個人資料保護與管理

個人資料管理暨盤點教育訓練

課程內容

- 個人資料管理概要
- 個人資料管理制度之生命週期
- BS 10012標準說明
- 個人資料流分析執行
- 實作討論

個人資料，無所不在

- 個人資料管理概要

個資法國際發展趨勢

1890年 隱私權的提倡
個人可不被打擾，安靜獨處生活的權力(the right be alone)

1980年 隱私與個資保護開始受到國際組織重視
OECD提出「隱私保護與個人資料跨境流通指導員則」

1995年 歐盟提出個人資料保護指令
歐蒙個人資料保護指令，影響包含我國在內之各國立法工作

2007年 APEC推動跨境隱私保護實驗計畫
我國為APEC成員之一，直接面臨來自國際上的壓力

資料來源：資策會

經濟合作暨發展組織 (OECD)

個人資料保護8大原則

限制蒐集原則	經本人同意，以合法、公正手段於適當場所蒐集	安全確保原則	資料必須採取合理安全保護措施，以免資料遭遺失、盜用、毀損、竄改或揭露的風險
品質確保原則	符合資料使用之目的，並確保資料之正確性、完整性和時效性	公開原則	對個人資料之開發、運用、政策等必須採取一般的公開政策
目的明確原則	進行蒐集的目的必須在蒐集的當時就闡述明確，爾後使用也必須受限於當初所訂目的，不得他用	個人參與原則	確認資料存在、資料內容、請求刪除或更正
限制目的外使用原則	非經本人同意不得作蒐集目的外利用	責任明確原則	資料管理者必須確保落實組織政策與執行措施以遵守上述各項原則

何謂個人資料？（個資法第2條）

自然人的
- 姓名
- 出生年月日
- 身分證號碼
- 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

一般個資

特種個資
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

有關醫療、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)

其他個資
- 得以直接或間接方式識別該個人之資料

個人資料的範圍

個人資料範圍

•醫療之個人資料，指除病歷及由醫師或其他之醫

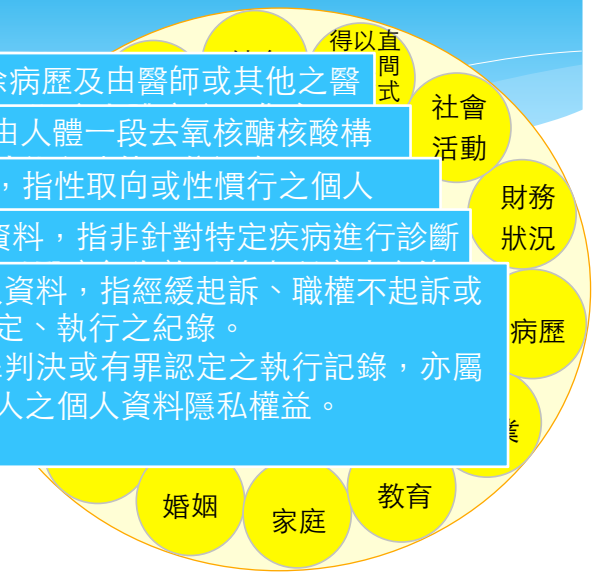
基因之個人資料，指由人體一段去氧核醣核酸構

•性生活之個人資料，指性取向或性慣行之個人

•健康檢查之個人資料，指非針對特定疾病進行診斷

•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、執行之紀錄。
•此外，有關有罪判決或有罪認定之執行記錄，亦屬之，以保護當事人之個人資料隱私權益。

會
接或
個人之資料。（個人資料包括備份檔案）



- 個人資料管理制度之生命週期

個資法對蒐集、處理、利用之損害賠償

個人資料保護法第28條

* 被害人雖**非財產上之損害**，亦得請求賠償相當之金額；**其名譽被侵害者，並得請求為回復名譽之適當處分**。
* 依前二項情形，**如被害人不易或不能證明其實際損害額時**，得請求法院依侵害情節，以**每人每一事件新臺幣五百元以上二萬元以下計算**。
* 對於**同一原因事實造成多數當事人權利受侵害之事件**，經當事人請求損害賠償者，**其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限**。
* 同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。
* 第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

蒐集之定義

何謂蒐集？ (§15符合特定目的)

