個人資料鑑別與盤點課程

聯準科技服務有限公司
資深顧問 吳文進
Email: alexwu0513@gmail.com
Mobile: 0911-371837
October 3, 2016

1.

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

2.

一、個人資料流之重要性

3.

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**。

4.

個人資料流之重要性

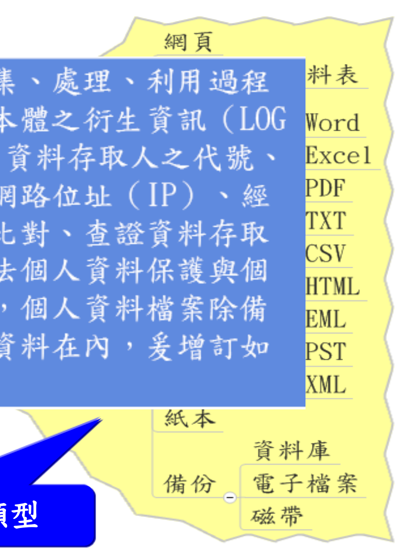
- **特種個人資料之定義**
- 本法第二條第一款所稱**病歷**，應指下列各款資料：
  - 醫師依醫師法執行業務所製作之病歷。
  - 各項檢查、檢驗報告資料。
  - 其他各類醫事人員執行業務所製作之紀錄。
- **醫療**：
  - 指除前項病歷以外，其他以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為之診察、診斷及治療；或基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術、或處置等行為全部或一部所產生之個人資料。
- **基因**：指由一段去氧核醣核酸構成，為生物體控制特定功能之遺傳單位訊息
- **性生活**：指性取向或性慣行之個人資料。
- **健康檢查**：指對於無明顯疾病症狀，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。

5.

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**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

6.

個人資料流之重要性

7.

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**。

8.

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**。

9.

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。**

10.

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。

11.

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)。

12.

二、個資法對蒐集階段之限制

13.

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。

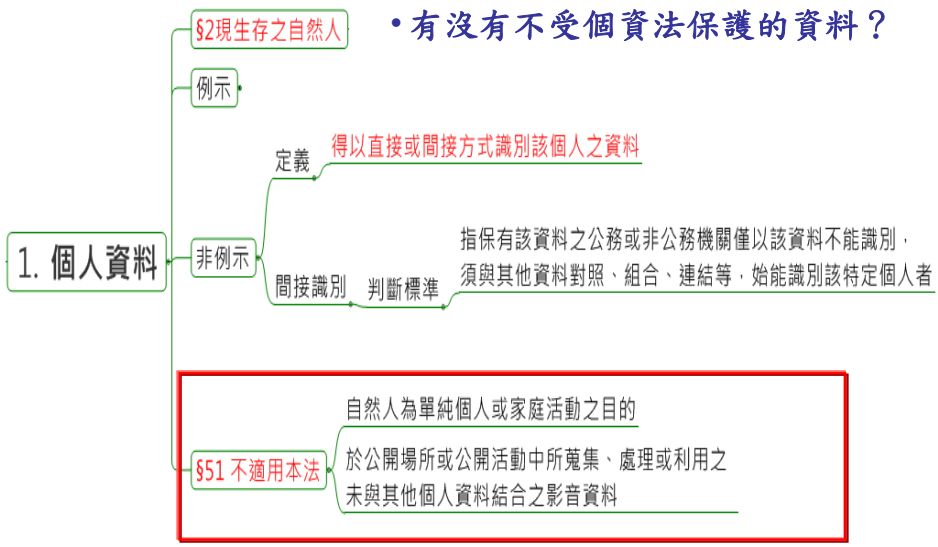
14.

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。

15.

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？

16.

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

17.

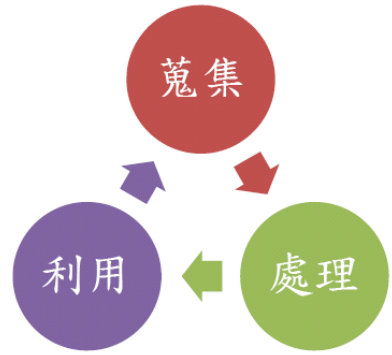
個人資料體檢步驟一：清點個人資料

- 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。

18.

