

公務機關因應個資法之策略與作法

楊光華 研究員
資訊工業策進會 科技法律研究所
ywenly59@iii.org.tw

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

© 2012資訊工業策進會

大綱

- 個資保護管理步驟方法論
- 個資保護管理步驟建置流程

© 2012資訊工業策進會

個資保護管理步驟方法論

結合個人資料保護法規與機關個人資料保護管理的步驟

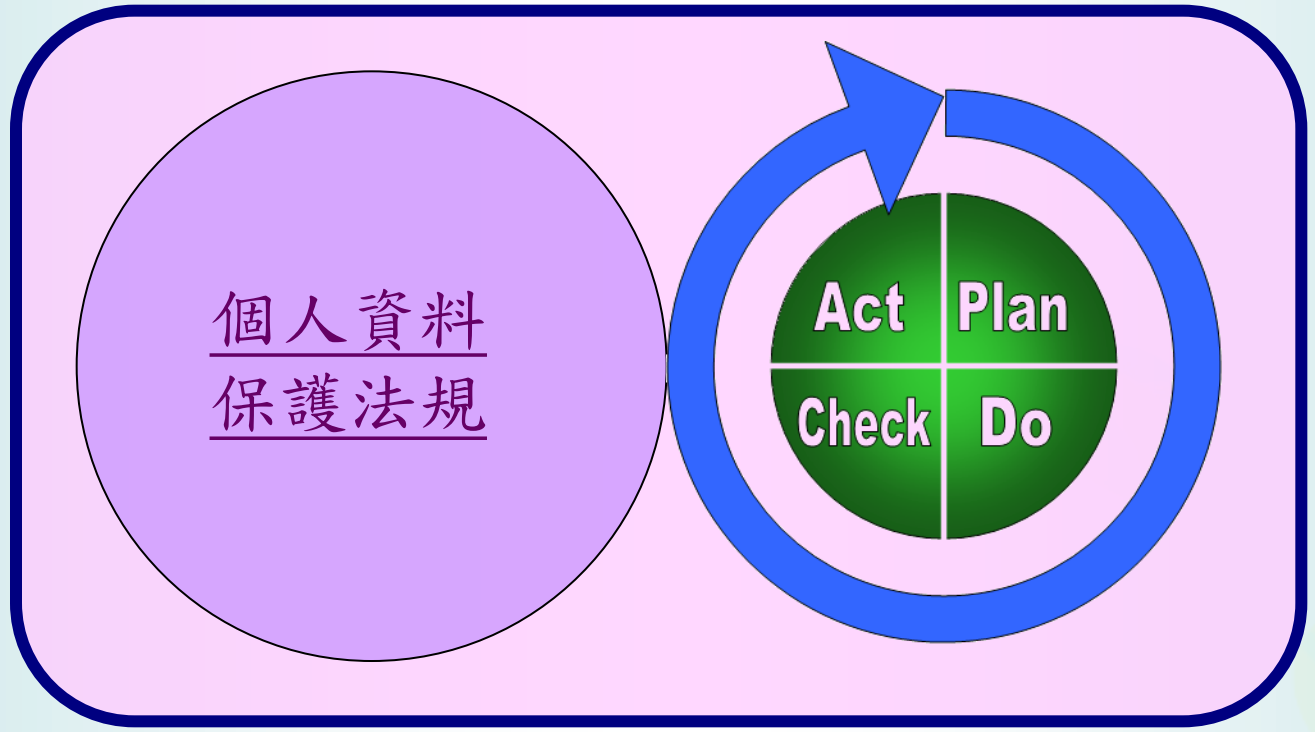
有效因應個資保護法令變動，契合法令規範

蒐集

處理

利用

國際傳輸



Plan

Do

Check

Act

將法律要求轉化為內部作業管理流程的控制點

© 2012資訊工業策進會

PDCA方法論下的管理步驟

訂定個資保護管理政策
成立執行小組
製作作業時程表
公告個資保護管理政策
盤點法規命令
盤點個人資料
風險評估與擬定風險對策
配置資源
訂定個人資料管理作業程序

Plan

Do

運作個資保護管理制度
實施教育訓練

Check

機關內部管理權責
文件記錄控管
內部稽核

Action

持續改善

資料來源：資策會科技法律研究所

© 2012資訊工業策進會

個資法與個資保護管理步驟項目對照

	個人資料保護法	管理制度項目
事業應訂定相關事項之規範與流程	§10當事人請求提供資料之權利	個人資料當事人相關權利
委外處理	§4委外視同委託機關	委託處理個人資料之監督
特種個人資料之蒐集、處理與利用	§6 特種個人資料之蒐集、處理及利用	特種個人資料之蒐集、處理及利用限制
告知事項	§§8、9告知事項	告知義務之履行
資料正確性之主動維護	§11事業主動維護資料正確	維護個人資料之正確性
個人資料之蒐集、處理與利用	§§19、20蒐集、處理及利用	合法、正當具連結性蒐集、處理之作業規範 利用之作業規範

