103年度個人資料保護暨內部稽核實務研習課程

簡報人：張曉芸
職　稱：法律研究員
財團法人資訊工業策進會
科技法律研究所
2014.12.9

資群聯訊網
策馬進雲端

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

大綱

- ◆個人資料保護與管理
  - ➢個人資料保護法重點說明
  - ➢個人資料保護與管理制度
- ◆經濟部個人資料保護作業稽核
  - ➢個人資料保護與管理作業說明
  - ➢個人資料保護與管理作業稽核
    - ✓確認稽核實施內容
    - ✓擬訂稽核計畫
    - ✓擬定查檢項目
    - ✓執行稽核
    - ✓撰寫稽核報告

大綱

- ◆個人資料保護與管理
  - ➢個人資料保護法重點說明
  - ➢個人資料保護與管理制度
- ◆經濟部個人資料保護作業稽核
  - ➢個人資料保護與管理作業說明
  - ➢個人資料保護與管理作業稽核
    - ✓確認稽核實施內容
    - ✓擬訂稽核計畫
    - ✓擬定查檢項目
    - ✓執行稽核
    - ✓撰寫稽核報告

個人資料保護法重點說明1/2

第一章 總則（第1條到第14條）

- 目的 / 定義 / 當事人權利 / 委外 / 個人資料蒐集處理利用原則 / 特種個人資料 / 當事人書面同意/ 告知/ 答覆當事人查詢、閱覽、複製本 / 個人資料正確性 / 個資違法事件之通知 / 回覆當事人權利行使 / 費用收取

第二章 公務機關對個人資料之蒐集、處理與利用（第15條到第18條）

- 特定目的內 / 特定目的外 / 持有檔案之公開 / 安全維護

第三章 非公務機關對個人資料之蒐集、處理與利用（第19條到第27條）

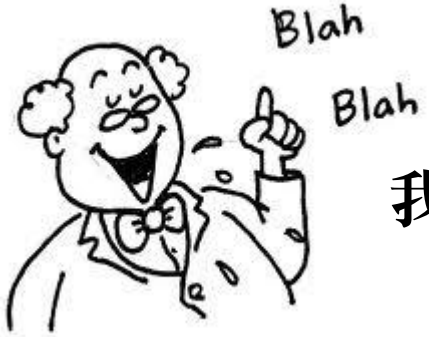
- 特定目的內 / 特定目的外 / 國際傳輸 / 行政檢查 / 違反個資之行政處分 / 檢查結果之公開 / 安全維護

第四章 損害賠償與團體訴訟（第28條到第40條）

第五章 罰則（第41條到第50條）

第六章 附則（第51條到第56條）

個人資料保護法重點說明2/2



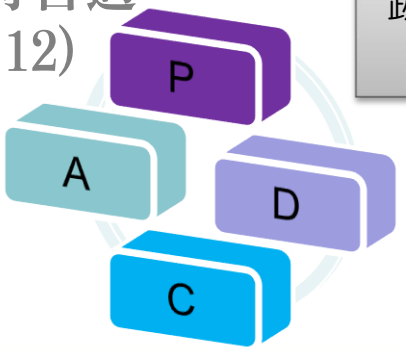
為了遵循個資法
我們到底要做什麼事？

- 適當的蒐集、處理、利用
- 受理當事人權力的行使
- 完善委外監督
- 落實安全管理
- 執行事故發生之通知
- 尊重當事人權益+促進資料合理利用

個人資料保護與管理制度

- 公務機關保有個人資料檔案，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損，滅失或洩漏。（個資法§18）
- 本法所稱適當安全維護措施、安全維護事項或適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，**採取技術上及組織上之必要措施**。（施行細則§12）
- 必要措施，以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。（施行細則§12）