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.....。**

19.

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。

20.

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)

23.

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。

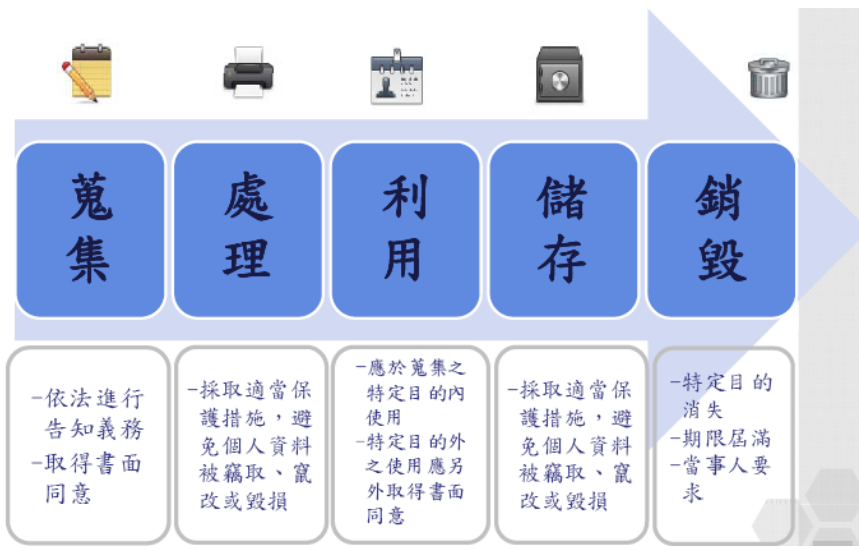
24.

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。

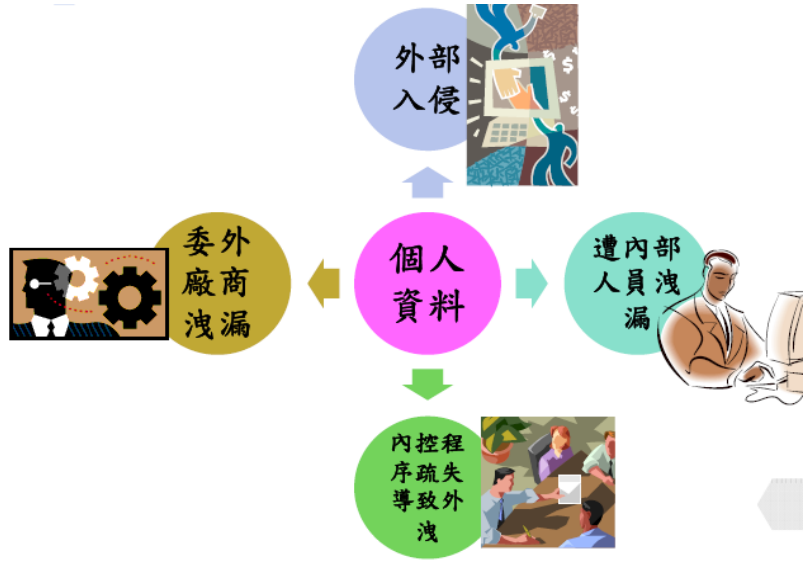
25.

個人資料管理制度



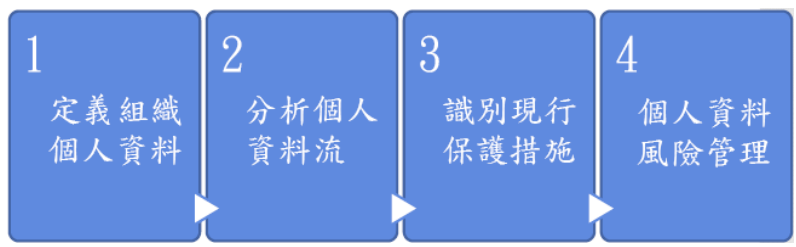
26.

