東華大學

個人資料管理文件宣導教育訓練

王吉祥(Davies)
2013.11

課程大綱

- BS 10012 標準暨個人資料保護法文件控管要求
- 個人資料管理制度文件架構暨文件生命週期
- 個資侵害事故之緊急應變
- 實務說明

課程大綱

- BS 10012 標準暨個人資料保護法文件控管要求
-
-
-

3

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
歐盟個人資料保護指令，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

4

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

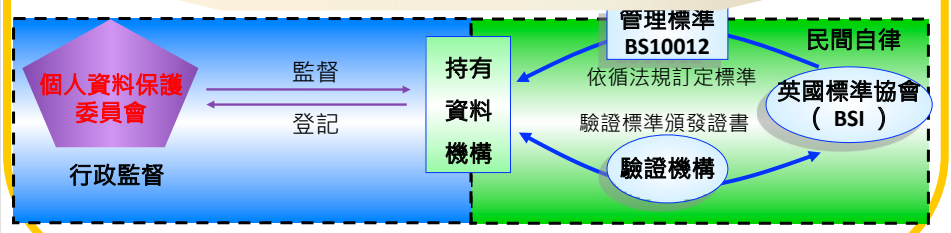
亞太經濟合作組織(APEC)

- 亞太經濟合作組織 (APEC) 參考經濟合作暨發展組織 (OECD) 的隱私保護及個人資料國際傳輸指導方針，於2004年制訂「亞太經濟合作組織隱私保護綱領」，做為提升各國隱私保護重要推動方針，並確保亞太地區各會員國間資訊自由流動，俾符合隱私保護綱領之規範原則。

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。

英國個人資料保護法(The Data Protection Act)



資料參考來源：經濟部

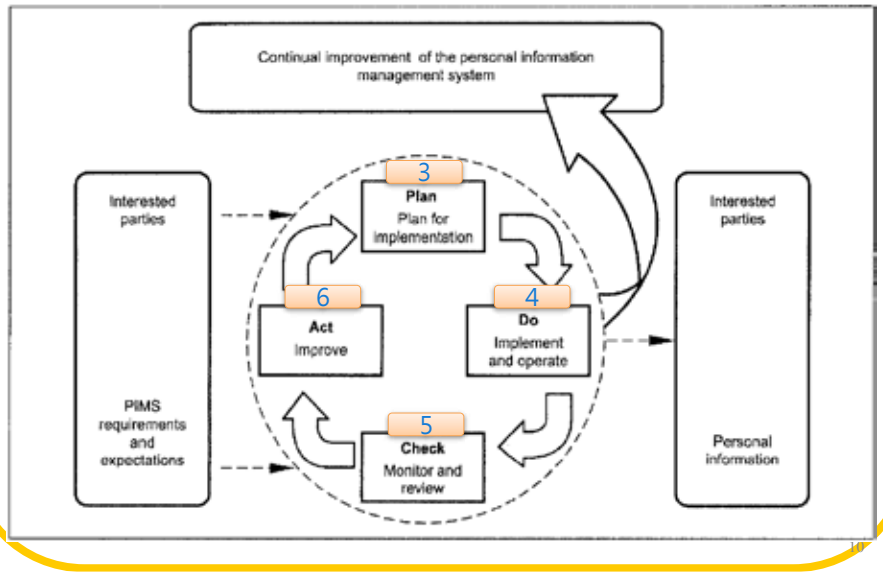
BS 10012 個人資料管理系統

- 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。

課程大綱

個人資料管理制度文件架構暨文件生命週期

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

11

規劃個人資料管理系統PIMS

- 3.1 建立和管理 PIMS
  - 組織應建立、實作、維護及持續改進PIMS以符合3.2～3.7的要求
- 3.2 PIMS 的範圍和目標
  - a) 個人資料管理需求
  - b) 組織的目標與義務
  - c) 組織可接受的風險等級
  - d) 適用之法令、規章、契約(合約)與專業職責
  - e) 個人和其他利害關係人之利益

12

規劃個人資料管理系統PIMS

- 3.3 個人資料管理政策
  - 組織應確保高階管理階層被附與發行及維護個人資料管理政策之責，而其政策中應明訂政策框架，並展現對於遵循個人資料保護法與好的實務的支持與承諾。

NOTE *Senior management might consist of the Board of Trustees/Directors, the Chief Executive and senior workers, the partners of the organization or the owner of a sole trader company.*