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



大綱

- ◆個人資料保護與管理
  - ➢個人資料保護法重點說明
  - ➢個人資料保護與管理制度
- ◆**經濟部個人資料保護作業稽核**
  - ➢**個人資料保護與管理作業說明**
  - ➢個人資料保護與管理作業稽核
    - ✓確認稽核實施內容
    - ✓擬訂稽核計畫
    - ✓擬定查檢項目
    - ✓執行稽核
    - ✓撰寫稽核報告

經濟部個人資料保護作業稽核

- **因應本部104年個人資料保護作業稽核，所屬機關應於本年度12月底前提出機關內部「個人資料保護管理作業說明」，並完成「個資保護作業稽核報告」，提交本部個人資料保護推動執行小組。**
- **「個人資料保護管理作業說明」得參考「經濟部個人資料保護作業手冊」P.53-P.55內容編寫。**
  - 人員及資源配置：是否配置管理人員及相當之資源進行個人資料保護工作。
  - 蒐集、處理、利用作業：檢視蒐集、處理、利用個人資料之流程中，是否依照法律規定以及內部管理程序進行。
  - 當事人權利行使作業：當事人行使權利時，本部各單位及所屬機關是否按照當事人權利行使流程進行回覆。
  - 個資盤點與風險分析：確認個資盤點作業是否確實完成，並針對各個風險作處分析並處置。
  - 事故通報與應變程序：於事故發生時，是否依規定通報，並作出應變處置及預防等措施。
  - 認知宣導與教育訓練：是否針對所屬人員進行認知宣導與教育訓練，並確實完成記錄。
  - 安全管理：是否針對資料安全管理、人員管理、設備管理等層面進行管控。
  - 使用紀錄、軌跡資料及證據保存：執行個資保護與管理制度之相關記錄，是否確實保存。
  - 委外作業：委外作業之情形，是否做好適當之監督。

經濟部個人資料保護作業稽核

◆ 經濟部個人資料保護作業總說明

經濟部個人資料保護作業總說明

大綱

- ◆個人資料保護與管理
  - ➢個人資料保護法重點說明
  - ➢個人資料保護與管理制度
- ◆經濟部個人資料保護作業稽核
  - ➢個人資料保護與管理作業說明
  - ➢**個人資料保護與管理作業稽核**
    - ✓**確認稽核實施內容**
    - ✓**擬訂稽核計畫**
    - ✓**擬定查檢項目**
    - ✓**執行稽核**
    - ✓**撰寫稽核報告**

經濟部個人資料保護作業稽核

經濟部及所屬機關個人資料保護管理要點（101.10.26 經法字第10104681660號函下達）

MOEA-個資保護管理要點

經濟部個人資料保護作業手冊（P.22）-資料安全稽核程序

- 依據個資法第18條、個資法施行細則第12條第2項第9款及第11款規定辦理
- 作業程序
  - 稽核時間：每年12月底之前
  - 稽核方式：
    1. 稽核小組或稽核專責人員擬定年度稽核計劃
    2. 於稽核預定日前兩週，選出執行內部稽核之人員
    3. 內部稽核執行人員不得稽核所屬部門
    4. 內部稽何執行人員於執行內部稽定日前一週內製作稽核項目表、根據稽核發現記錄稽核結果。
    5. 稽核發現缺失應做成改善計畫，並完成個資管理稽核報告送本部執行小組備查