個人資料外洩管道



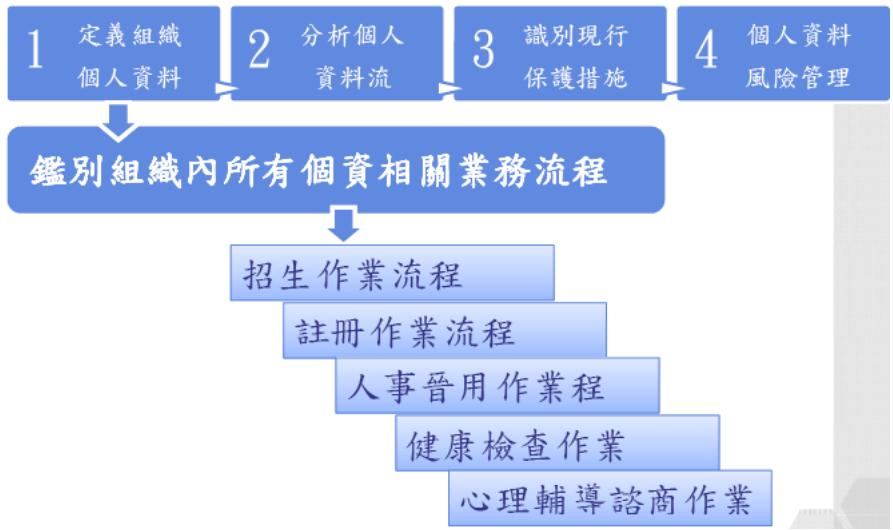
27.

個人資料保護程序



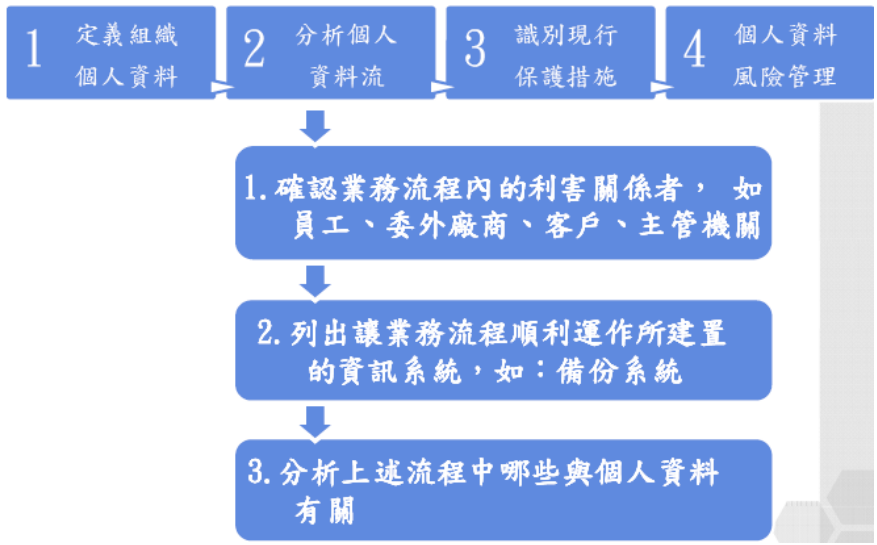
28.