13

規劃個人資料管理系統PIMS

- 3.4 政策內容
  - a) 僅於合法組織需求下，始得進行個人資料之處理
  - b) 僅針對特定目的蒐集必要的個人資料，且不過度的處理個人資料
  - c) 明確告知當事人其個人資料將如何被使用及被誰使用
  - d) 僅處理相關且適當的個人資訊
  - e) 公平與合法的處理個人資訊(參考 4.7);
  - f) 組織應維護一份個人資料清冊(參考 4.2);
  - g) 確保個人資料的正確性，並於必要時進行更新
  - h) 僅依法或合法的組織目的下保存個人資料

14

規劃個人資料管理系統PIMS

- i) 尊重當事人對其個人資料所能行使之權利，包含其申請閱覽權
- j) 確保所有個人資料安全
- k) 當組織將個人資料傳輸之非歐盟成員之國家時，應確保其具善良保護之機制
- l) 個人資料保護法令所允許之例外情形的應用
- m) 發展與建立PIMS，使個人資料保護政策能實行
- n) 鑑別內、外部利害關係者及其參與PIMS治理與運作的程度
- o) 於PIMS明確界定員工之責任和歸責性(參考3.5)

15

規劃個人資料管理系統PIMS

- 3.5 職責和歸責性

高階管理團隊應負起組織管理個人資料之責。(可參考4.1.1).

- 職責應包含：
  - a) 核准個人資料管理政策
  - b) 依政策發展和施行PIMS
  - c) 應遵循政策執行安全及風險管理 (可參考4.13.1)
- 應指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循(可參考4.1.2)
- 藉由流程與程序的實行、適當的員工發展或對於不符合事項制訂管控程序，以確保所有同仁皆能遵循個人資料管理政策之要求

16

規劃個人資料管理系統PIMS

- 3.6 資源提供
- 組織應決定並提供建立、實行、操作和維護PIMS的資源。
- 3.7 將PIMS嵌入組織文化
  - a) 透過持續的教育訓練與認知課程，以提高、強化與維持所有員工對PIMS的認知
  - b) 建立對PIMS認知訓練有效性評量程序
  - c) 對所有員工傳達以下的重要性：
    - 1) 達成PIMS目標
    - 2) 遵循政策
    - 3) 對政策的持續改善
  - d) 確保每個員工都瞭解他們如何影響組織PIMS

17

PIMS的建置與運作

- 4.1 責任的配置(Key appointments)
  - 4.1.1 高階管理階層
  - 4.1.2 遵循政策的日常職責
  - 4.1.3 資料保護代表
- 4.2 辨識及記錄個人資料的使用情況
  - 4.2.1 組織應維護一份個人資料分類清冊
  - 4.2.2 具高風險的個人資料
- 4.3 認知及教育訓練
- 4.4 風險評鑑

18

PIMS的建置與運作

- 4.5 PIMS 持續更新
- 4.6 通告
- 4.7 公正與合法的處理
  - 4.7.1 個人資料的蒐集與處理
  - 4.7.2 隱私公告與聲明之記錄
  - 4.7.3 隱私公告與聲明之取得
  - 4.7.4 隱私公告與聲明之可用性
  - 4.7.5 第三方

19

PIMS的建置與運作

- 4.8 個人資料處理的目的
  - 4.8.1 處理準則
  - 4.8.2 新目的的同意
  - 4.8.3 資料分享
  - 4.8.4 資料配對
- 4.9 適當、相關且不過度
  - 4.9.1 適當性
  - 4.9.2 相關且不過度
- 4.10 正確性

20

PIMS的建置與運作

- 4.11 保留及處置
- 4.12 個人的權利
  - 4.12.1 個人的權利(符合法定時間限制)
  - 4.12.2 抱怨與申訴
- 4.13 安全議題
  - 4.13.1 安全控制
  - 4.13.2 儲存及管理
  - 4.13.3 傳輸
  - 4.13.4 存取控制
  - 4.13.5 安全評估
  - 4.13.6 安全事故管理

21

PIMS的建置與運作

- 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

22

PIMS的監控與審查

- 5.1 內部稽核
  - 5.1.1 稽核計畫
  - 5.1.2 稽核員的挑選
  - 5.1.3 稽核需求
- 5.2 管理審查
  - a)來自PIMS 使用者之回饋
  - b)由組織人員所辨識及提升之風險
  - c)稽核結果
  - d)程序審查之紀錄
  - e)資訊技術提升及替換之結果