* 指以任何方式取得個人資料。
  * 直接蒐集：直接從當事人取得個人資料。(§8)
  * 間接蒐集：透過第三方取得個人資料。(§9)
    * 委外：如104、市調公司、信用卡業務。
    * 非委外：如主管機關提供。

第 8 條
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。

第 9 條
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。

處理之定義

何謂處理？ (§15符合特定目的)

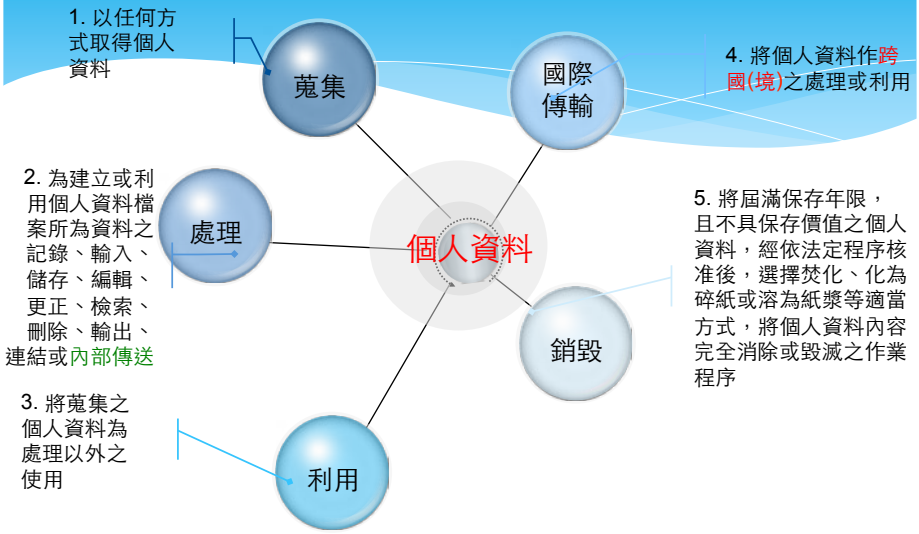
* 指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正(§11)、複製 、檢索、刪除、輸出、連結或內部傳送。
  * 新增文件、建檔案、輸入系統。
  * 編輯檔案、刪除檔案、儲存檔案、複製檔案。
  * 檢索查詢、更正錯誤、製作連結。
  * 內部傳送至別部門/單位。

利用之定義

何謂利用？(§16符合特定目的及目的外之利用)

* 指將蒐集之個人資料為處理以外之使用。
  * 對當事人使用其個資：如使用通訊錄打電話或寄信、E-mail。
  * 揭露第三方：如提供檢調單位調查、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。

個人資料檔案之生命週期

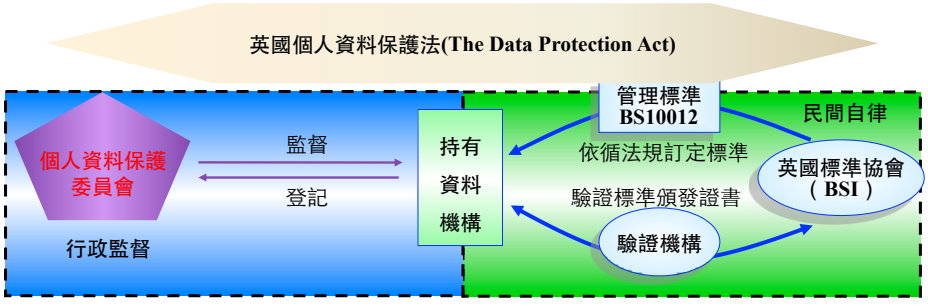


✧ 個人資料檔案盤點重點在於個資之生命週期

- BS 10012標準說明

英國BS 10012

- 英國於1998年將歐盟之「個人資料保護指令」與「電子通訊隱私指令」內國法化為「個人資料保護法」（The Data Protection Act 1998）。並由個資保護委員（Information commissioner）監督法令執行。
- 2001、2007修正擴大個人資料適用範圍，引發適用困擾。
- 英國標準協會（BSI）於2009年5月順應企業需要正式推出一套個人資料管理之標準（BS10012），協助企業遵循英國個人資料保護法。