個人資料保護程序



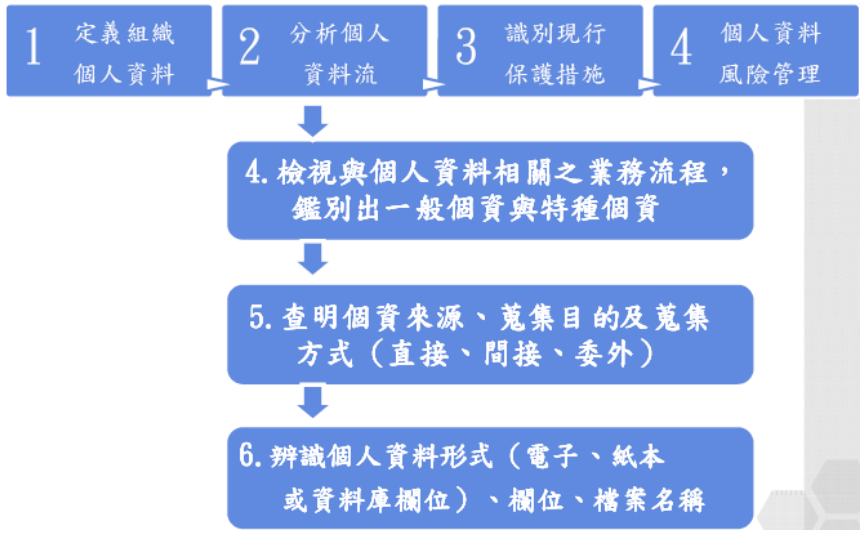
29.

個人資料保護程序



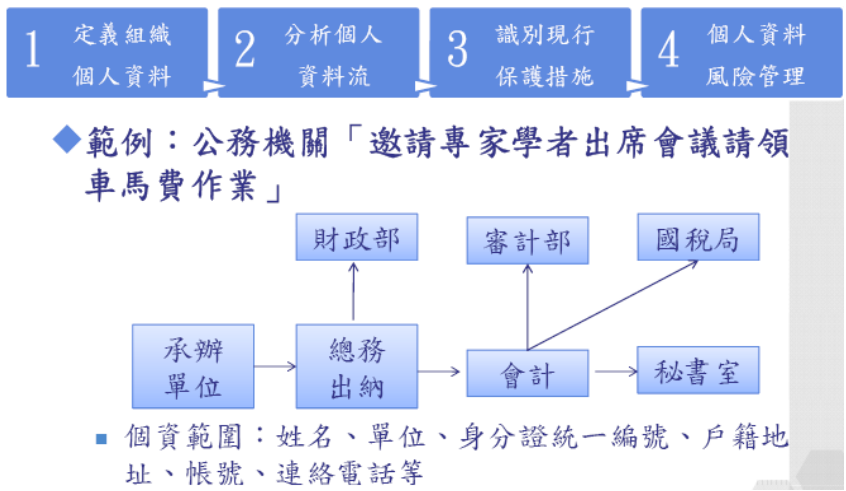
30.

個人資料保護程序



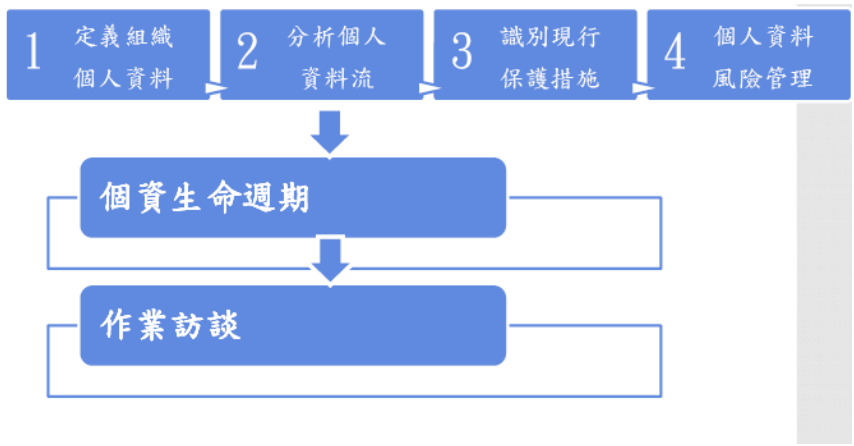
31.

個人資料保護程序



32.