© 2012資訊工業策進會

個資法與個資保護管理步驟項目對照

	個人資料保護法	個資保護步驟項目
特定目的與利用範圍變更告知	§20特定目的外利用	特定目的與利用範圍變更之告知
教育訓練及基礎設施之建立	§27 I 安全措施建立	教育訓練
內部安全措施採行之必要	§ 27 I 安全措施建立	安全管理措施
外部主管機關要求計畫訂定	§27 II 主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法	安全管理措施 機關人員監督 委託處理個人資料之監督

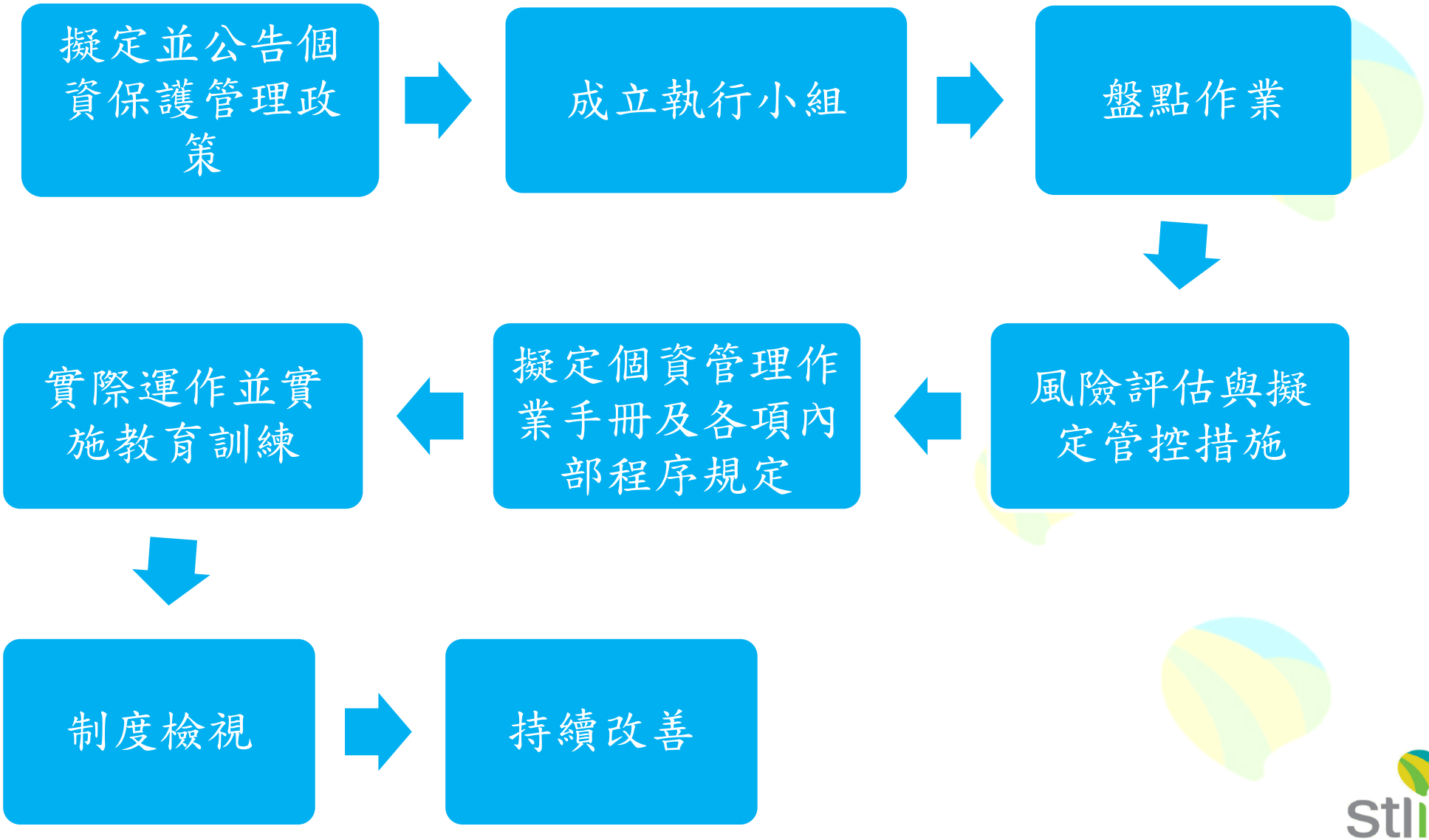
© 2012資訊工業策進會

大綱

- 個資管理步驟方法論
- 個資管理步驟建置流程