稽核程序

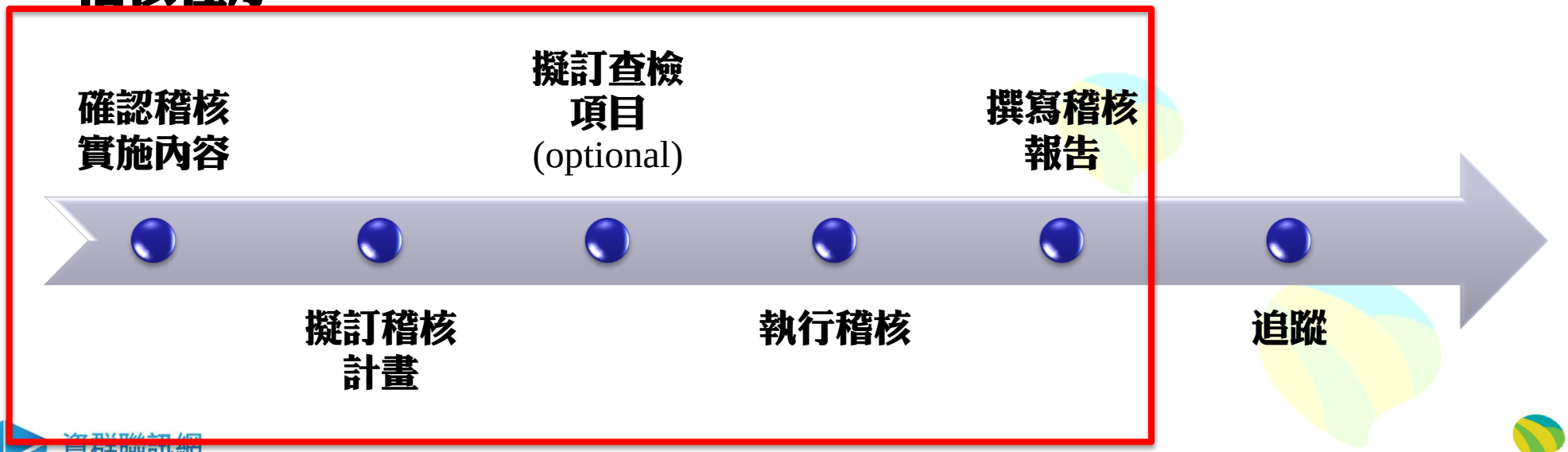
◆為實施稽核，應建立稽核專案

➢稽核專案必須能夠確認受稽核之管理系統的有效性

◆稽核專案的執行包括管理與評估稽核目標是否有達成

➢PDCA

◆稽核程序



稽核程序-確認稽核實施內容

- **於實施稽核前應與受稽核者聯繫**
  - 與受稽核者建立溝通
  - 確認實施稽核的權威性(authority)
  - 提供必要的資訊，例如稽核範圍、時程、方法和團隊
  - 要求受稽核者提供必要的資訊以規劃稽核活動
  - 其他
- **決定稽核的可行性**
  - 確認稽核目標可達成

稽核程序-擬訂稽核計畫

範例：

經濟部中區聯合服務中心稽核計畫
稽核時間：2014年12月1日
受稽單位：經濟部中區聯合服務中心
稽核範圍：國貿局派駐業務、商業司派駐業務、中小企業處派駐業務、加工出口區派駐業務
稽核成員：稽核員-A、稽核員-B

時間	稽核成員	受稽單位	備註
9:00-9:30	All	**啟始會議**	
9:30-12:00	**稽核員-A** **稽核員-B**	**國貿局派駐** **商業司派駐**	
12:00-13:30	**休息**		
13:30-15:30	**稽核員-A** **稽核員-B**	**中小企業處派駐** **加工工出口區派駐**	
15:30-16:00	All	**整理稽核發現**	
16:00-16:30	All	**結束會議**	

練習-擬訂稽核計畫

請針對自已單位設計一份稽核計畫(10分鐘)

稽核程序-擬訂查檢項目

- **了解受稽對象的作業流程**
  - 例：經濟部中區聯合服務中心-國貿局派駐業務內容：
    - ✓中部地區廠商申辦貨品輸出入電子簽證應檢附相關文件數量之核扣
    - ✓「廠商擬用之英文名稱預查」 及「出進口廠商登記」案件之受理
    - ✓提供貨品輸出入規定事項、相關書表販售及其他貿易業務相關問題之轉介與答覆
    - ✓配合國貿局辦理中部地區經貿研討會、外貿商機說明會及協助處理服務中心業務
- **辨識與個人資料有關之作業流程**
  - 例：配合國貿局辦理中部地區經貿研討會、外貿商機說明會及協助處理服務中心業務
    - ✓ 研討會/說明會活動辦理作業流程

