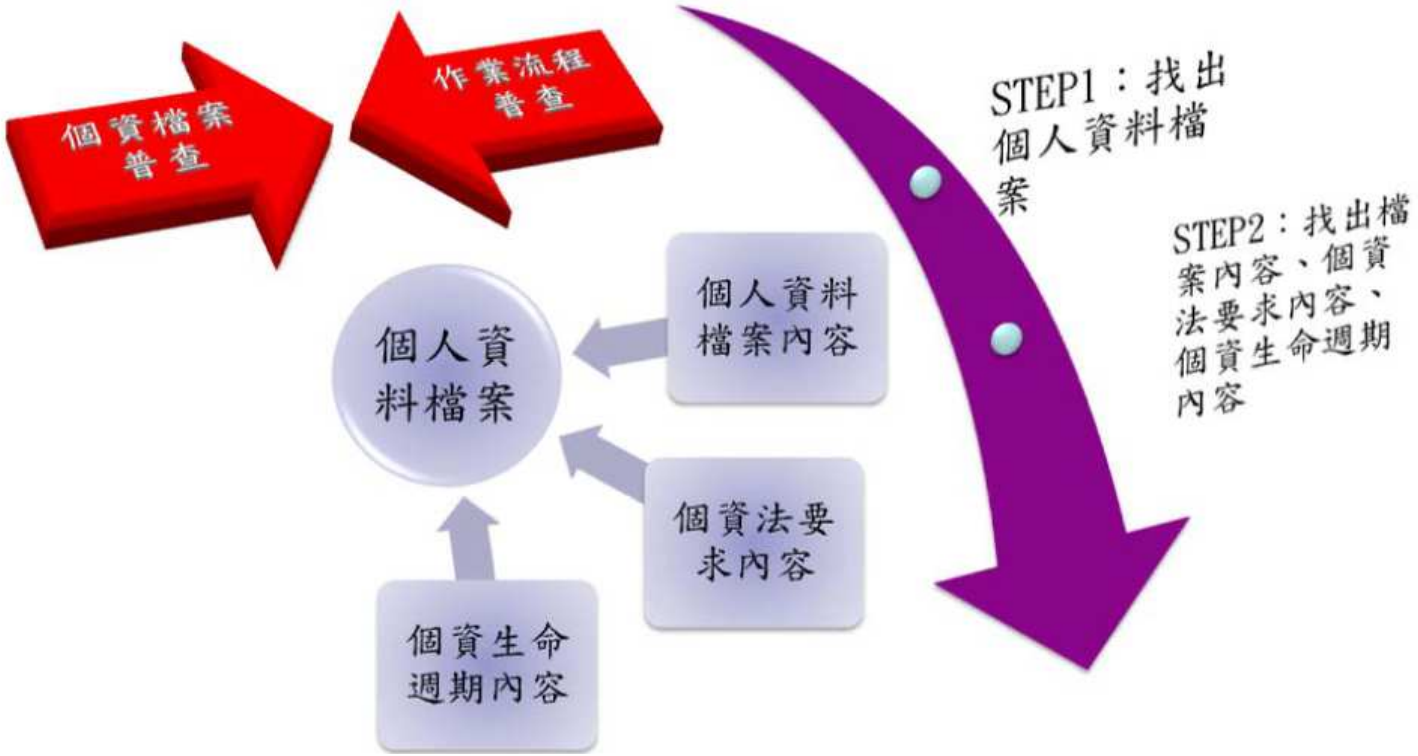
個人資料盤點是什麼

◆透過清查與個人資料有關之表單、記錄，歸納出個人資料檔案（盤點）清冊。

為什麼要做個人資料盤點

- 了解機關內部所保有之個人資料檔案
- 界定要納入管理措施的個人資料檔案
- 確認目前所保有之個人資料之適法性
- 確認風險評鑑措施的標的
- 確認當事人權利行使的標的
- 個資法第18條：公務機關應公開其保有之個人資料檔案

如何進行個人資料盤點


個資檔案普查
作業流程普查
STEP1：找出個人資料檔案
STEP2：找出檔案內容、個資法要求內容、個資生命週期內容
個人資料檔案
個人資料檔案內容
個資法要求內容
個資生命週期內容