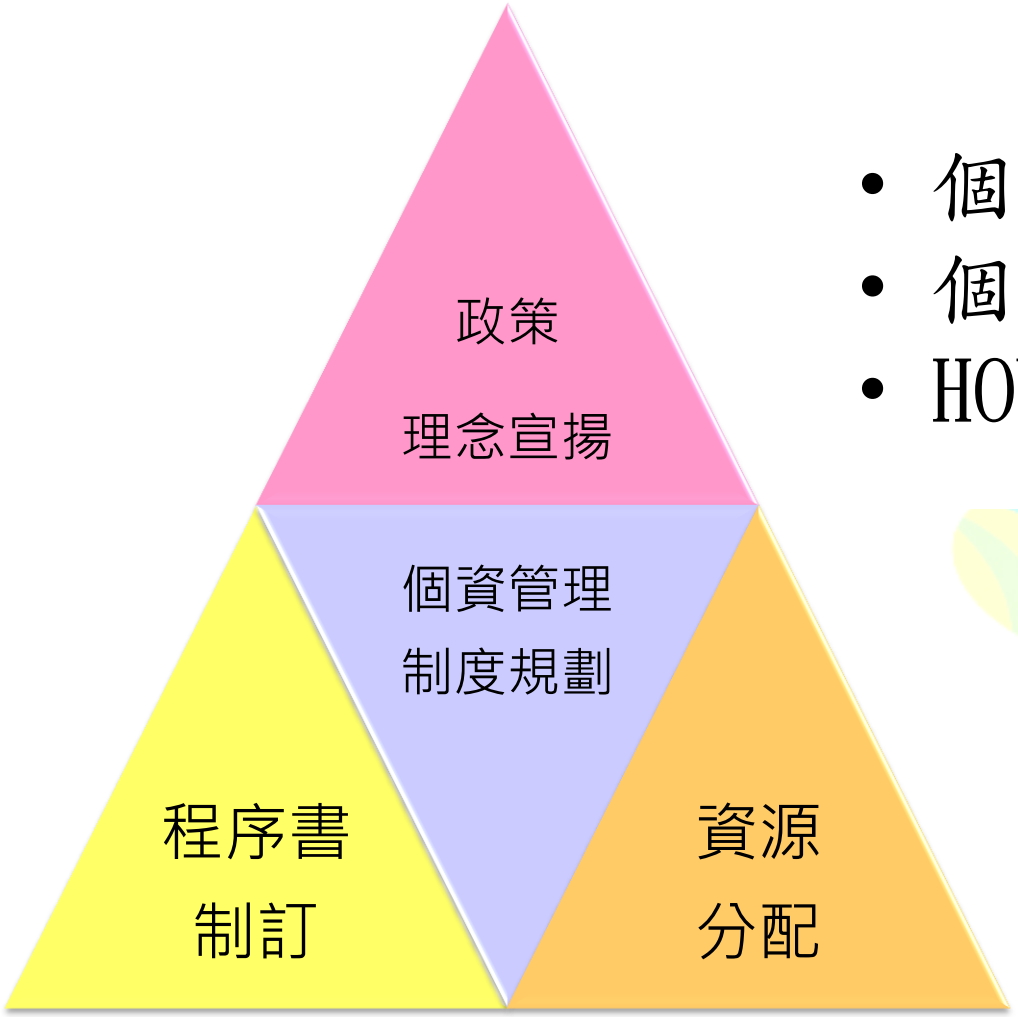
© 2012資訊工業策進會

個資保護管理步驟建置流程



© 2012資訊工業策進會

擬定個資保護管理政策（1）



- 個資保護WHY
- 個資保護HOW
- HOW TO DO

© 2012資訊工業策進會

擬定個資保護管理政策（2）

- 由機關代表人就下列事項對機關內外部宣示：
  - 遵守個人資料保護法或其他有關個人資料保護之規範
  - 依告知當事人之特定目的與機關法定職務之必要範圍內蒐集、處理個人資料，並不為目的外利用
  - 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
  - 對應當事人權利行使及有關個人資料保護之申訴、諮詢
  - 持續維運改善個資保護管理作業