稽核程序-擬訂查檢項目

- 辨識與個人資料有關之作業流程所涉及之蒐集、處理、利用行為模式
  - 人員
  - 設備
  - 環境
- 確認稽核標準（=經濟部暨所屬機關個人資料保護管理要點）內容
- 擬定查檢項目

稽核標準應為『經濟部暨所屬機關個人資料保護管理要點』非查檢表項目，稽核之執行切勿以查檢項目為依歸

稽核程序-擬訂查檢項目

範例：

經濟部中區聯合服務中心稽核計畫
稽核時間：2014年12月1日
受稽單位：經濟部中區聯合服務中心
稽核範圍：國貿局派駐業務-研討會/說明會活動辦理作業
稽核成員：稽核員-A

稽核項目	稽核內容	稽核結果
蒐集處理利用作業	研討會/說明會活動辦理時，所蒐集之個人是否具備特定目的？	
	研討會/說明會活動辦理時，所蒐集之個人是否具備屬於國貿局的法定職務？	
	蒐集程序是否依規定奉簽核後為之？	
	個人資料之利用，是否符合特定目的之範圍？	

練習-擬訂查檢項目

請依「經濟部個人資料保護管理要點」規定，就「國貿局派駐業務-研討會/說明會活動辦理作業」設計個人資料檔案安全稽核的查檢項目（20分鐘）

稽核程序-執行稽核

◆TOPDOWN or DOWNSTREAM

- 從程序開始
- 例：研討會/說明會活動辦理作業流程

◆BOTTOM UP or UPSTREAM

- 從紀錄開始
- 例：研討會/說明會報名表、研討會/說明會報名清單、研討會/說明會簽到表……

稽核程序-執行稽核

稽核項目	可能符合要求的證據
蒐集、處理、利用作業	1. 個人資料盤點清冊 2. 個人資料蒐集網頁/文件 3. 個人資料提供的公文、信件 4. 個人資料簽奉核定（蒐集、目的外利用、補充/更正、刪除/銷毀、停止處理利用）的公文 5. 當事人書面同意書 6. 延長保存期限的申請公文 7. 刪除/銷毀紀錄
當事人權利行使作業	1. 當事人權利申請、回覆之信件、電話錄音 2. 個人資料簽奉核定（查詢、閱覽、複製本、補充/更正、刪除/銷毀、停止處理利用）的公文 3. 延期審查之書面理由信件 4. 駁回申請之回覆
盤點與風險分析作業	1. 個人資料盤點與風險評估清冊 2. 個人資料檔案公告項目連結 3. 個人資料檔案風險處理對策

稽核程序-執行稽核

稽核項目	可能符合要求的證據
事故通報與應變作業	1. 事故通報紀錄 2. 事故應變小組會議紀錄(3. 事故通知當事人紀錄 4. 事故檢討會議紀錄
委外作業	1. 委外契約 2. 委外稽核紀錄 3. 委外廠商評選紀錄 4. 委外稽核發現事項追蹤紀錄
安全管理作業	1. 已寄送信件之加密 2. 進出入管控之設備/紀錄 3. 人員保密協定 4. 軟硬體設備更新維護紀錄 5. 資料存取紀錄 6. 共用資料夾測試
其他	1. 教育訓練紀錄 2. 各項紀錄保存/調閱清冊

稽核程序-執行稽核

- ◆稽核執行過程中應做筆記，留存必要稽核紀錄。
- ◆發現事實經判斷為不符合時，應有客觀證據支持。
- ◆不符合之事項應歸因於未能：
  - ➢符合「經濟部個人資料保護管理要點」要求
  - ➢其他資訊安全管理要求
- ◆不符合事項之陳述應報括：
  - ➢稽核員發現的事實
  - ➢被抽樣的證據
  - ➢不符合的條文
- ◆稽核紀錄應有雙方簽名確認之紀錄。
- ◆非不符合事項但可列為議題者，亦可列入稽核紀錄中。

