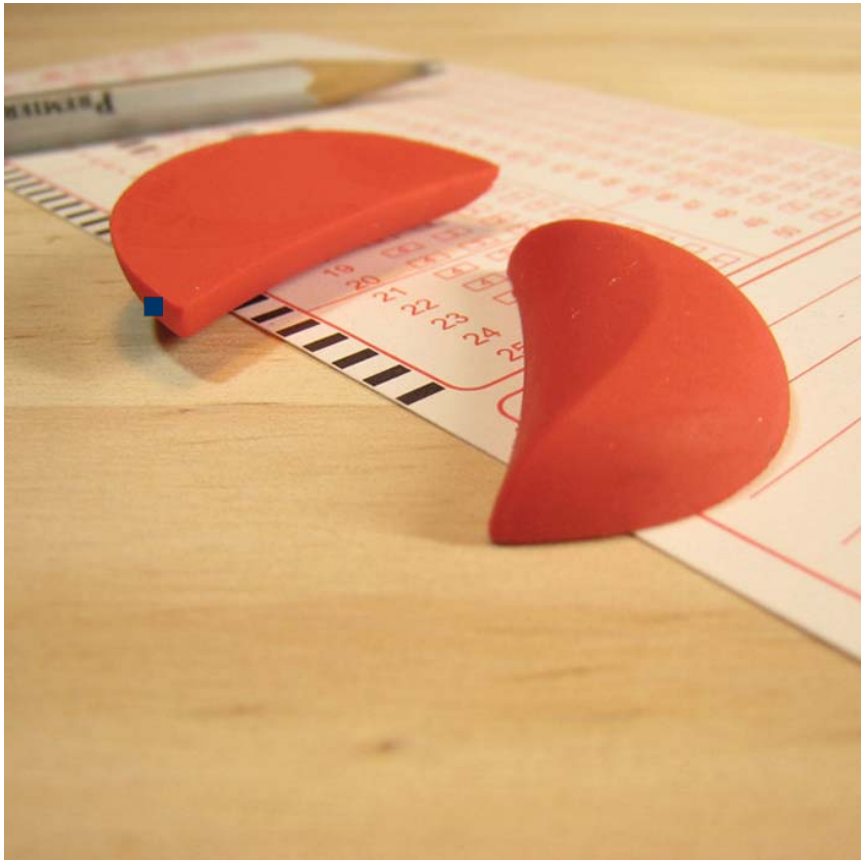
個人資料保護法對教育(公立)機關之衝擊與因應對策

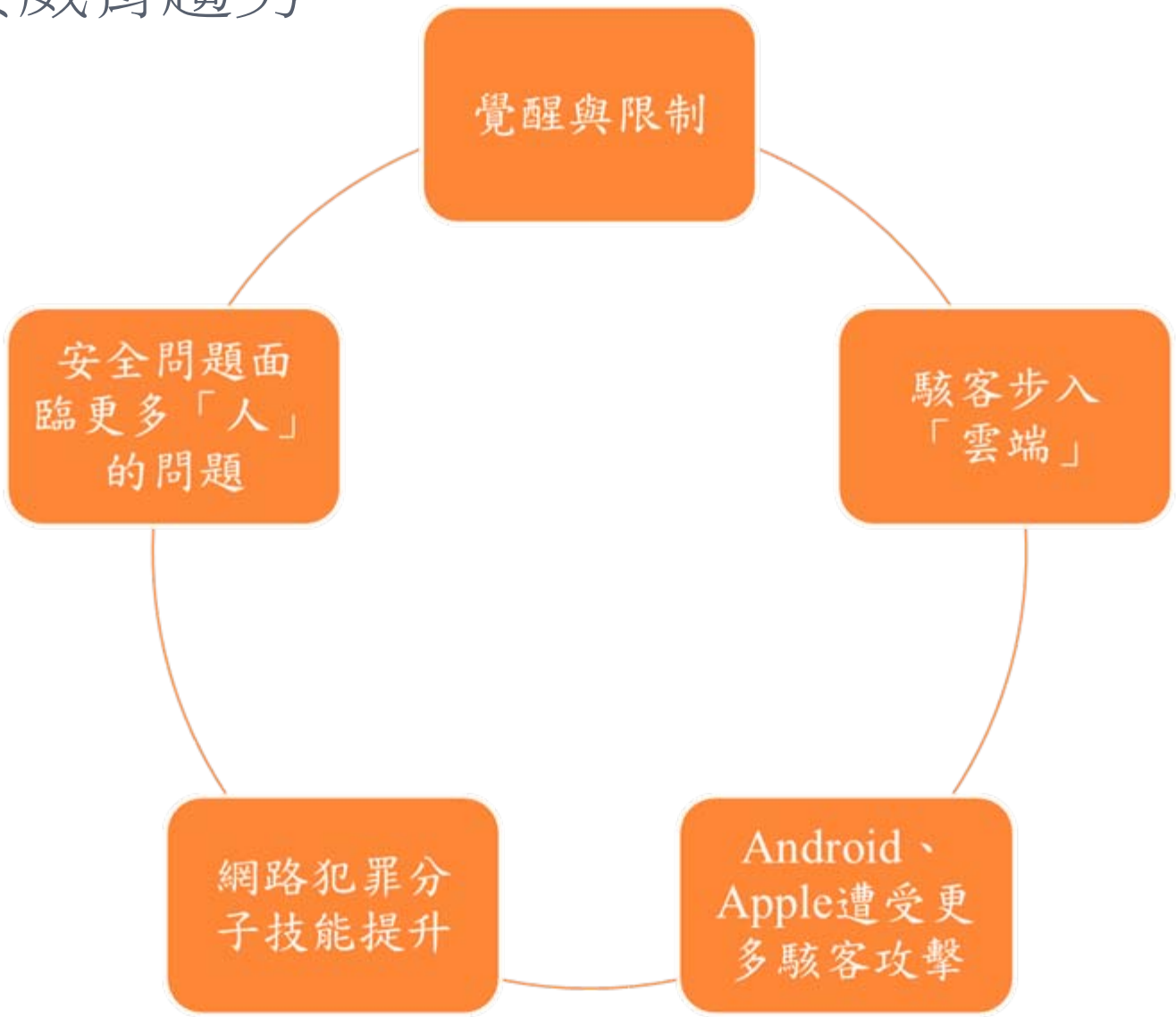
AGENDA

- Topic
  - 資訊安全與威脅趨勢
  - 個資外洩案例討論
  - 新版個人資料保護法
  - 影響評估與因應策略

資訊安全與威脅趨勢



資安威脅趨勢


覺醒與限制
駭客步入「雲端」
Android、Apple遭受更多駭客攻擊
網路犯罪分子技能提升
安全問題面臨更多「人」的問題

網路犯罪分子技能提升

安全問題面臨更多「人」的問題

【國際中心／綜合報導】英國的最高反恐警官，8日不慎讓警方欲逮捕的恐怖份子嫌犯名單與行動細節曝光，為免夜長夢多，警方於是提前於8日晚即兵分多路展開逮捕行動，約有12人被捕，洩密警官遭反對黨嚴批後辭職謝罪。

倫敦警察總局主管反恐任務的助理局長奎克（Bob Quick），8日前往唐寧街首相府做一項簡報，下車時手上拿的反恐機密文件內容翻在外面，結果被首相府外的攝影記者拍得一清二楚，且快速對外傳播。

英國的反恐最高階警官奎克8日丟官，全因他手上抱著的這份文件。奎克於首相府前下車，手上的反恐機密文件被攝影記者拍個正著，內容一清二處，還登上英國所有報紙頭版，當局因此被迫提前展開一項反恐逮捕行動。