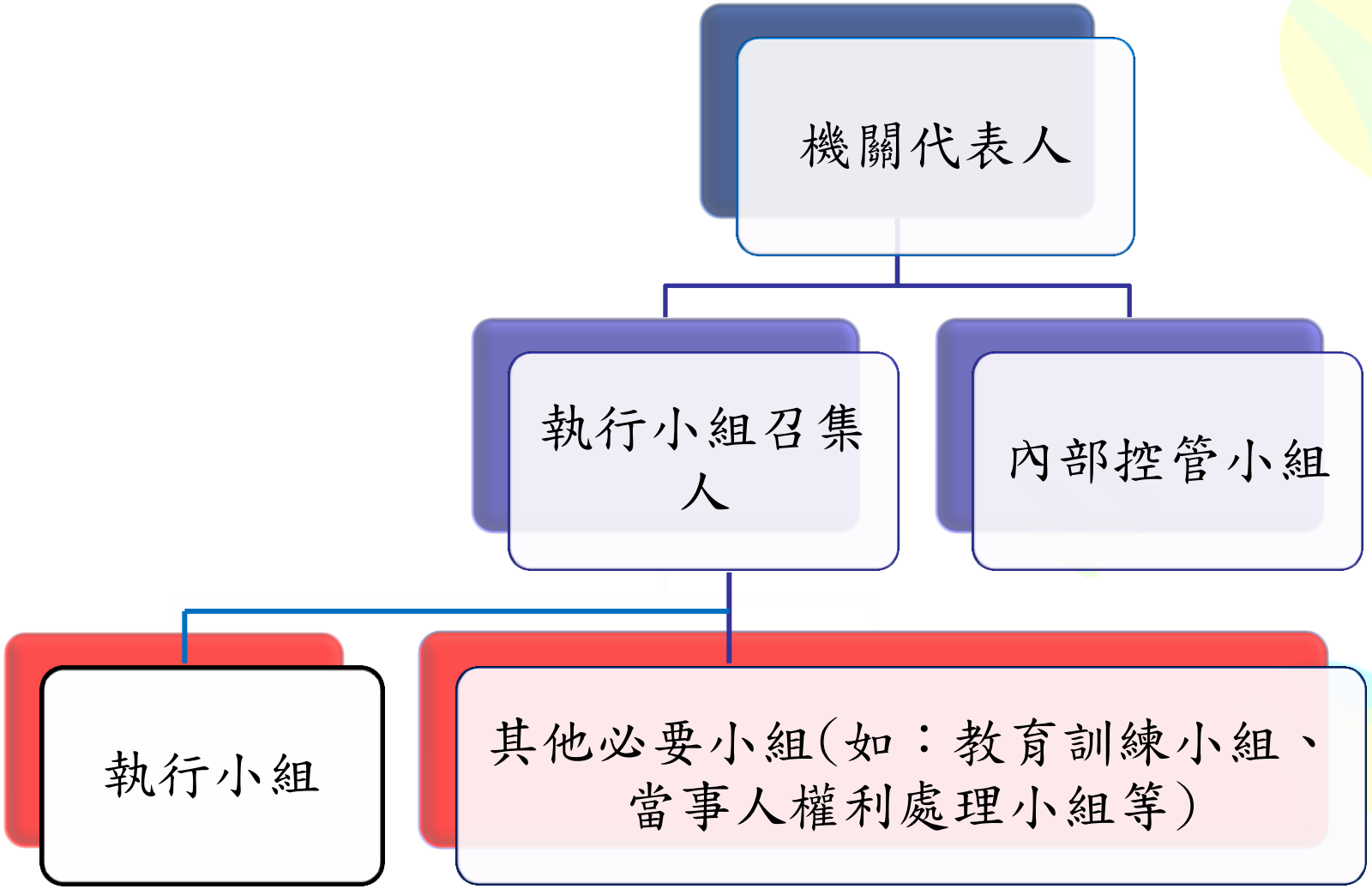
© 2012資訊工業策進會

成立執行小組（1）

- 「電腦處理個人資料保護法施行細則」修正草案第9條第2項第1款：成立管理組織、配置相當資源
- 重要事項：
  - 建立組織架構及擬定權責劃分規則
  - 管理組織架構及權責分工：選擇執行小組成員
  - 配置相當資源：執行小組成員接受個資保護管理教育訓練費用或引進輔導顧問服務費用

© 2012資訊工業策進會

成立執行小組（2）



© 2012資訊工業策進會

盤點作業（1）

◆法規盤點

- ➢ 盤點個人資料保護法規、行政院所屬各機關之個人資料檔案安全維護計畫、管理制度標準及其他相關規範
- ➢ 重要事項：
  - ✓ 建立法規盤點作業程序規則
  - ✓ 建立法規盤點清冊
  - ✓ 依法令變動情形定期或不定期檢視修訂法規盤點清冊

© 2012資訊工業策進會

盤點作業（2）

法規分類	法規名稱	主管機關	制訂/修正	適用範圍	特殊規定	備註
個人資料	個人資料保護法	法務部	99/5/26修正	所有機關	由主管機關訂定個人資料檔案安全維護計畫	預定101/10/1施行
個人資料	公職人員財產申報法	法務部	99/1/9修正	第二條人的範圍	第十六條：申報人喪失第二條所定應申報財產之身分者，其申報之資料**應保存五年**，期滿應予銷毀。但經司法機關或監察機關依法通知留存者，不在此限。 前項期限，自申報人喪失所定應申報財產身分之翌日起算。	
資訊安全	行政院及所屬機關資訊安全管理規範	行政院研考會	1999/11/16頒佈	行政院及所屬機關		