稽核程序-執行稽核

範例：

經濟部中區聯合服務中心稽核計畫
稽核時間：2014年12月1日
受稽單位：經濟部中區聯合服務中心
稽核範圍：國貿局派駐業務-研討會/說明會活動辦理作業
稽核成員：稽核員-A

項次	稽核紀錄
1.	**研討會/說明會活動辦理委託ABC法人執行，委託內容包含活動相關之個人資料蒐集、處理、利用作業，但無個人資料委外監督管理紀錄。例：合約編號000123與ABC法人之委外合約未訂定個人資料保護相關條文。本項作業不符合「經濟部暨所屬機關個人資料保護管理要點」第24條規定。**

練習：不符合事項陳述

請參考附件案例，判斷不符合事件，並練習陳述你所發現的不符合事件。(25分鐘)

案例

稽核程序：撰寫稽核報告

一份完整稽核報告應包含稽核專案

- **執行之人、範圍、時地、地點**
- **整體發現事項之說明**
- **各項不符合事項之陳述**
- **其他應說明之事項**

經濟部中區聯合服務中心稽核報告
稽核時間：2014年12月1日
受稽單位：經濟部中區聯合服務中心
稽核範圍：國貿局派駐業務、商業司派駐業務、中小企業處派駐業務、加工出口區派駐業務
稽核成員：稽核員-A、稽核員-B
查核結果：本次查核共發現___項不符合事項。

本報告為機密文件，僅限內部使用。

- 本次訪查係透過與受查單位面談，現場觀察以及文件記錄查閱進行；產業政策組併以隨機抽測方式檢視人員就個人資料保護管理認知。
- 查核共發現**2件**不符合事項：

1. XXXXXXXXXXXXXXXXXX
2. XXXXXXXXXXXXXXXXXXX

- 不符合事項已於查核現場與受查人員進行溝通，並於紀錄上確認簽名。受查單位主管應再進一步追蹤。

練習：編寫稽核報告

請參考附件案例，判斷不符合事件，並練習撰寫稽核報告。

- 本簡報未經授權不得翻印、轉載或以任何方式重製。
- 本簡報之內容不構成任何實質法律意見，如有任何法律諮詢需求，請不吝與我們連繫。

附件：稽核簡介1/2

◆稽核

➢獲取稽核證據(audit evidence)與評估其是否符合稽核準則(audit criteria)之系統化、獨立且制度化程序

◆內部稽核vs.外部稽核

附件：稽核簡介1/2

- ◆稽核準則
  - ➢作為比對稽核證據的參數，包括政策、程序或其他要求
- ◆稽核證據
  - ➢與稽核準則有關的記錄、事實說明或其他資訊
- ◆稽核發現(audit finding)
  - ➢稽核證據與稽核準則相互比對後，所取得的結果
    - ✓符合(conformity)：與稽核準則完全相符合
    - ✓不符合(non- conformity)：與稽核準則不符合
- ◆稽核結論(audit conclusion)
  - ➢於考量稽核目標與所有的稽核發現後，所作成的稽核結果

附件：稽核原則

- ◆正直(integrity)
  - ➢稽核人員應誠實且不偏頗地管理稽核專案(audit program)
- ◆公正呈現(fair presentation)
  - ➢必須真實地與正確地報告稽核證據、稽核發現與稽核結論
- ◆專業上應有之注意(due professional care)
  - ➢以合理且謹慎的態度進行稽核
- ◆機密性(confidentiality)
  - ➢確保資訊之安全，妥適地處理或使用敏感性或機密性資訊
- ◆獨立性(independence)
  - ➢中立且客觀地進行稽核與做成結論
- ◆以證據為基礎的方式(evidence –based approach)