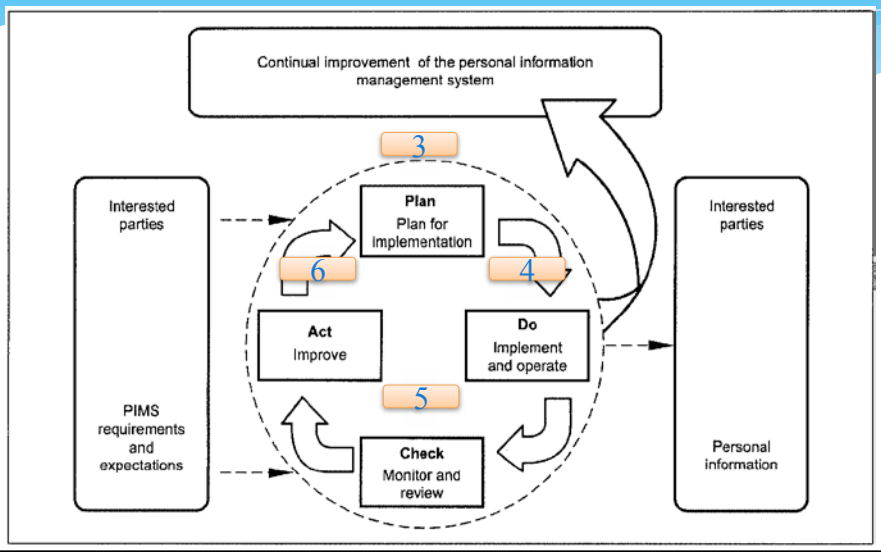
資料參考來源：經濟部

BS 10012 個人資料管理系統

BS 10012的全名為「資料保護–個人資訊管理系統之要求（Data protection–Specification for a personal information management system）」，其中，資料保護法案所要求應遵守的8項資料保護原則，非常適合各組織作為制定個人資料保護的參考，內容說明如下：

* 個人資料不可以非法或不公正方式蒐集、處理。
* 個人資料應限於以特定目的之方式蒐集、處理。
* 個人資料應以充分、相關，而非逾越其原本之目的處理。
* 個人資料應求準確，並在必要時及時更新。
* 個人資料之保存，不得超過其原定目的之保存期限。
* 個人資料之處理，應依照當事人之權限及法令規範。
* 組織應採取適當的資料保護技術和措施，防止個人資料遺失或毀壞。
* 個人資料不得轉移到歐洲經濟區以外的國家或地區。

Plan-Do-Check-Act (PDCA) 循環



規劃個人資料管理系統PIMS

3.1 建立和管理 PIMS
3.2 PIMS 的範圍和目標
3.3 個人資料管理政策
3.4 政策內容
3.5 職責和歸責性
3.6 資源提供
3.7 將PIMS嵌入組織文化

PIMS的建置與運作-1

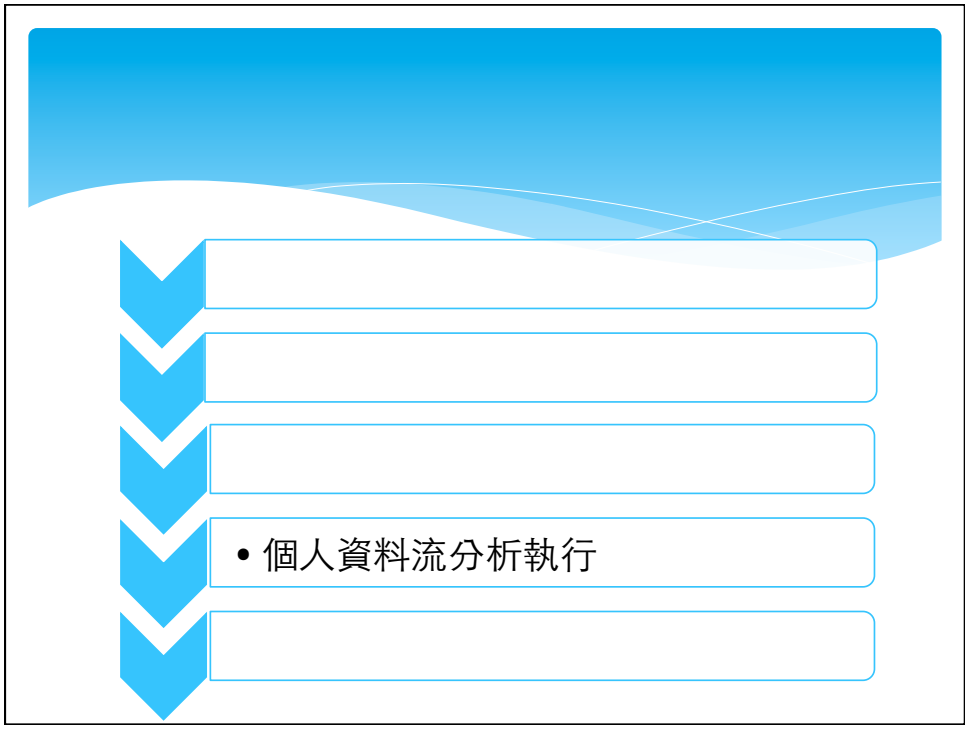
4.1 責任的配置(Key appointments)
4.2 辨識及記錄個人資料的使用情況
4.3 認知及教育訓練
4.4 風險評鑑
4.5 PIMS 持續更新
4.6 通告
4.7 公正與合法的處理
4.8 個人資料處理的目的
4.9 適當、相關且不過度
4.10 正確性