個人資料保護程序



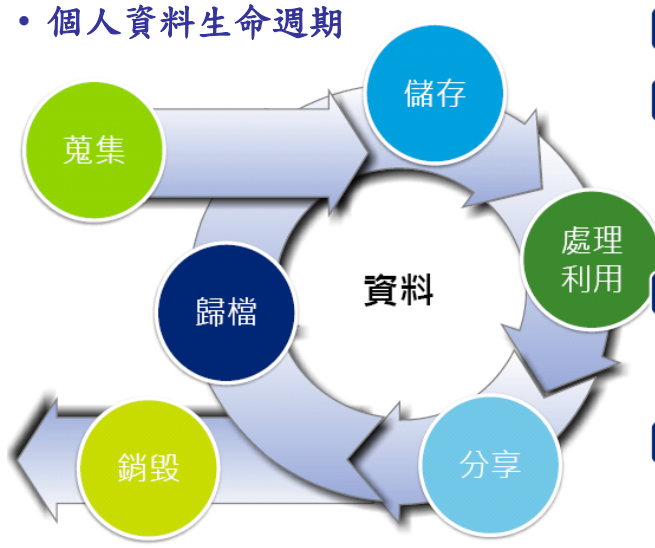
33.

分析個人資料流

34.

分析個人資料流

- 個人資料生命週期



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。

35.

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。

36.

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、單位名稱、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 XX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	姓名、單位名稱、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 XX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

39.

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	姓名、單位名稱、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 XX小姐 xxxx-xxxx#xxx	教育訓練執行期間	無	無	無	無	無	本機帳密保護

40.

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	
X X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、單位名稱、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	X X組	本機作業Excel表	X X組	無	台灣	X X組	報名通訊聯繫	X X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

41.

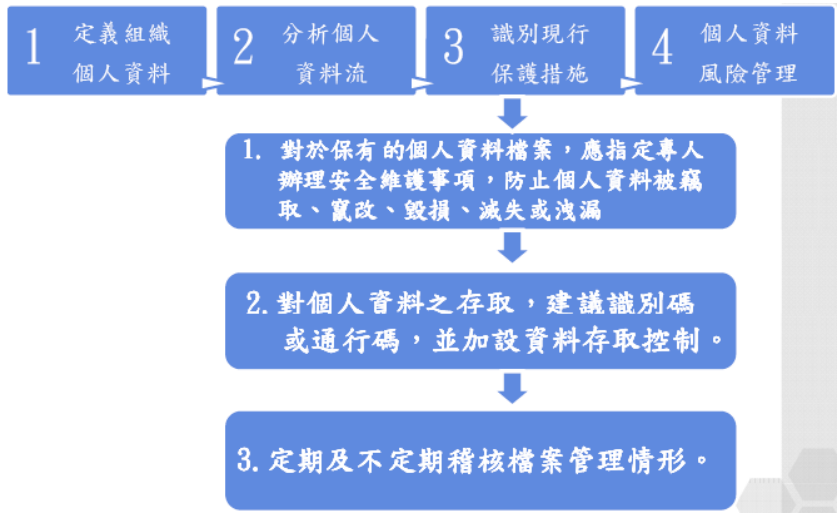
分析個人資料流

◆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

42.

個人資料保護程序

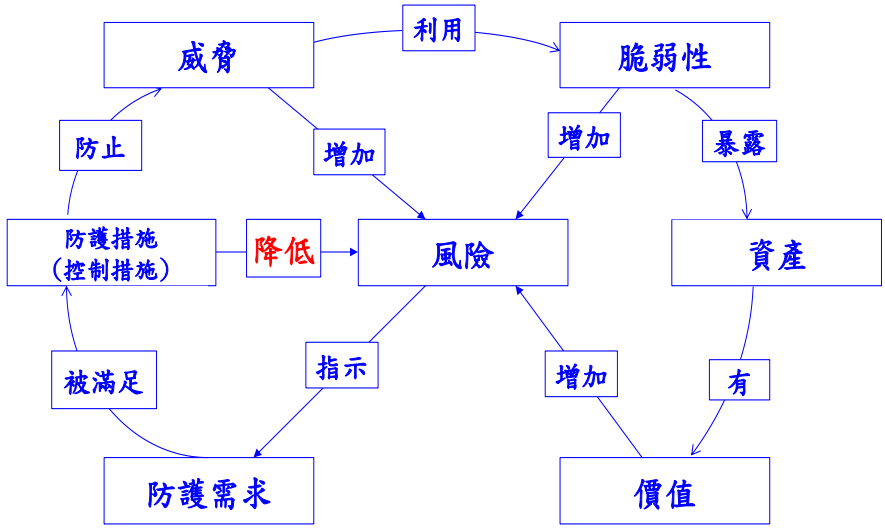


43.