23

PIMS的監控與審查

  - f)來自主管機關評估後之正式要求
  - g)抱怨事件的處理
  - h)已發生之資安事故及資料外洩事件
- 管理審查應提供所有可能造成PIMS變更之詳細資訊，其資料來源可為政策的調整、可能影響作業遵循之程序與技術。
- 當PIMS發生重大變更後，應立即執行稽核作業。

24

PIMS的改善

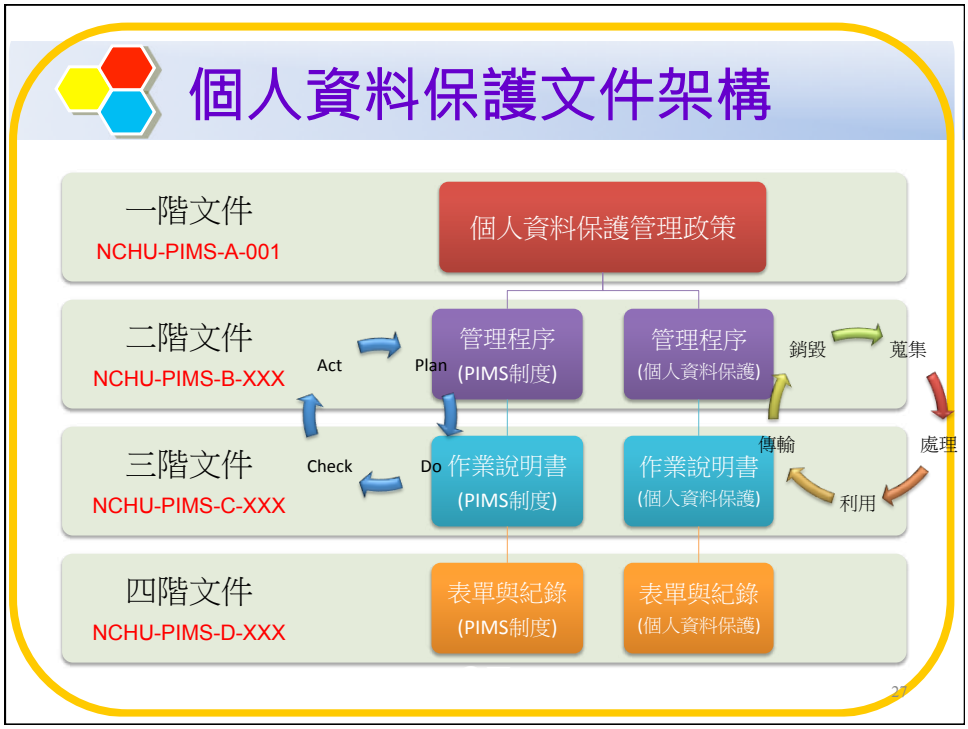
- 6.1 矯正與預防措施
  - 6.1.1 概述
  - 6.1.2 預防措施
  - 6.1.3 矯正措施
- 6.2 持續改進

25

英國標準BS 10012(PIMS) V.S 國內個人資料保護法

BS 10012相關管理規範摘要	國內個人資料保護法相關管理規範摘要	
1.善盡告知義務	1.善盡告知義務	11.個資定義不同(未包含種族、政黨等)
2.依特定目的蒐集個資	2.依特定目的蒐集個資	12.提供閱覽或製給複製本
3.公正且合法使用個資	3.公正且合法使用個資	13.規範特種資料不得蒐集
4.保護個人隱私相關項目	4.保護個人隱私相關項目	14.區分公務機關與非公務機關之處理方式
5.確保存取控制之安全	5.確保存取控制之安全	15.具團體訴訟機制
6.確保資料之正確性	6.確保資料之正確性	
7.確保資料傳輸之安全	7.確保資料傳輸之安全	
8.確保個人修改之權利	8.確保個人修改之權利	
9.妥善處理抱怨與申訴	9.妥善處理抱怨與申訴	
10.落實委外安全管理	10.落實委外安全管理	

26


個人資料保護文件架構
一階文件
NCHU-PIMS-A-001
個人資料保護管理政策
二階文件
NCHU-PIMS-B-XXX
管理程序
(PIMS制度)
管理程序
(個人資料保護)
Act
Plan
銷毀
蒐集
三階文件
NCHU-PIMS-C-XXX
Check
Do
作業說明書
(PIMS制度)
作業說明書
(個人資料保護)
傳輸
處理
利用
四階文件
NCHU-PIMS-D-XXX
表單與紀錄
(PIMS制度)
表單與紀錄
(個人資料保護)