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**。

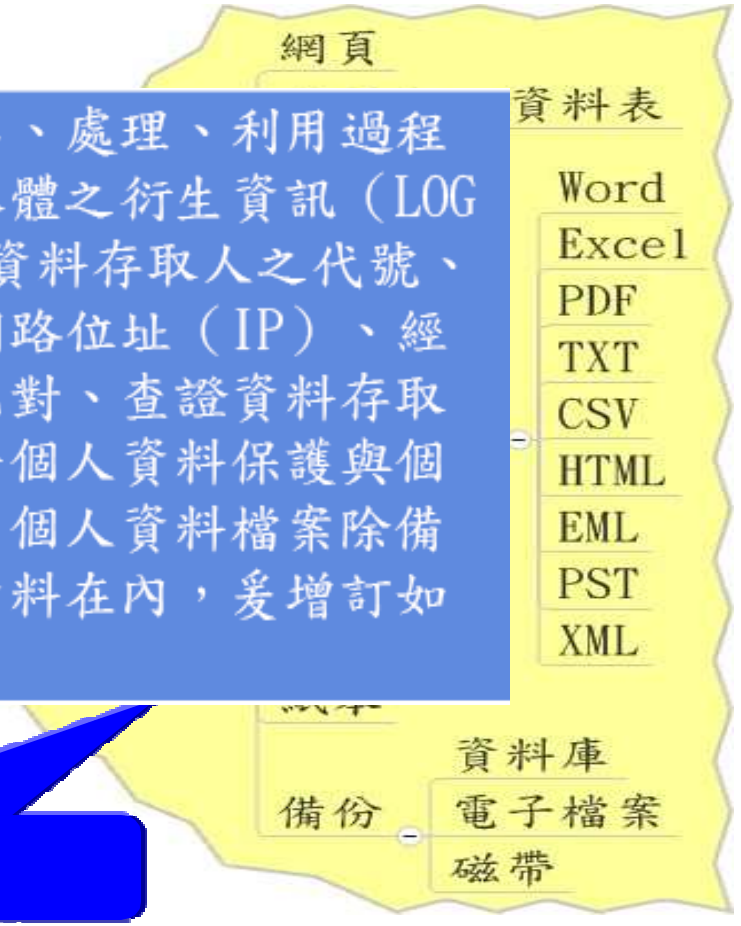
個人資料流之重要性

- **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**：指由一段去氧核醣核酸構成，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機
方　式
人資料
- 施行
細 條
第
檔案資
軌跡
- 注意**軌跡資料**可能之
衝 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。



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
金融帳號、財務狀況
金融
學生學籍資料、成績、教職員資料
教育
商業行銷
檢健療醫
病歷、健康檢查記錄
通訊、網路
電信帳單、網路會員資料
利福會社
身心障礙別、醫療證明
戶政地政
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保護直接加在資料本身。

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)。

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

- 1. 個人資料
  - §2現生存之自然人
  - 例示
  - 非例示
    - 定義：得以直接或間接方式識別該個人之資料
    - 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

•有沒有不受個資法保護的資料？

個人資料體檢步驟一：清點個人資料

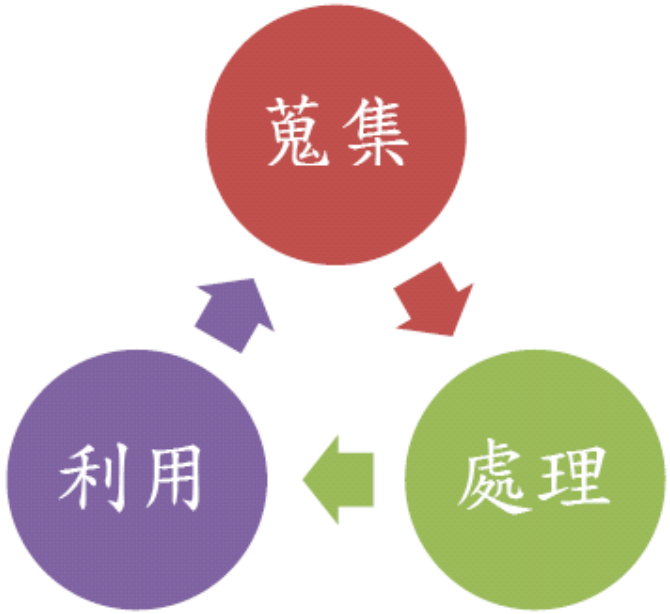
- **電子郵件**
  - **只有E-mail算不算是個人資料??**
  - 機關將收集他人電子郵遞住址(E-mail)資料提供他人查詢服務，如其**並未與自然人之姓名等相結合，尚不足以識別該個人者**，則該資料即非上 開規定所稱之個人資料，並無電腦處理個人資 料保護法規定之適用。
  - 法務部94年05月06日法律決字第0940017397號

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ag年6月21日法律字第nagnn23aaa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。
  - 經當事人同意。
  - 對當事人權益無侵害。

告知之義務-直接蒐集個資

- 第 8 條 (§§16) (立法院於104年12月15日完成三讀修正)
  - 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。
    - 二、蒐集之目的。
    - 三、個人資料之類別。
    - 四、個人資料利用之期間、地區、對象及方式。
    - 五、當事人依第三條規定得行使之權利及方式。
    - 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
  - 有下列情形之一者，得免為前項之告知：
    - 一、依法律規定得免告知。(§§9)
    - 二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。(§§10、§§11)
    - 三、告知將妨害公務機關執行法定職務。(§§10)
    - 四、告知將妨害公共利益。
    - 五、當事人明知應告知之內容。
    - 六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

告知之義務-間接蒐集個資

- 第 9 條 (§§16)
  - 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。
  - 有下列情形之一者，得免為前項之告知：
    - 一、有前條第二項所列各款情形之一。
    - 二、當事人自行公開或其他已合法公開之個人資料。(§§13)
    - 三、不能向當事人或其法定代理人為告知。
    - 四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。(§§17)
    - 五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。
    - 第一項之告知，得於首次對當事人為利用時併同為之。

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
  - 本法中華民國九十九年五月二十六日修正公布 之條文施行前，非由當事人提供之個人資料， 於本法一百零四年十二月十五日修正之條文施 行後為處理或利用者，應於處理或利用前，依 第九條規定向當事人告知。(§54)

個人資料體檢步驟五：未違法蒐集、處理或利用特種資料

- 第 6 條 (立法院於104年12月15日完成三讀修正)
  - 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。但有下列情 形之一者，不在此限：
    - 一、法律明文規定。(§§9)
    - 二、公務機關執行法定職務或非公務機關履行法定　義務必要範圍內，且事前或事後有適當安全維護措 施。(§§10、§§11、§§12)
    - 三、當事人自行公開或其他已合法公開之個人資料。(§§13)
    - 四、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，且資　料經過提供者處理後或經蒐集者依其揭露方式無從 識別特定之當事人。

個人資料體檢步驟五：未違法蒐集、處理或利用特種資料

- 第 6 條 (續) (立法院於104年12月15日完成三讀修正)
  - 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
  - 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。
  - 依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