© 2012資訊工業策進會

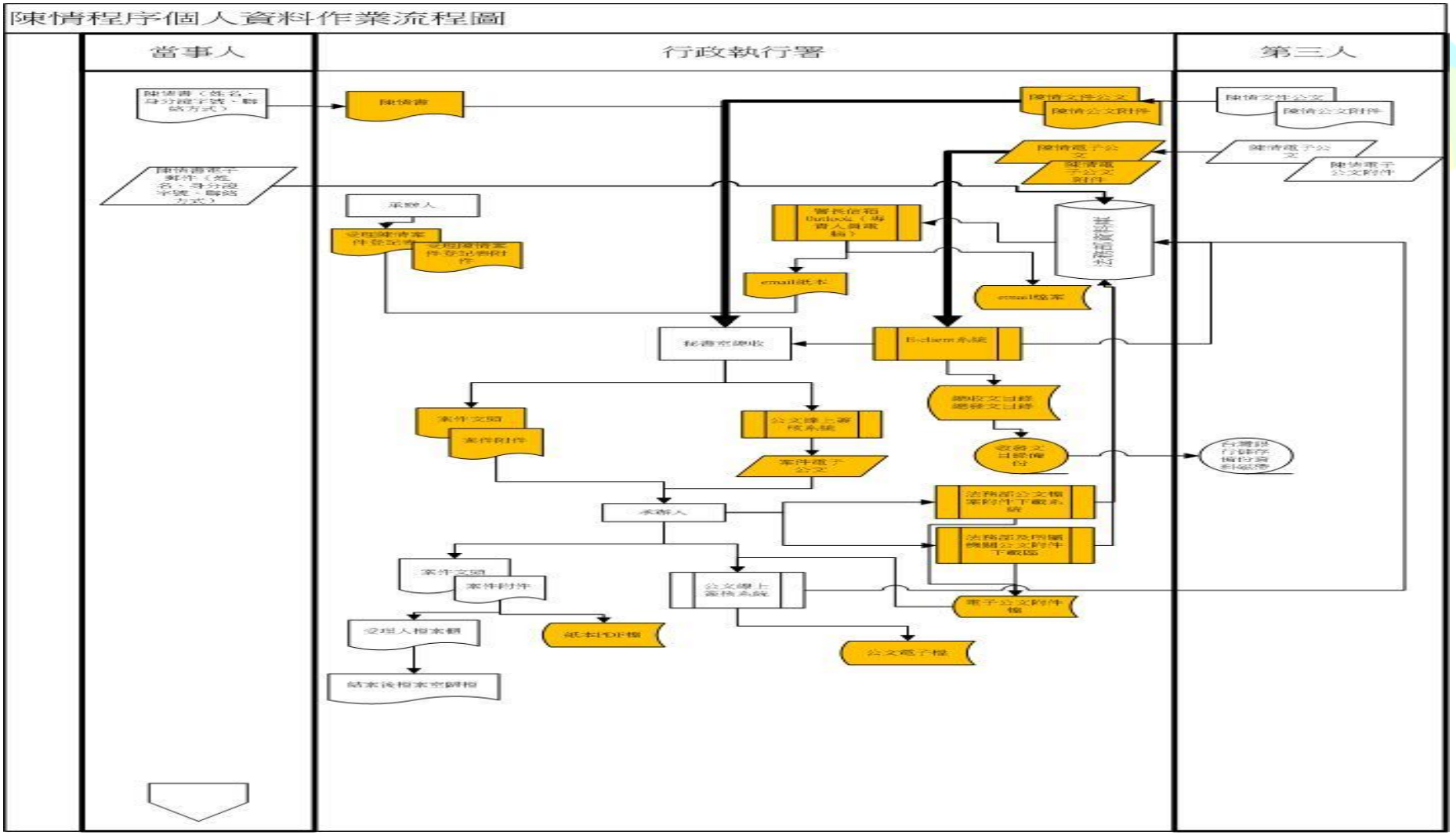
盤點作業（3）

◆個資盤點

- 「電腦處理個人資料保護法施行細則」修正草案第9條第2項第2款：界定個人資料之範圍
- 重要事項：
  - ✓ 建立個資盤點程序作業規則
  - ✓ 盤點個人資料檔案
  - ✓ 個人資料作業流程
  - ✓ 建立個資盤點清冊
  - ✓ 定期或不定期依機關組織法定職務變動檢視修訂個人資料作業流程及個資盤點清冊