（取材自網路、法新社）

個資外洩案例討論

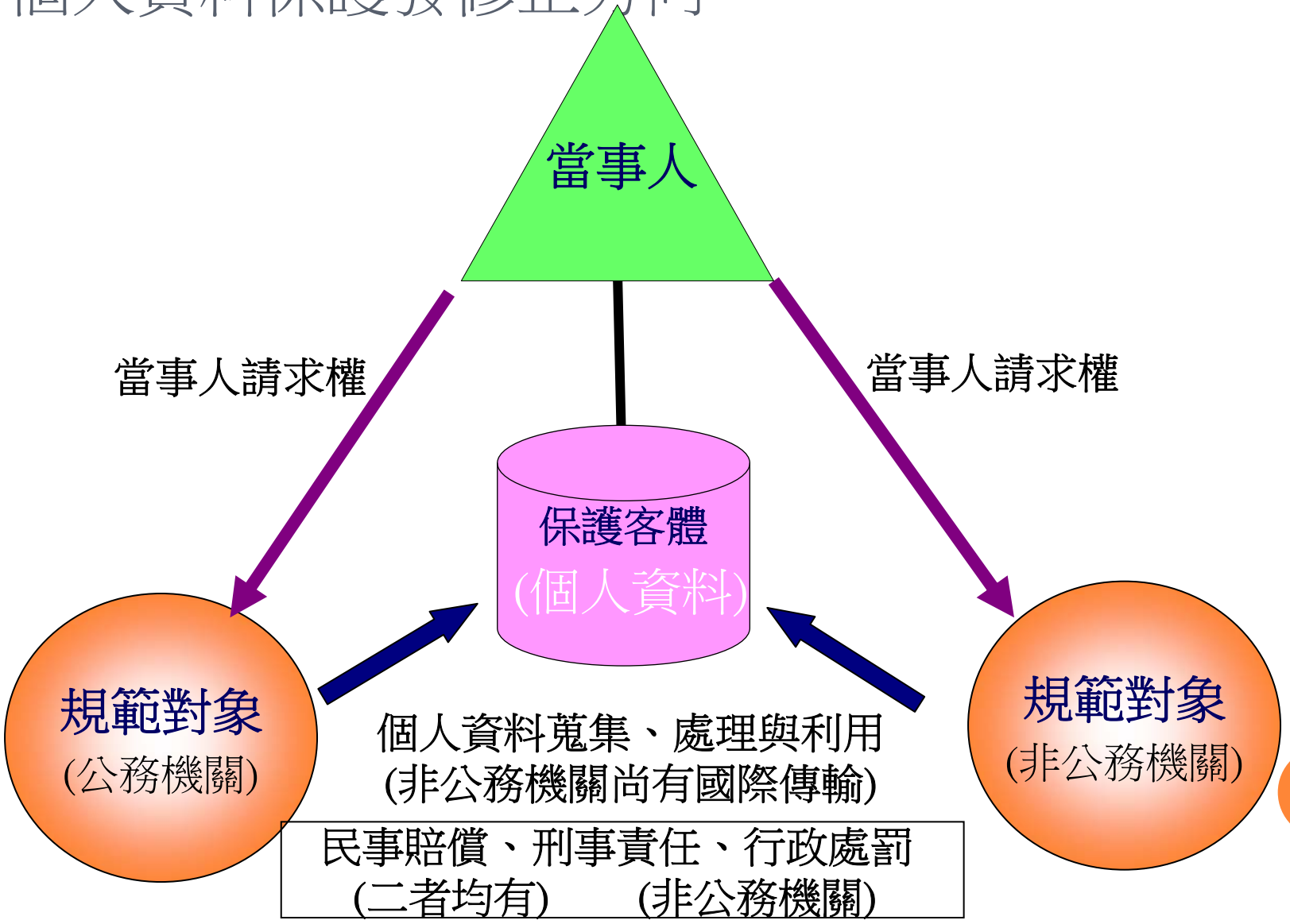
SONY PSN(1/2)

- 頭條新聞速報>SONY將於1日召開記者會-說明PSN個資被竊狀況
- 2011年5月1日 11:00 ｜記者湯蕙如／綜合報導
- 針對 PlayStation Network 因被入侵恐導致最多 7700 萬份個資流出一事，Sony 於 4 月 30 日確定將於 5 月 1 日 14：00（台灣時間 13：00）召開記者會說明，並由 Sony 執行副總裁暨索尼電腦娛樂（SCE）總裁平井一夫出席主持，解釋並說明 PSN 目前針對入侵和個資外洩狀況、服務重新上線時程等。
- 自 20 日 SONY 旗下提供遊戲軟體為主的 PlayStation Network 和音樂影像多媒體的 Qriocity 遭入侵後相階停服；緊接著在 27 日官方發表聲明，坦言相關用戶的個資可能遭受駭客竊取，雖然信用卡資料有加密保護，原始資料難以洩漏，但仍呼籲使用者留心近期內的付款紀錄。

SONY PSN(2/2)

- 這起事件造成各國政府與業界關注，根據華爾街日報日前推估，SONY 這次的個資外洩事件，光是賠償金額就可能花費 2 兆日圓，這些還不包括相關社會責任和社內的責任歸屬問題，預計這起事件將是 SONY 空前危機。
- 原文網址: SONY將於1日召開記者會　說明PSN個資被竊狀況 | 頭條新聞 | NOWnews 今日新聞網 http://www.nownews.com/2011/05/01/11490-2709094.htm#ixzz1N47uxZny