個人資料保護文件說明
PIMS管理制度
一階文件
個人資料保護
Act
Plan
文件管理程序
二階文件
當事人權利聲明
蒐集處理利用
管理程序
矯正預防程序書
個人資料檔案
安全維護計畫
風險評鑑程序書
三階文件
安全管控
作業說明
稽核作業程序書
業務終止後個人
資料處理方法
四階文件
相關表單與紀錄
相關表單與紀錄
http://www.nchu.edu.tw
中興大學 - 個人資料保護與管理文件資料皆可線上下載(需申請帳號)

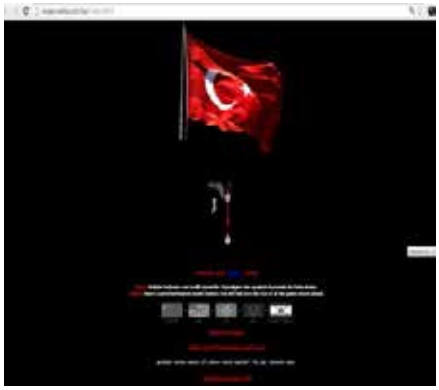
來源	過去情形	現階段挑戰
惡意駭客	資訊系統破壞或入侵知識僅由少數駭客掌握，相關技術具有進入門檻	攻擊工具垂手可得，人人都可是駭客，24小時進行主動、無時差攻擊
民眾	僅注重服務的效率與品質	開始具備個人資料保護與資訊安全意識，並重視個人資料安全
媒體	未關注個資保護議題	媒體爆料文化盛行，監督企業或政府機關的資訊保護作為
法律規範	電腦處理個人資料保護法(84年公布)	「個資法」2012.10 公佈施行

個資外洩管道

- 問卷
- 電話客服中心
- 網購
- **掛馬網站、設計不良的網站**
- **駭客入侵**
- **社群網站**
- **P2P軟體使用**
- 銀行申請單
- 會員手冊
- 信用卡
- 內部人員
- 補習班
- 電子謄本系統
- 直銷公司
- 盜版光碟
- **即時通訊軟體(IM)**
- 無個資保護認知
- **釣魚網站**
- 委外廠商

台灣Nokia行銷網站被駭，150萬個資可能外洩

- Nokia委外經營的5個台灣行銷網站遭駭客入侵，目前駭客已公佈17萬筆資料，由於缺乏證據證實駭客取得的資料數量，Nokia估計約150萬筆資料可能被竊。
- Nokia發生重大資安事件，台灣委外經營的5個行銷活動網站被駭客入侵，約150萬筆消費者個資可能被竊，Nokia已關閉這些網站，同時通知用戶防範。
- 台灣Nokia對外發出聲明，表示該公司委託網路行銷公司Agenda經營的5個台灣行銷活動網站遭駭客入侵，駭客已公佈17萬筆資料，經過調查後，Nokia可能有150萬筆先前在台灣舉辦行銷活動的消費者個人資料外洩，Nokia已採取因應措施，關閉網站、修復伺服器漏洞，移除資料庫，同時以電子郵件、簡訊通知客戶。



資料來源：isecurity

Evernote遭駭，要求近五千萬用戶改密碼

- 如果你是雲端筆記服務Evernote的愛用者，可能要注意一下這則新聞了。Evernote近五千萬名用戶發出修改密碼的通知函，理由是遭到駭客攻擊，導致大量用戶的帳號、電子郵件地址和密碼疑似外露。這也是繼Twitter和Facebook等社交網站遭遇駭客攻擊後，再一次有知名網站遇駭。
- Evernote透過官方部落格表示，用戶在Evernote中所記錄的各項內容並未被擷取，但為了小心起見，還是建議用戶儘快設定新密碼，以保障資訊安全。
- Evernote指出，該公司最初發現了非比尋常的可能性惡意活動。有些人用了不正當手法獲取了Evernote的帳號名稱、電子郵件和密碼。隨後，Evernote立即對該公司各平台的應用軟體進行升級，並協助所有用戶重新設定一組新密碼。
- Evernote執行長菲爾.李賓（Phil Libin）相當重視這起事件，他表示：「我們沒有儲存任何有關用戶的支付訊息，因此不會有與支付相關的資訊外露狀況。」

資料來源：isecurity

課程大綱

實務說明

應變計畫(個案範例)

個資外洩應變計畫

聯絡資訊

王吉祥 講師暨資深經理
+886 970 350 128
dvings@gmail.com