個人資料保護法修正案 2023.05.16通過

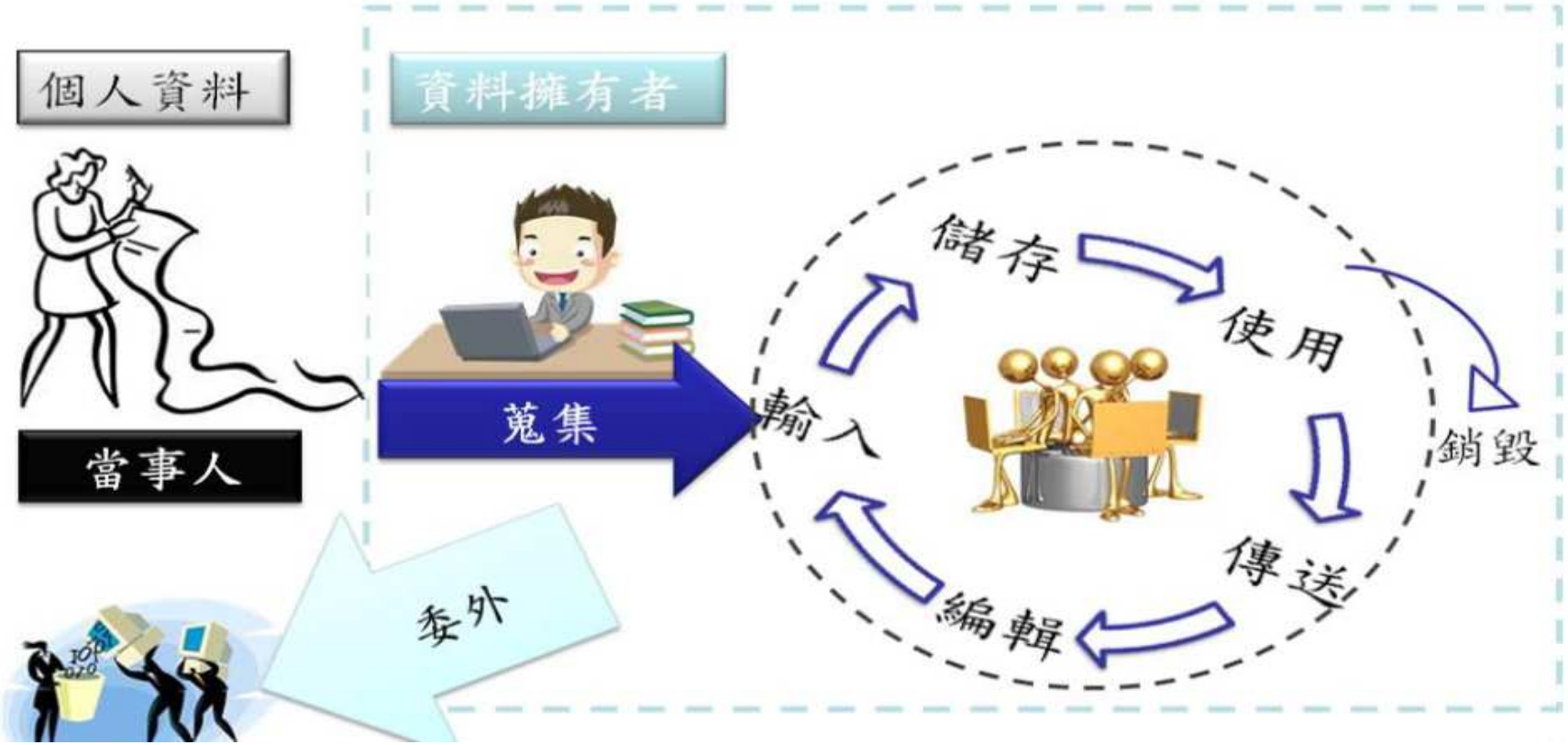
- **由「個人資料保護委員會」擔任個資法主管機關**

增訂個資法第1條之1規定，由個資保護委員會擔任個資法主管機關，呼應憲法法庭第13號判決意旨，以獨立監督機制解決目前個資法分散式管理下之實務監管問題，並與國際趨勢接軌。**(由行政院籌備)**

- **提高非公務機關違反安全維護義務的罰則**

現行個資法第48條規定，非公務機關違反安全維護義務者，中央目的事業主管機關或地方政府須先限期命其改正，屆期未改正者，方得處新臺幣2萬元至20萬元罰鍰，為督促違反安全維護義務之非公務機關儘速改善個資保護，新修正個資法第48條第2項及第3項規定，非公務機關違反安全維護義務者，中央目的事業主管機關或地方政府可直接裁處新臺幣2萬元至200萬元罰鍰，毋須先限期命其改正；屆期未改正或情節重大者，罰鍰則可提高至新臺幣15萬元至1,500萬元。