個人資料保護發修正方向



保護客體(1/5)

- 保護客體
  - 新法：個人資料
  - 舊法：電腦處理之個人資料

保護客體(2/5)

- 保護客體
  - 當事人之個人資料
    - 當事人
    - 指個人資料之本人。
    - 現行法上所稱之當事人，以自然人為限，不包括法人之資料 (公司法、營業秘密法等) 。
    - 自然人又以尚生存之自然人為限，不包括死亡者之個人資料。

保護客體(3/5)

- 個人資料之定義

個人資料保護法	電腦處理個人資料保護法
第二條　本法用詞，定義如下： 一、個人資料：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。 (下略)	第三條　本法用詞定義如左： 一、個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。 (下略)

保護客體(4/5)

- 新法增訂舊法所無之「特種資料」概念

個人資料保護法	電腦處理個人資料保護法
第六條　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。但有下列情形之一者，不在此限： 一、法律明文規定。 二、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，且有適當安全維護措施。 三、當事人自行公開或其他已合法公開之個人資料 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，且經一定程序所為蒐集、處理或利用之個人資料。 前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。	

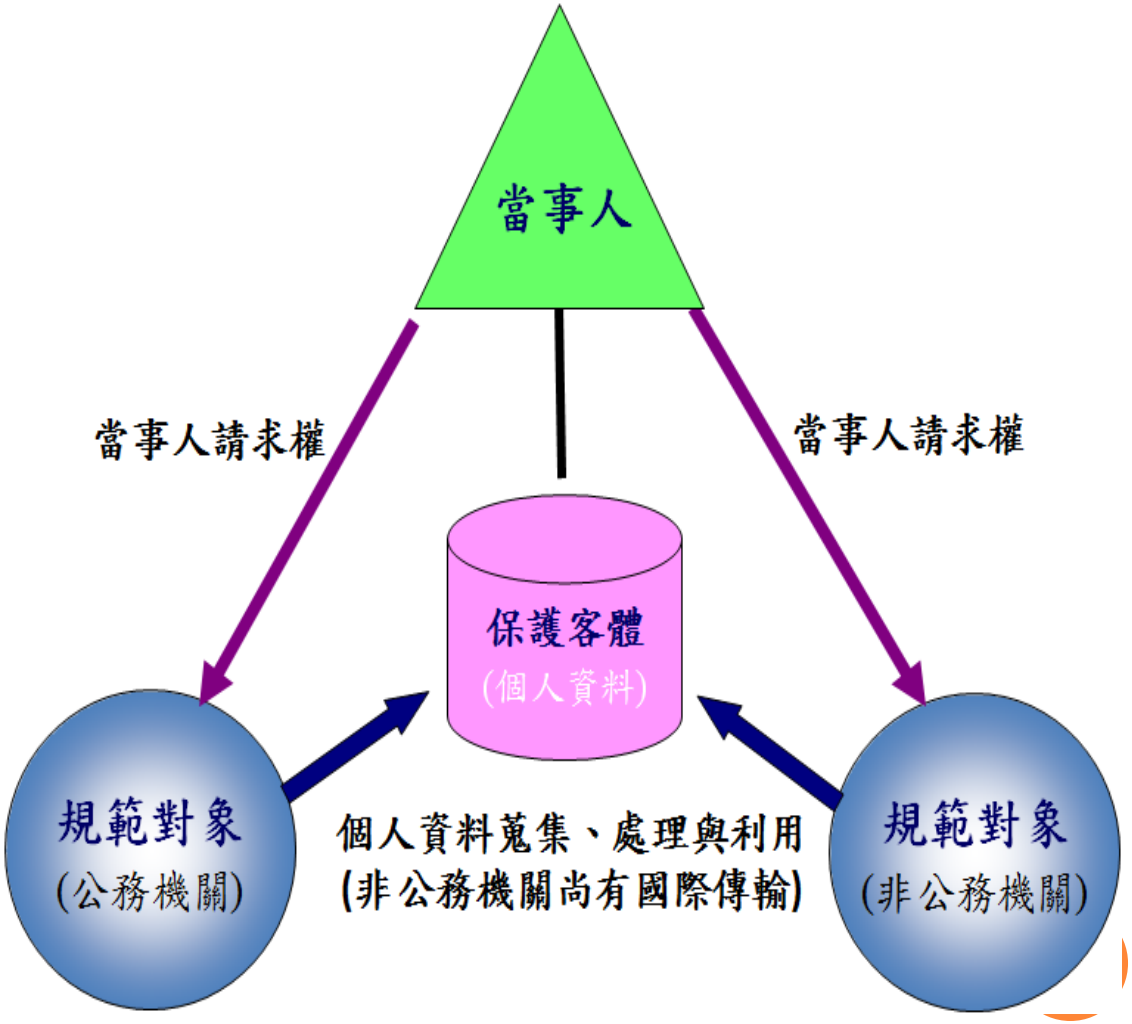
保護客體(5/5)