PIMS的建置與運作-2

4.11 保留及處置
4.12 個人的權利
4.13 安全議題
4.14 將個人資料傳輸於EEA(歐盟)之外(EEA=European Economic Area)
4.15 揭露予第三方
4.16 轉包處理
4.17 維護

PIMS的監控、審查及改善

5.1 內部稽核
5.2 管理審查
6.1 矯正與預防措施
6.2 持續改進



實作討論(一)業務流程分析

個人資料流之重要性-1

* 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。

* 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-2

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。

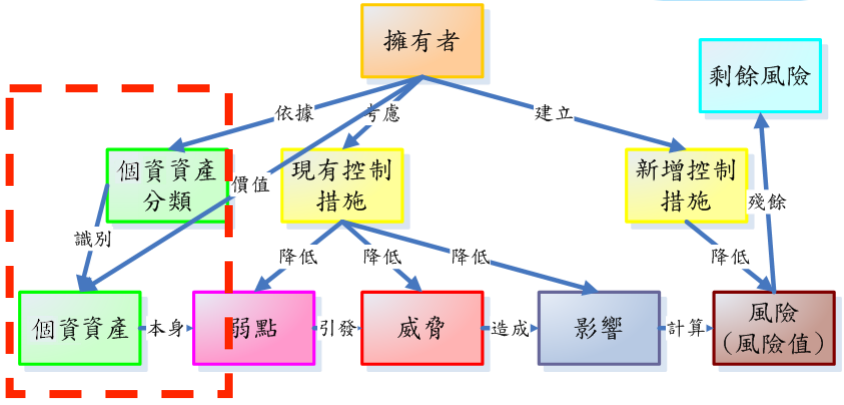
* 瞭解這份檔案日常的使用者、維護者及檔案使用狀況；
* 清查檔案曾經被哪些員工閱覽過，這些員工又看過哪些其他的檔案；
* 追查除了外洩檔案外，洩密者還看過哪些檔案。

個人資料流之重要性-3

* 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)。

- 實作討論

建立個資資產原則



個人資料盤點時機

每年應至少執行一次個人資料檔案鑑別作業。

於下列情形發生時，亦得針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案鑑別之作業：

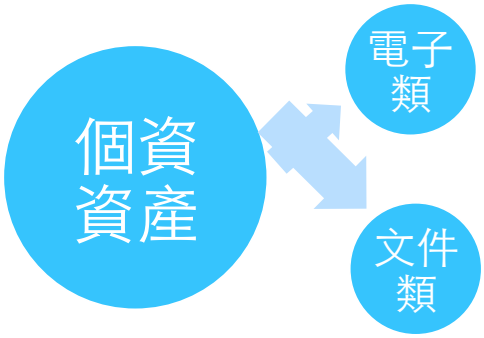
* 組織變更：如部門異動。
* 作業流程改變：如業務異動。
* 個人資料檔案異動：如：表單異動、服務異動。

個資盤點技巧

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。鑑別出所有與個人資料相關之營運流程，並針對各個流程細項了解其流程架構。

* 從最完整之業務執掌找尋與個資相關之業務。
* 業務之業務流程所有過程會接觸到之含個人資料之表單與資訊系統。
* 非自身業務，但會接觸與個資相關之別人業務，如：員工旅遊保險、公文會簽（過水表單）。
* 備份資料。

實作討論(二)個資盤點實務



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。

33

免盤入個資清冊之個人資料

剔除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。

實作討論(三)個資衝擊分析