個資生命週期內容



個資生命週期內容

蒐集

以任何方式取得個人資料

處理

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

蒐集、處理、利用的對象、期間、方式為何？

個資清查盤點表

個資盤點表

單位名稱	
單位主管	
盤點人員	

編號	資料檔案名稱	保有機關名稱及聯絡方式	保有依據(法定職務)	特定目的	個人資料之類別	特種個人資料		檔案數量	資料型態	資料蒐集/處理				資料處理/利用							
										(原始+蒐集方法)or(加工+加工方法)二選一填寫				內部傳送		保管		外部傳送		廢棄	委託
						特種個資種類	法定要件(無特種個資免填)	(僅需填寫一年大約件數)		原始資料	蒐集方法	加工資料	加工方法	資料流向	傳送方式	保管方式	保存期限	資料流向	傳送方式		
1						□無 □醫療 □基因 □性生活 □健康檢查 □犯罪前科			□電子 □紙本	□直接向當事人蒐集 □間接蒐集(來源：____)	□Email □網站 □電話/現場口頭 □傳真 □紙本送達 □其他____	原始檔案/系統名稱： _____	□輸入/編輯 □輸出/列印 □影印 □掃描 □其他____		□人員親送 □Email □系統 □其他 _____	□儲存個人電腦(電子) □儲存於資料庫/主機(電子) □存放個人櫃/抽屜(紙本) □存放檔案室(紙本) □其他____	□法定保存期限 _____ □自訂保存期限 _____ □無保存期限		□人員親送 □郵寄 □傳真 □Email □其他 _____	□刪除 □碎紙銷毀 □其他	□有 □無

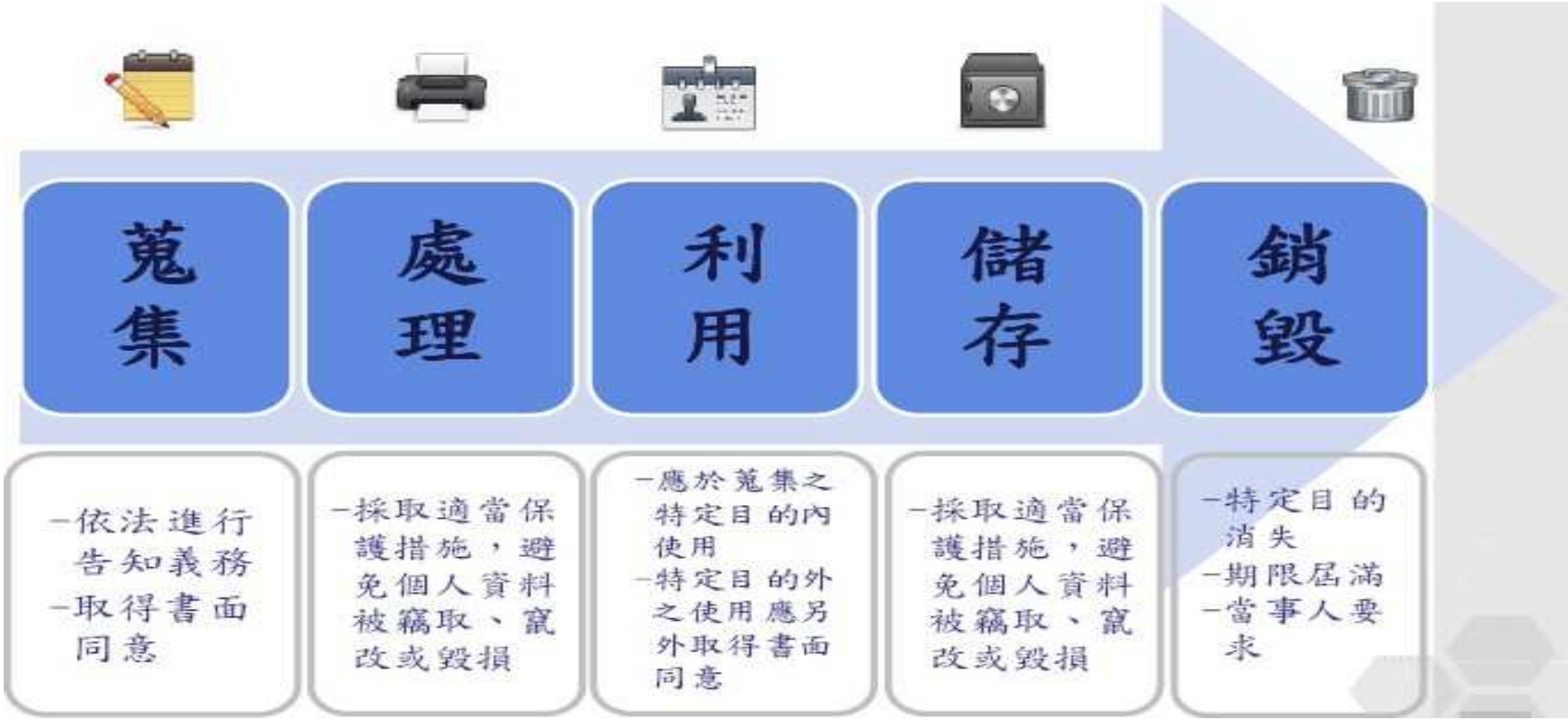
個資清查盤點表(範例)

個資盤點表(參考範例)