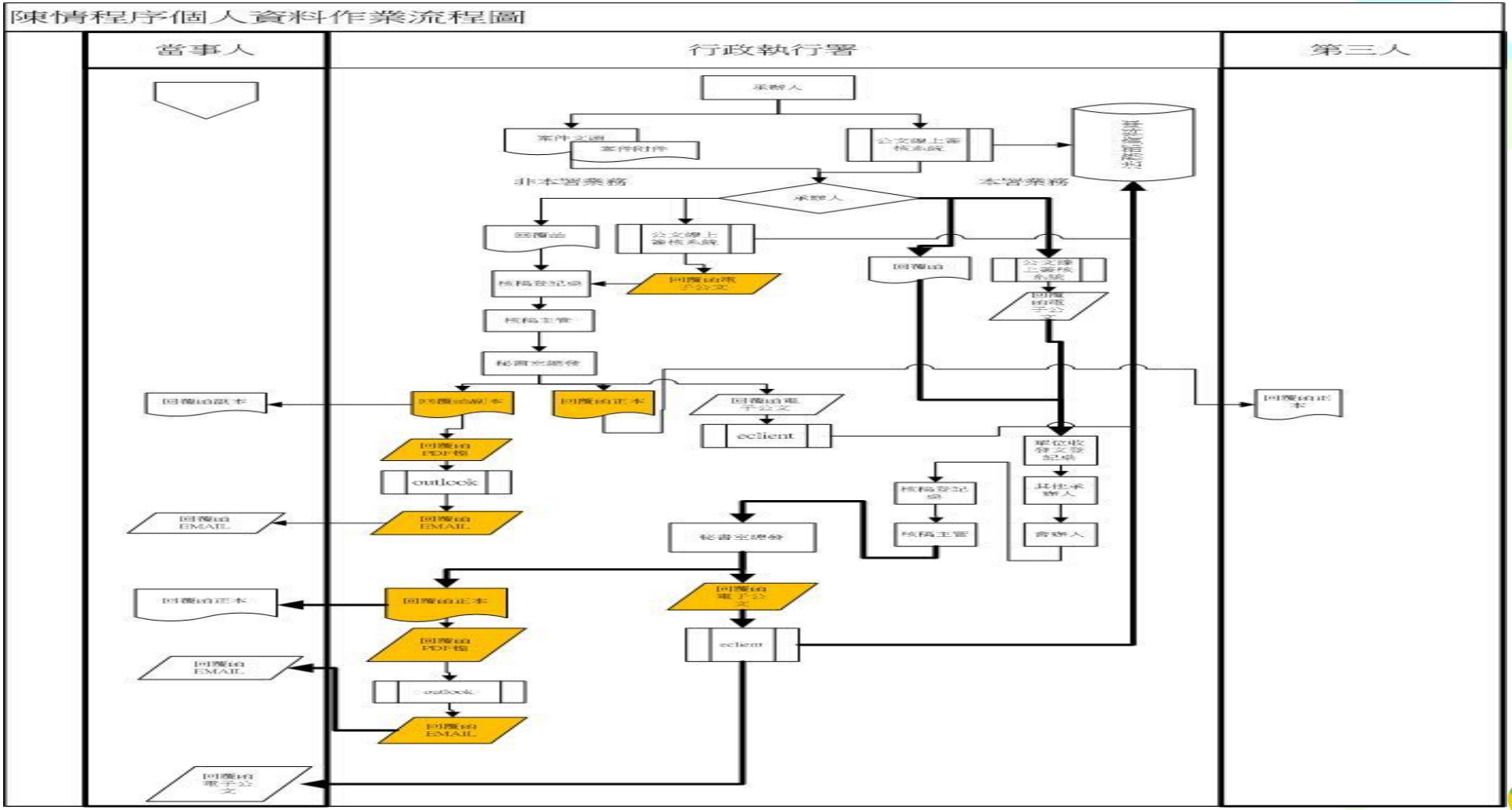
© 2012資訊工業策進會

盤點作業（4）



© 2012資訊工業策進會

盤點作業（5）



© 2012資訊工業策進會

盤點作業（6）

範例：法務部「各單位內部保有及管理個人資料之項目彙整表」

項目 / 單位名稱	個人資料檔案名稱	法律依據	特定目的	個人資料類別	個人資料之範圍	有否特種資料？何種特種資料？	有無監督管理之非公務機關及其名稱

© 2012資訊工業策進會

風險評估與擬定管控措施（1）

- 「電腦處理個人資料保護法施行細則」修正草案第9條第2項第3款：個人資料之風險評估及管理機制
- 重要事項
  - 建立風險評估作業程序規則
  - 建立風險評估清冊
  - 定期或不定期檢視修訂風險評估清冊

© 2012資訊工業策進會

風險評估與擬定管控措施（2）

新增業務

個資盤點清冊

風險分析的程序

- 明確個人資料作業的業務內容
- 明確個人資料作業內容
- 認識作業情境上的風險
- 擬定風險對策
- 反映到相關公司內部規則
- 掌握剩餘風險

風險評估清冊

核決風險評估清冊

© 2012資訊工業策進會

風險評估與擬定管控措施（3）

◆明確個人資料作業內容

陳情作業流程資料		＜陳情處理流程＞
＜陳情作業流程＞		①蒐集 ↓ ②輸入 ↓ ③處理（分文） ↓ ④利用（擬回覆函） ↓ ⑤傳遞（） ↓ ⑥保管・銷毀
提出陳情 ↓ 受理 ↓ 分文 ↓ 處理陳情 ↓ 發函回覆	＜個資盤點清冊＞ 1. 陳情書(紙本媒體) 2. 由網路或首長電子信箱所收到的陳情郵件	