二、個資資產分類原則

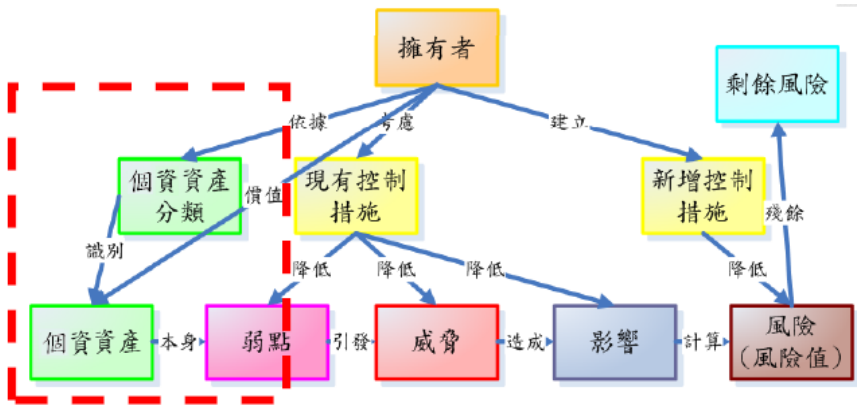
44.

建立個資資產原則



45.

建立個資資產原則



46.

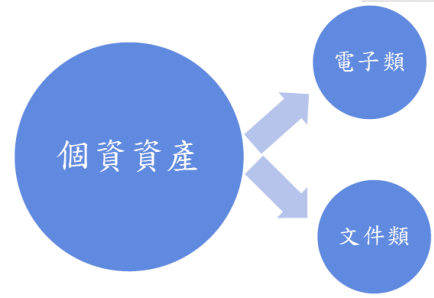
個資資產分類

◆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。

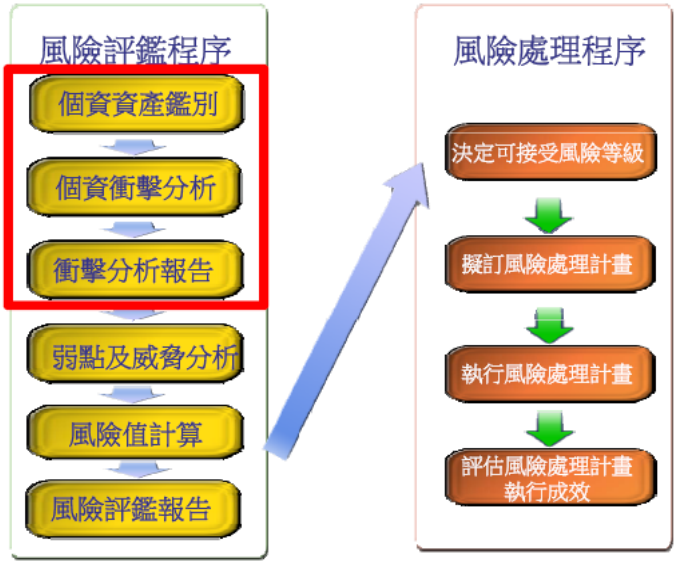


47.

二、建立個資資產清冊

48.

個人資料風險管理程序



49.

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。

50.

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輸入、編輯、複製、刪除、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	保單及聯絡方式	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	是否含醫療基因性生活健康檢查犯罪前科	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	個資利用對象	台灣地區或是國外	個資利用之方式及目的	個資保單及聯絡方式	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）

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	姓名民國身分統一證號、業務聯絡方式（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	

Q&A

～如有任何問題・歡迎隨時來電詢問～