- 原則：不得蒐集、處理或利用特種資料。
- 例外：下列四者

法律明文規定	
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，且有適當安全維護措施	
當事人自行公開或其他已合法公開之個人資料	
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，且經一定程序所為蒐集、處理或利用之個人資料	前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之

受規範之主體(1/5)

- 受規範之主體
  - 公務機關。
  - 非公務機關。



受規範之主體(2/5)

- 電腦處理個人資料保護法
  - 公務機關
  - 　依法行使公權力之中央或地方機關。
  - 非公務機關
  - 　公務機關以外之事業、團體或個人
    - 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人
    - 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業
    - 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人

受規範之主體(3/5)

- 經指定之事業、團體或個人
  - 實務上業經指定之例
    - 百貨公司業。
    - 零售式量販業。
    - 私立就業服務機構。
    - 期貨業。
    - 不動產經紀業。
  - 經濟部與法務部於99年2月22日會銜公告，指定「無店面零售業」(網路購物及型錄購物)自99年7月1日起，適用電腦處理個人資料保護法。

受規範之主體(4/5)

- 過往被指定之事業，須辦理登記或許可
  - 經法務部會同中央目的事業主管機關指定之事業、團體或個人，應於指定之日起六個月內，辦理登記或許可。
  - 新法第56條第2項規定舊法第19-22條、第43條之刪除，自公布日生效。無店面零售業指定適用個資法一事，不因新法通過而改變，但業者僅須循遵舊法規定即可，已無須辦理登記並取得執照。

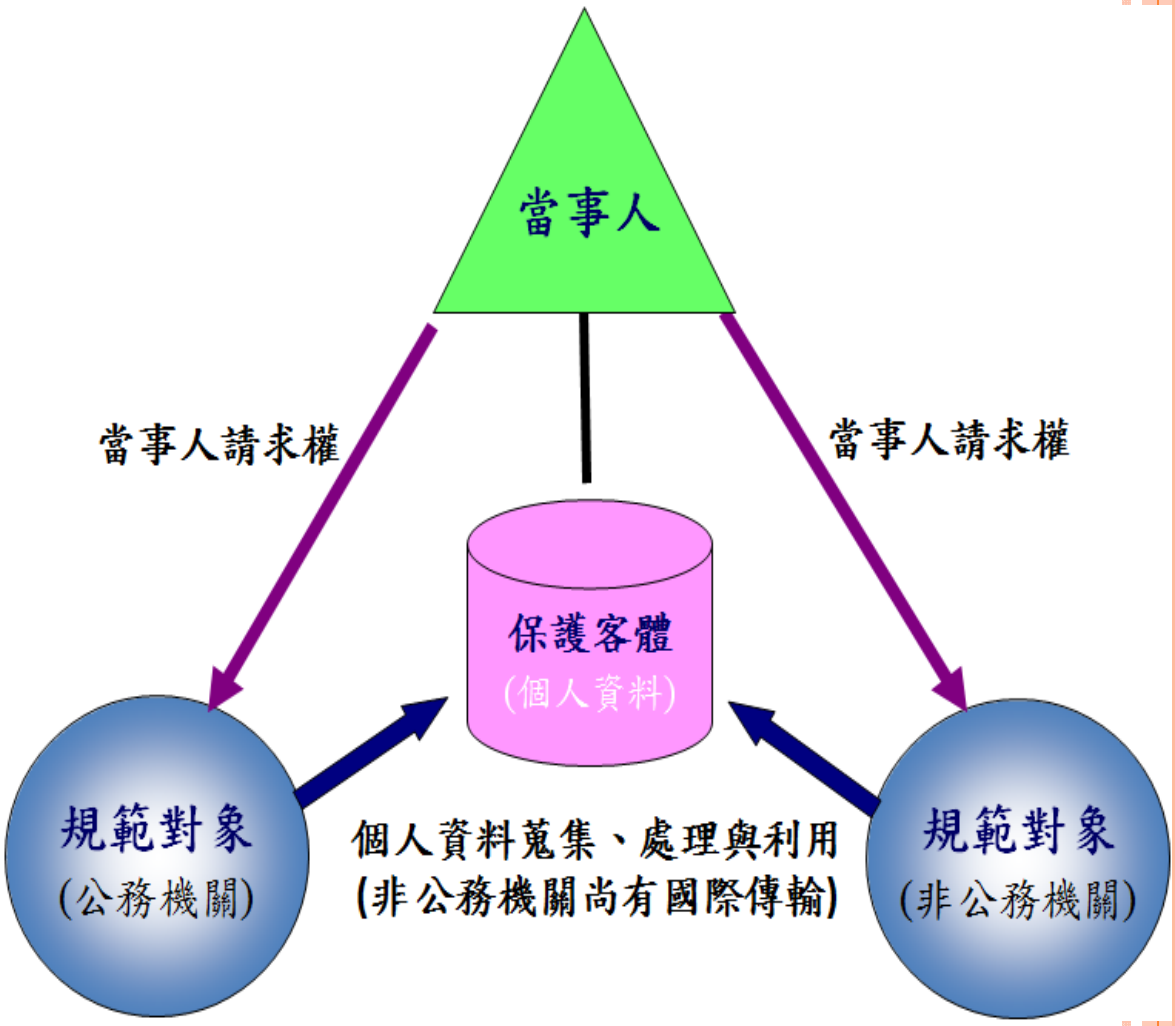
受規範之主體(5/5)