單位名稱	
單位主管	
盤點人員	

編號	資料檔案名稱	保有機關名稱及聯絡方式	保有依據(法定職務)	特定目的	個人資料之類別	特種個人資料		數量	資料型態	資料蒐集/處理				資料處理/利用							
										(原始+蒐集方法)or(衍生+衍生方法)二選一填寫				內部傳送		保管		外部傳送		廢棄	委託
						特種個資種類	法定要件	(僅需填寫一年大約件數)		原始資料	蒐集方法	衍生資料	衍生方法	資料流向	傳送方式	保管方式	保存期限	資料流向	傳送方式	廢棄方式	
1	僑外投資申請文件	經濟部（投審會）	外國人投資條例	044投資管理 119發照與登記	C001辨識個人者 C003政府資料中之辨識者 C032財產	■無 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	X		□電子 ■紙本	■直接向當事人蒐集 □間接蒐集(來源：__)	紙本	原始檔案/系統名稱：_____	X	組長、委員會	■人員親送 □Email □系統 □其他_____	□儲存個人電腦(電子) □儲存於資料庫/主機(電子) □存放於公務櫃(紙本) ■存放檔案室(紙本) □其他____	□法定保存期限_____ □自訂保存期限_____ ■永久保存	x	□人員親送 □郵寄 □傳真 □Email □系統 □其他_____	□刪除 □燒毀 □碎紙銷毀 ■無	■無 □有
2	僑外投資審議管理資訊資料庫	經濟部（投審會）	外國人投資條例	044投資管理 119發照與登記	C001辨識個人者 C003政府資料中之辨識者 C032財產	■無 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	X		■電子 □紙本	X	X	原始檔案/系統名稱：僑外投資申請文件檔	■輸入/編輯 □輸出/列印 □影印 □掃描 □其他____	組長、委員會	■人員親送 □Email □系統 □其他_____	□儲存個人電腦(電子) ■儲存於資料庫/主機(電子) □存放個人櫃/抽屜(紙本) □存放檔案室(紙本) □其他____	□法定保存期限_____ □自訂保存期限_____ ■永久保存	x	□人員親送 □郵寄 □傳真 □Email □系統 □其他_____	□刪除 □燒毀 □碎紙銷毀 ■無	■無 □有
3	審定投資額文件檔	經濟部（投審會）	外國人投資條例	044投資管理 119發照與登記	C001辨識個人者 C002辨識財物者 C003政府資料中之辨識者 C081收入、所得、資產與投資 C093財務交易	■無 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	X		□電子 ■紙本	■直接向當事人蒐集 □間接蒐集(來源：__)	紙本	原始檔案/系統名稱：_____	X	X	X	□儲存個人電腦(電子) □儲存於資料庫/主機(電子) □存放於公務櫃(紙本) ■存放檔案室(紙本) □其他____	□法定保存期限_____ □自訂保存期限_____ ■永久保存	x	□人員親送 □郵寄 □傳真 □Email □系統 □其他_____	□刪除 □燒毀 □碎紙銷毀 ■無	■無 □有
4	僑外投資申請文件(提供用)	經濟部（商業司）	外國人投資條例	038行政執行 039行裁罰 119發照與登記 136資(通)訊與資料庫管理	C001辨識個人者 C003政府資料中之辨識者	■無 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	X		■電子 ■紙本	X	X	原始檔案/系統名稱：僑外投資申請文件檔	■輸入/編輯 ■輸出/列印 ■影印 ■掃描 □其他____	X	X	N/A	N/A	央行、目弟事業主管機關	■人員親送 ■郵寄 □傳真 □Email ■系統 □其他	□刪除 □燒毀 □碎紙銷毀 ■無	■無 □有

個人資料管理制度



個人資料外洩管道

個人資料風險評估

風險評估是什麼

- 風險是指在一定時間內、一定條件下可能發生的結果的不確定性
- 風險評估：將預測出的風險，藉由系統性分析，決定風險程度進而進行風險管理

為什麼要風險評估

◆藉由分析個人資料檔案在機關內部的風險，進而導引出管理控制之概念，透過管理控制手段以確實降低風險，達到保護個人資料之效果。

如何進行風險評估

風險評估流程

- 明確個人資料作業情境、作業內容
- 認識處理作業情境上的風險
- 分析發生可能性與衝擊性

風險評估-1/4

個資盤點清冊

	資料蒐集/處理			資料處理/利用							
(原始+蒐集方法)or(加工+加工方法)二選一填寫				內部傳送		保管		外部傳送		委託	廢棄方法
原始資料	蒐集方法	加工資料	加工方法	資料形式	傳送方式	保管方式	保存期限	資料形式	傳送方式		