© 2012資訊工業策進會

風險管控措施（5）

情境	個人資料檔案名稱	風險類型	具體風險	對策	公司內部規則	剩餘風險
蒐集	履歷表、人事基本資料表、學歷證件	□違法 □目的外利用 □竊取 □竄改 □毀損 □滅失 □洩漏	未為告知或未同意行銷 紙本遭竊 紙本資料遺失 紙本資料外洩			
利用	筆試成績、面試成績	□違法 □目的外利用 □竊取 □竄改 □毀損 □滅失 □洩漏	未為告知或未同意行銷 紙本遭竊 紙本資料遺失 紙本資料外洩			

© 2012資訊工業策進會

擬定內部各項程序規定（1）

- 內部程序規則項目
  - 緊急事故應變程序
  - 個人資料蒐集處理、利用作業程序
  - 當事人權利行使及申訴諮詢程序
  - 個人資料安全管理程序
  - 教育訓練
  - 個人資料管理制度文件記錄管理程序
  - 內部控管
  - 改善及預防制度之持續改善

© 2012資訊工業策進會

擬定內部各項程序規定（2）

◆緊急應變措施

➢「電腦處理個人資料保護法施行細則」修正草案第9條第2項第4款：事故之預防、通報及應變機制

➢重要事項

✓訂定緊急事故作業程序

✓緊急事故處理權限及單位

✓查明後告知當事人使知悉事故發生之方式，並提供後續查詢與處理管道

✓ 防止損害擴大方法

✓ 避免類似事故再次發生方法

✓ 事故通報機制

© 2012資訊工業策進會

擬定內部各項程序規定（3-1）

◆蒐集、處理及利用作業程序

➢重要事項

✓蒐集、處理利用之原則

- ■尊重當事人之權益
- ■依誠實及信用方法
- ■不得逾越特定目的之必要範圍
- ■與蒐集之目的具有正當合理之關聯

✓行銷時特別應注意

- ■行銷時應於蒐集之特定目的必要範圍內
- ■當事人表示拒絕接受行銷時 ，應即停止利用其個人資料行銷
- ■於首次行銷時，提供當事人表示拒絕接受行銷之方式，並支付所需費用

✓確認蒐集、處理及利用符合個人資料保護法第19條之特定情形

✓資料安全控管作業流程

© 2012資訊工業策進會

擬定內部各項程序規定（3-2）

◆蒐集、處理及利用作業程序

➢ 重要事項

- ✓ 確認蒐集已符合個人資料保護法第8、9條
  - ■ 直接蒐集時告知事項完整性
  - ■ 直接蒐集時之告知時點
  - ■ 直接蒐集時免為告知之確定
  - ■ 間接蒐集時告知事項完整性
  - ■ 間接蒐集時之告知時點
  - ■ 間接蒐集免為告知之確定
  - ■ 以書面、電話、傳真、電子文件或其他適當方式告知

© 2012資訊工業策進會

擬定內部各項程序規定（4）

◆當事人權利行使

➢重要事項

- ✓訂定當事人權利行使之程序規則
- ✓確認依法得不回應當事人權利行使之程序
- ✓當事人提出權利行使之窗口
- ✓當事人權利行使之書面或方法
- ✓確認當事人本人或其代理人之方法
- ✓回覆當事人權利行使之期間

© 2012資訊工業策進會

擬定內部各項程序規定（5-1）

- 安全管理措施
  - 重要事項
    - ✓ 資料安全管理
    - ✓ 設備安全管理

© 2012資訊工業策進會

擬定內部各項程序規定（5-2）

◆安全管理措施

- ➢ 例：保險業個人資料檔案安全維護計畫標準
  - ✓ 保險業應指定專人負責管理電腦設備，並加強安全防護措施。
  - ✓ 保險業對個人資料檔案之主機、週邊設備及相關設施等電腦設備，應加強天然災害及其他意外災害之防護。
  - ✓ 保險業對於儲藏個人資料檔案之磁碟、磁帶等媒體，應責成專人管理，並建立備援制度。
  - ✓ 個人資料之輸出入，均應建立識別碼、通行碼之管理制度；重要之個人資料，並應加設資料存取控制。前項識別碼及通行碼，應視需要經常更新。

© 2012資訊工業策進會

擬定內部各項程序規定（5-3）

◆安全管理措施

➢例：保險業電子商務紀錄保存及內部控制管理自律規範第7條網路設備安全防護

- ✓ 所有網路硬體設備應安置於安全地點
- ✓ 安置網路硬體設備之地點應加裝不斷電系統或備用發電機，並依法令規定設置必要及合格之消防安全設施
- ✓ 安置網路硬體設備之地點應建立安全維護及人員進出之控管機制