- 新法(個人資料保護法)

公務機關：指依法行使公權力之中央或地方機關或行政法人
非公務機關：指前款以外之自然人、法人或其他團體 (新法已取消行業別之限制)
受委託者：受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關

受規範之行為

- 受規範行為
  - 蒐集
  - (電腦)處理
  - 利用
  - 國際傳輸
  - (非公務機關)



新「個人資料保護法」下之操作(1/7)

- 新法調整部分用語，並增訂國際傳輸之定義。

蒐集：指為建立個人 料檔案而取得個人資料 **指以任何方式取得個人資料** 〔 直接向當事人蒐集 間接從第三人取得
處理：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、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
國際傳輸：指將個人資料作跨國（境）之處理或利用 〔 機關內部之資料傳送 (資料處理) 將資料提供當事人以外之第三人 (資料利用)

新「個人資料保護法」下之操作(2/7)

- 合法之個人資料蒐集/處理
  - 公務機關之蒐集/處理(§15)
    - 執行法定職務所必要範圍內。
    - 經當事人書面同意。
    - 對當事人權益無侵害。
  - 非公務機關之蒐集/處理(§19)
    - 須有特定目的並符合下列事項之一:
      - 法律明文。
      - 與當事人有契約或類似契約關係。
      - 當事人自行公開或其他已合法公開。
      - 學研機構基於公共利益為學術或統計必要，資料並經提供者處理後或蒐集者依其揭露方式無從識別當事人。
      - 經當事人書面同意。

新「個人資料保護法」下之操作(3/7)

- 適當之安全措施
  - 公務機關：專人辦理(§18)。
  - 非公務機關：適當安全措施(§27)。
- 特定範圍外之利用
  - 公務/非公務機關相同條件部分：
    - 法律明文。
    - 免除他人生命、身體、自由、財產之危險。
    - 防止他人權益之重大危害。
    - 公務/學研機構為學術或統計必要並經特殊處理。
    - 當事人書面同意。

新「個人資料保護法」下之操作(4/7)

- 個別特殊條件：
  - 公務機關：
    - 維護國家安全/增進公共利益。
    - 有利於當事人權益。
  - 非公務機關：
    - 特定目的外之行銷，當事人表示拒絕接受，應即停止利用其個資行銷
    - 須提供首次行銷當事人得拒絕接受之方式，並支付所需費用

新「個人資料保護法」下之操作(5/7)

- 當事人書面同意之要件(§7) －告知義務之實踐
  - 蒐集時之書面同意
    - 指當事人經蒐集者告知本法之應告知事項後所為之書面同意。
  - 特定範圍外利用之書面同意
    - 指當事人經蒐集者明確告知特定目的外知其他利用目的、範圍及同意與否對其權益之影響後，所為之書面同意。