作業情境

加工

- 輸入/編輯
- 輸出/列印
- 影印
- 掃描

內部傳送

- 人員親送
- Email
- 系統
- 其他

保管

- 儲存個人電腦(電子)
- 儲存於資料庫/主機(電子)
- 存放個人櫃/抽屜(紙本)
- 存放檔案室(紙本)
- 其他

外部傳送

- 人員親送
- 郵寄
- 傳真
- Email
- 其他

刪除

- 刪除
- 碎紙銷毀
- 其他

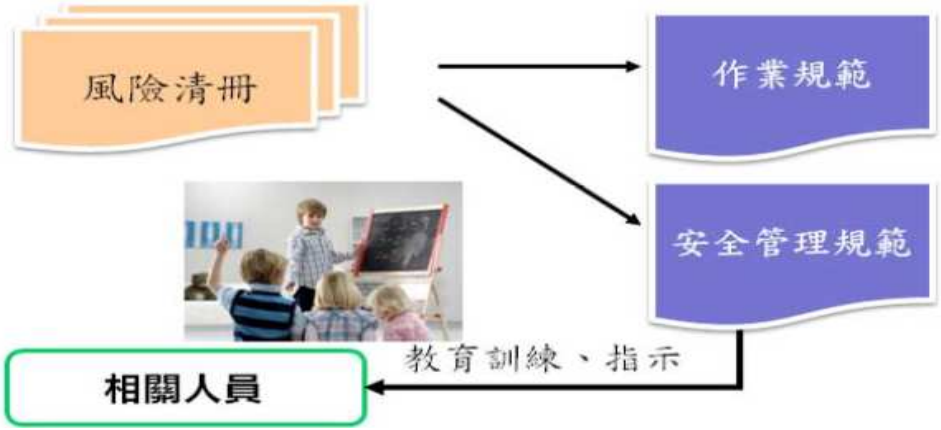
作業內容

風險評估-2/4

參考風險類型暨風險對策表分析個資檔案風險

以個資識別程度個資檔案筆數、是否有特種個資判斷檔案價值

設定優先處理順序，價值高的應優先處理



◆所訂定的風險處理對策，必須徹底讓相關部門負責人瞭解。除將風險對策反應在相關內部規範或作業程序書，使相關業管人員可以隨時參照外，也必須加以教育訓練與指示

風險評估-3/4個人資料檔案價值

◆個人資料識別程度（舉例）

識別程度	定義
H	姓名+身份證字號
M	姓名+生日.....不含身份證字號
L	不含姓名、身份證等直接識別性個資

◆個人資料檔案數量（舉例）

檔案數量	定義
H	500筆以上
M	100~500（不含）筆
L	100筆以下

風險評估-4/4個人資料風險等級

◆個人資料檔案衝擊（舉例）

衝擊程度	定義
H	損害賠償1000萬以上
M	損害賠償200萬-1000萬
L	損害賠償200萬以下

◆發生可能性（舉例）

發生可能性	定義
H	非常可能會發生
M	有可能會發生
L	不太可能會發生

風險處理

個資風險評鑑表

風險評鑑表(參考範例)

單位名稱	
單位主管	
填表人員	

個人資料檔案	有無特種個資	個資識別程度	檔案數量(一年大約件數)	個人資料檔案價值	作業情境	作業內容	具體風險類型	個人資料檔案衝擊	發生可能性	風險等級	風險處理對策
	□無 □有				加工						
					內部傳送						
					保管						
					外部傳送						
					刪除						
	□無 □有				加工						
					內部傳送						
					保管						
					外部傳送						
					刪除						

個資風險評鑑表(範例)

風險評鑑表(參考範例)

單位名稱	
單位主管	
填表人員	

個人資料檔案	有無特種個資	個資識別程度	檔案數量(一年大約件數)	個人資料檔案價值	作業情境	作業內容	具體風險類型	個人資料檔案衝擊	發生可能性	風險等級	風險處理對策
公司設立登記文件	■無 □有	H	M	H	加工						
					內部傳送		收發記載不確實以致遺失	M	M	M	確認收受記錄媒體內容、件數，雙方留存收受記錄
					保管		不當存取(任何人都可以進入檔案室取得資料)	M	M	M	限制人員進入檔案室、重要資訊應上鎖保管
					外部傳送						
					刪除						
公司登記事項卡	■無 □有	H	M	H	加工						
					內部傳送		收發記載不確實以致遺失	M	M	M	確認收受記錄媒體內容、件數，雙方留存收受記錄
					保管		不當存取(任何人都可以進入檔案室取得資料)	M	M	M	限制人員進入檔案室、重要資訊應上鎖保管
					外部傳送						
					刪除						
公司設立登記資料庫	■無 □有	H	M	H	加工						
					內部傳送						
					保管		伺服器遭外部攻擊	H	M	M	安裝防毒軟體並定期更新防毒碼、使用弱點掃描
					外部傳送						
					刪除						
公司設立登記檔案(提供用)	■無 □有	L	L	L	加工						
					內部傳送						
					保管	輸入系統儲存	不當存取(任何人都可以進入檔案室取得資料)	M	L	L	限制人員進入檔案室、重要資訊應上鎖保管
					外部傳送	提供央行、目的事業主管機關審查	郵寄過程中遺失	L	L	L	採取掛號、雙掛號可留記錄的郵寄方法
					刪除						
公司名稱及所營事業登記預查表	■無 □有	H	M	H	加工						
					內部傳送						
					保管		不當存取(任何人都可以進入檔案室取得資料)	M	M	M	限制人員進入檔案室、重要資訊應上鎖保管
					外部傳送						
					刪除						
公司名稱暨所營事業預查申請表(電子)	■無 □有	H	M	H	加工						
					內部傳送						
					保管		伺服器遭外部攻擊	H	M	M	安裝防毒軟體並定期更新防毒碼、使用弱點掃描
					外部傳送						
					刪除						

個人資料安全防護

社交工程定義

- 社交工程是**利用人性的弱點(貪心、好奇心...)或人際之信任關係進行詐騙**，是一種非「全面」技術性的資訊安全攻擊方式。(例如藉由電話、電子郵件或假扮身分來進行社交工程)
  - **不須高深的資訊技術即可獲取**帳號、密碼、信用卡密碼、身分證號碼、姓名、地址或其他身分或**機密資料的方法**。
  - 就算擁有高科技的資安設備、高效能的防護系統，**只要需要人為操作，就有遭受社交工程攻擊的危機。**

社交工程 - 攻擊目的

- 竊取機密檔案/文件
- 針對性資料蒐集(企業商業機密[新研發產品])
- 線上遊戲之有價財產(遊戲寶物)
- 部落格或社群網站之帳號密碼
- 工作商業機密資料
- 跳板(殭屍電腦)
- 監控使用者行為
- 智慧型手機使用者個資(通訊錄、E-Mail等)

社交工程攻擊管道與手法

- 電話詐騙(早期的攻擊管道)
- 電子郵件隱藏惡意程式
- 網路釣魚
- 圖片中的惡意程式
- 偽裝修補程式
- 軟體弱點與零時差攻擊
- USB隨身碟
- 即時通訊軟體也成為傳播惡意程式的途徑
  - LINE
  - SKYPE