© 2012資訊工業策進會

擬定內部各項程序規定（5-4）

◆安全管理措施

➢例：保險業電子商務紀錄保存及內部控制管理自律規範第九條電子商務資訊安全管理

- ✓ 保險業應訂定網路安全規劃與管理作業，以達成整體網路作業之安全管理
- ✓ 網路安全政策
- ✓ 網路安全服務管理
- ✓ 網路安全連結
- ✓ 主機與要保人端設備安全防護
- ✓ 身分識別和驗證

© 2012資訊工業策進會

擬定內部各項程序規定（5-5）

◆安全管理措施

➢例：保險業電子商務紀錄保存及內部控制管理自律規範第九條電子商務資訊安全管理

- ✓網域劃分與安全控制
- ✓ 防火牆安全管理
- ✓ 遠端連線控制
- ✓ 網路安全監控
- ✓ 監控處理程序
- ✓ 事件安全記錄
- ✓ 入侵偵測檢視
- ✓ 防範電腦病毒及惡意軟體之攻擊

© 2012資訊工業策進會

擬定內部各項程序規定（6-1）

◆委外監督

➢ 重要事項

- ✓與委託人確定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間
- ✓與委託人確定應採取之必要措施
- ✓非有必要不為複委託
- ✓與委託人確定違反個人資料保護法規或委託契約條款時，應向委託人通知之事項及採行之補救措施
- ✓與委託人確定其他保留指示之事項

© 2012資訊工業策進會

擬定內部各項程序規定（6-2）

◆委外監督

➢重要事項

- ✓於委託關係終止或解除時，返還個人資料載體及刪除儲存於所持有個人資料之刪除
- ✓與委託人確認定期執行之狀況，並提出記錄確認結果
- ✓確認委託人指示之範圍內為蒐集、處理或利用個人資料
- ✓認委託人之指示有違反個人資料保護法或個人資料保護之相關法規命令應立刻通知委託人

© 2012資訊工業策進會

擬定內部各項程序規定（6-3）

◆委外監督

➢例：保險業電子商務紀錄保存及內部安全控制作業管理自律規範第11條委外處理

- ✓ 簽訂電子商務之租購或資訊作業委外服務計劃書。
- ✓ 慎選具有足夠安全管理能力及經驗之廠商作為委辦對象。
- ✓ 事前審慎評估可能潛在之各項風險。
- ✓ 與委外廠商簽訂適當的資訊安全協定及課予相關安全管理責任，並納入契約條款。
- ✓ 逐年檢討評估委外廠商之履約情形，如有未履行或未達約定之服務水準者，應要求檢討改進，必要時得終止部分或全部契約，並依法追究其責任。

© 2012資訊工業策進會

擬定內部各項程序規定（7）

◆教育訓練

➢ 重點事項

- ✓ 建立教育訓練計畫
- ✓ 教育訓練重點應包含：
  - ■ 個人資料保護的重要性及做到個人資料保護的優點
  - ■ 在個人資料保護中所擔任的角色與責任
  - ■ 違反個人資料保護時可能受到的處罰
- ✓ 確認機關職員參加教育訓練成果的機制
- ✓ 按當年度教育訓練計畫實施結果檢視修正下一年度教育訓練計畫之程序

© 2012資訊工業策進會

擬定內部各項程序規定（8）

◆個人資料管理制度文件記錄管理程序

➢重要事項

✓確定文件紀錄之適用範圍

✓文件修訂與版本變更時之作法與權責

✓文件之保存、公佈及所時得供職員查詢之處所

✓紀錄製作與保存之權責

✓紀錄查驗與紀錄真實性

© 2012資訊工業策進會

擬定內部各項程序規定（9-1）

◆內部控管：「電腦處理個人資料保護法施行細則」第9條第2項第9款「資料安全稽核機制」

- 重要事項
  - ✓ 建立內部控管計畫
  - ✓ 內部控管之公正性與獨立性
  - ✓ 確認內部控管成果之機制
  - ✓ 按當年度內部控管之實施結果檢視修正下一年度整體個資管理步驟之實施

© 2012資訊工業策進會

擬定內部各項程序規定（9-2）

◆內部控管

➢例：保險業電子商務紀錄保存及內部安全控制作業管理自律規範 第12條電子商務安全稽核

- ✓ 是否留有足供安全稽核之記錄資訊。
- ✓ 是否已建立防範不法入侵之機制。
- ✓ 是否已建立安全修復機制。
- ✓ 是否有定期更新修補程式。
- ✓ 是否已建立警示系統，對於安全違例事件的發生能立即採取有效防範措施。

© 2012資訊工業策進會

擬定內部各項程序規定（10）

◆改善及預防制度之持續改善

➢重要事項

- ✓建立改善及預防制度之持續改善機制
- ✓確認改善及預防制度之持續改善之查檢項目
- ✓確認改善及預防制度之持續改善之方法
- ✓確認改善及預防制度之持續改善方法之有效性
- ✓按確認改善及預防制度之持續改善之結果修正整體個資管理步驟之實施

© 2012資訊工業策進會

感謝聆聽
敬請指教

© 2012資訊工業策進會