✓蒐集機關名稱
✓蒐集目的
✓個人資料類別
✓個人資料利用之期間、地區、對象及方式
✓當事人基本權利行使方式
✓當事人得自由選擇提供個人資料時，不提供對其權益之影響
✓由第三人取得個人資料之來源資訊

✘特殊情況下得免告知

Q：上述兩個同意，可否設計於同一份文件？

Q：書面同意，可否以「電子方式」為之？

新「個人資料保護法」下之操作(6/7)

- 新法要求非公務機關應採行適當安全措施。

個人資料保護法	電腦處理個人資料保護法
第二十七條　非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 中央目的事業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。 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。	第二十六條　第十二條、第十三條、第十五條、第十六條第一項及第十七條之規定，於非公務機關準用之。 非公務機關準用第十六條第一項規定酌收費用之標準，由中央目的事業主管機關定之。

新「個人資料保護法」下之操作(7/7)

- 新法同時增訂通知義務。

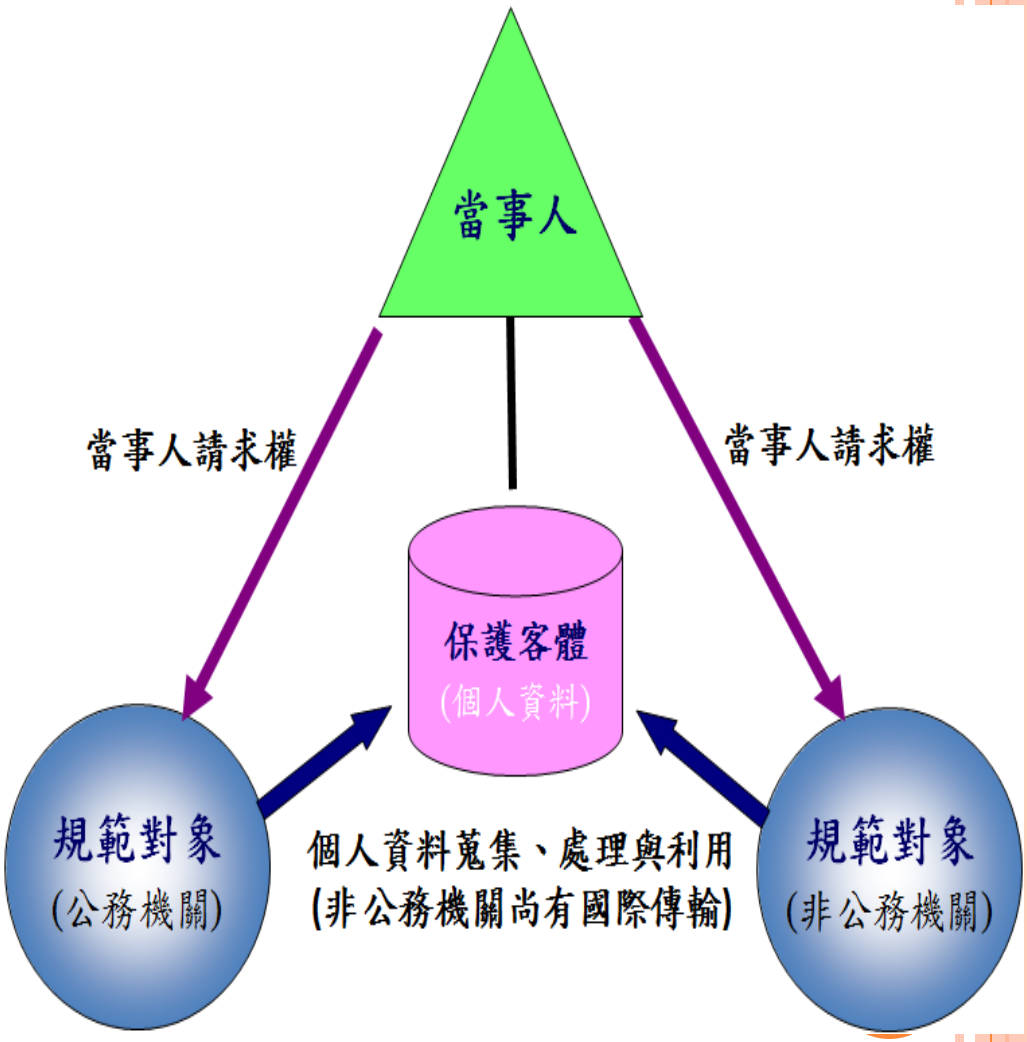
個人資料保護法	電腦處理個人資料保護法
第十二條 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。	