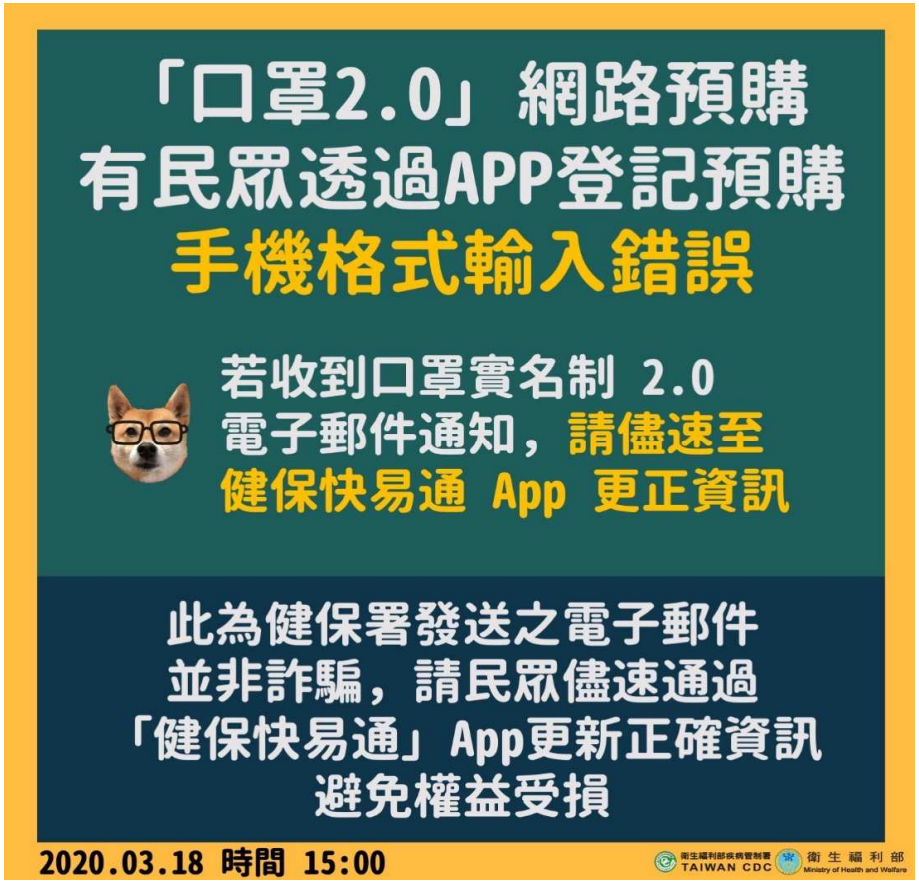
社交工程 - 電話詐騙(I)

- 社交工程手法最早使用的管道是以電話為媒介，假冒各種身分，利用公司員工容易相信與缺乏警覺性的人性弱點，誘騙出帳號、密碼等機密資料。

詐騙來電排名(統計日期：109年03月09日至109年03月15日)		
1	002425928137	假冒機構公務員詐財
2	+886226553000	假冒花旗銀行
3	+4994178878412	假冒拍賣賣家
4	009225543313	假冒機構公務員詐財
5	+886223776163	假冒拍賣賣家
6	+8866227695000	假冒中國信託商業銀行
7	+16609569250	假冒拍賣賣家
8	009425717902	假冒機構公務員詐財
9	+88622182131	假冒玉山商業銀行
10	0092502664336	假冒機構公務員詐財

社交工程 - 電話詐騙(II)

- 收到口罩實名制2.0電子郵件通知，請儘速至健保快易通App更正資訊，指揮中心提醒，此為健保署發送之電子郵件，並非詐騙，請民眾儘速通過「健保快易通」App更新正確資訊，避免權益受損。



社交工程 - 電話詐騙(III)

- 請小心
- 賣場或銀行客服不會要求操作自動櫃員機（ATM）、自動存款機（CDM）、提領現金、購買遊戲點數，那些都是詐騙！
- 來電顯示含「+」號，就是境外來電，小心有詐！
- 看見臉書貼文活動限定iPhone 一支只要5000、10000元（低於市價），就是詐騙。

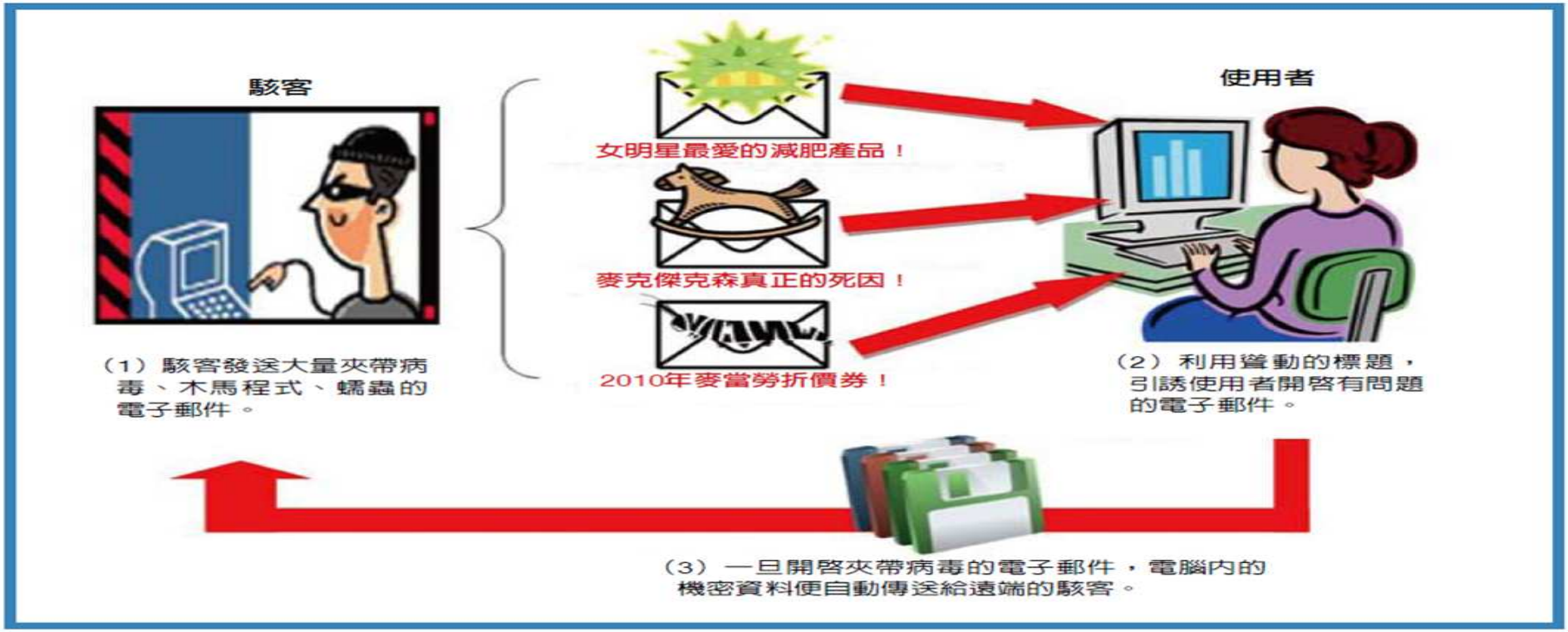
社交工程 - 電子郵件篇

- 駭客利用電子郵件夾帶病毒、木馬等惡意程式，信件標題再藉由熱門時事、養身保健或情色相關等聳動標題，引誘使用者開啟郵件中所夾帶的惡意程式。

每131封電郵就有一封包含惡意連結或附件

- 你的email中毒了嗎？你還在用懶人密碼嗎？你知道每131封電郵中，就有一封包含惡意連結或附件，比例創五年來新高？電子郵件已成為網路攻擊者實施感染的首選途徑，嚴重威脅用戶安全。

社交工程 - 電子郵件惡意程式



利用電子郵件進行社交工程的過程

社交工程 - 網路釣魚攻擊示意

釣魚郵件案例(偽造銀行網站)

釣魚郵件案例(仿冒網站)

www.landbank.com.tw	www.1andbank.com.tw
www.104.com.tw	www.1O4.com.tw
www.bot.com.tw	www.b0t.com.tw
www.acer.com.tw	www.accer.com.tw

真

假

社交工程的預防

- 隨時具備危機意識，對於任何詢問重要資料的人士，都需小心求證
- 單位內對權限應加以分級控管，非屬個人分內事宜，不應掌握帳號、密碼等特殊權限，防止因不了解安全等級而不慎外流重要資料
- 安裝防毒軟體，設定個人防火牆，並定期更新病毒碼
- 針對電腦應用程式應隨時更新修補程式；設定安全密碼（8碼以上，包括英數與符號字元），避免太簡單易遭破解的密碼
- 重要資料檔案要加密防護(WORD、Excel)

教育機構個資防護

個人資料保護及安全維護

- 機關學校應指定**單位副首長為機關召集人**，統籌決策與執行單位內資訊安全與個資隱私業務之資源整合運用。
- 機關學校應**指定專人**依相關法令辦理安全維護及保管事項，作為機關內部之個人資料管理代表。機關組織編制較小者，則統一由該機關**「個資保護聯絡窗口」**兼辦專責人員業務。
- 機關學校應設置並指定「個資保護聯絡窗口」，作為機關學校間個資業務協調聯繫之對口、機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。另單位應將「個資保護聯絡窗口」之**聯繫方式（如：電話、email）置於單位網站**，以便利民眾提出申訴與救濟。

個人資料保護及安全維護(cont.)

- 個人資料檔案應**定期備份**，並防止個人資料被竊取、竄改、毀損、滅失或洩露。個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定**使用範圍及調閱或存取權限**。個人資料檔案之處理行為應設置使用者代碼及通行碼，不得與他人共用並定期更新。另視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，並**留存使用者身分、識別帳號與其行為紀錄以供事後稽查**。
- 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身份之登入通行碼，並視業務及資料重要性，考量其他輔助安全措施。個人資料檔案使用完畢後，應即退出應用程式，不得留置於電腦終端機。

個人資料保護及安全維護(cont.)

- 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，宜**建立相關之授權、監督及行為記錄機制**。
- 內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對**轉交或傳輸行為加以記錄流向備查**。
- 對於個人資料之調閱宜經申請並核准，並加以**記錄其調閱身分及行為**。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

個人資料保護及安全維護(cont.)

- 以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原檔案查核。
- 機關學校單位管理之網站或網頁內容，於確有必要公布個人資料時，**需經所屬單位主管核准，且依相關法律及規範處理，始得公布。**
- 學校應於法律允許之範圍內提供資料當事人下列權利：
- 1. 查詢或請求閱覽。
- 2. 請求製給複製本。
- 3. 請求補充或更正。
- 4. 請求停止蒐集、處理或利用。
- 5. 請求刪除。

適當安全措施

- 一、配置管理之人員及相當資源。
- 二、界定個人資料之範圍。
- 三、個人資料之風險評估及管理機制。
- 四、事故之預防、通報及應變機制。
- 五、個人資料蒐集、處理及利用之內部管理程序。
- 六、資料安全管理及人員管理。
- 七、認知宣導及教育訓練。
- 八、設備安全管理。
- 九、資料安全稽核機制。
- 十、使用紀錄、軌跡資料及證據保存。
- 十一、個人資料安全維護之整體持續改善。


Q
A