何謂適當方式，尚待法務部進一步補充說明

當事人之權利

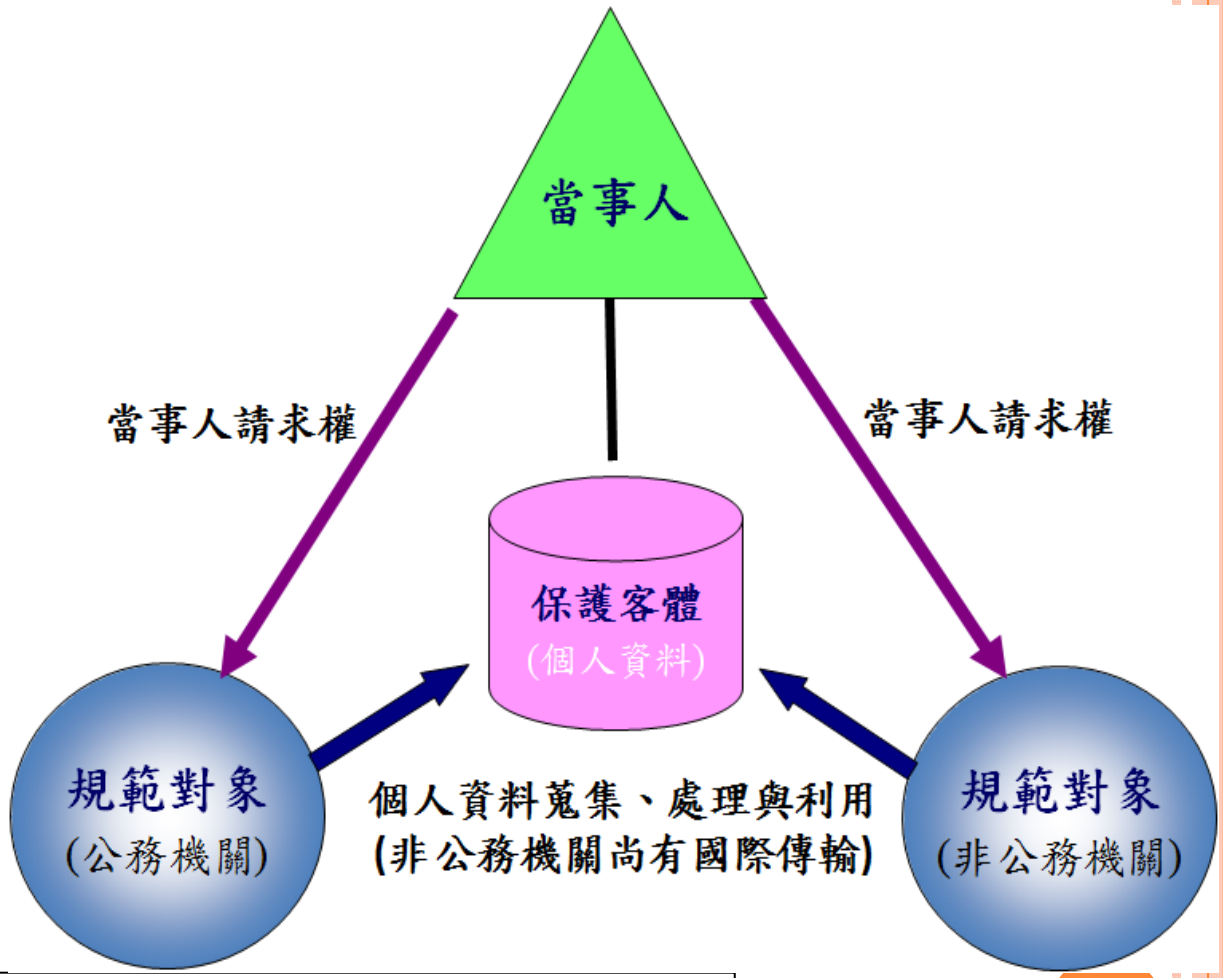
- 當事人之權利
  - 查詢、閱覽。
  - 製給複製本。
  - 補充或更正。
  - 停止處理或利用。
  - 刪除。

不得預先拋棄或以特約限制之



責任規範(1/3)

- 責任規範
  - 民事賠償。
  - 刑事責任。
  - 行政處罰。



民事賠償、刑事責任、行政處罰

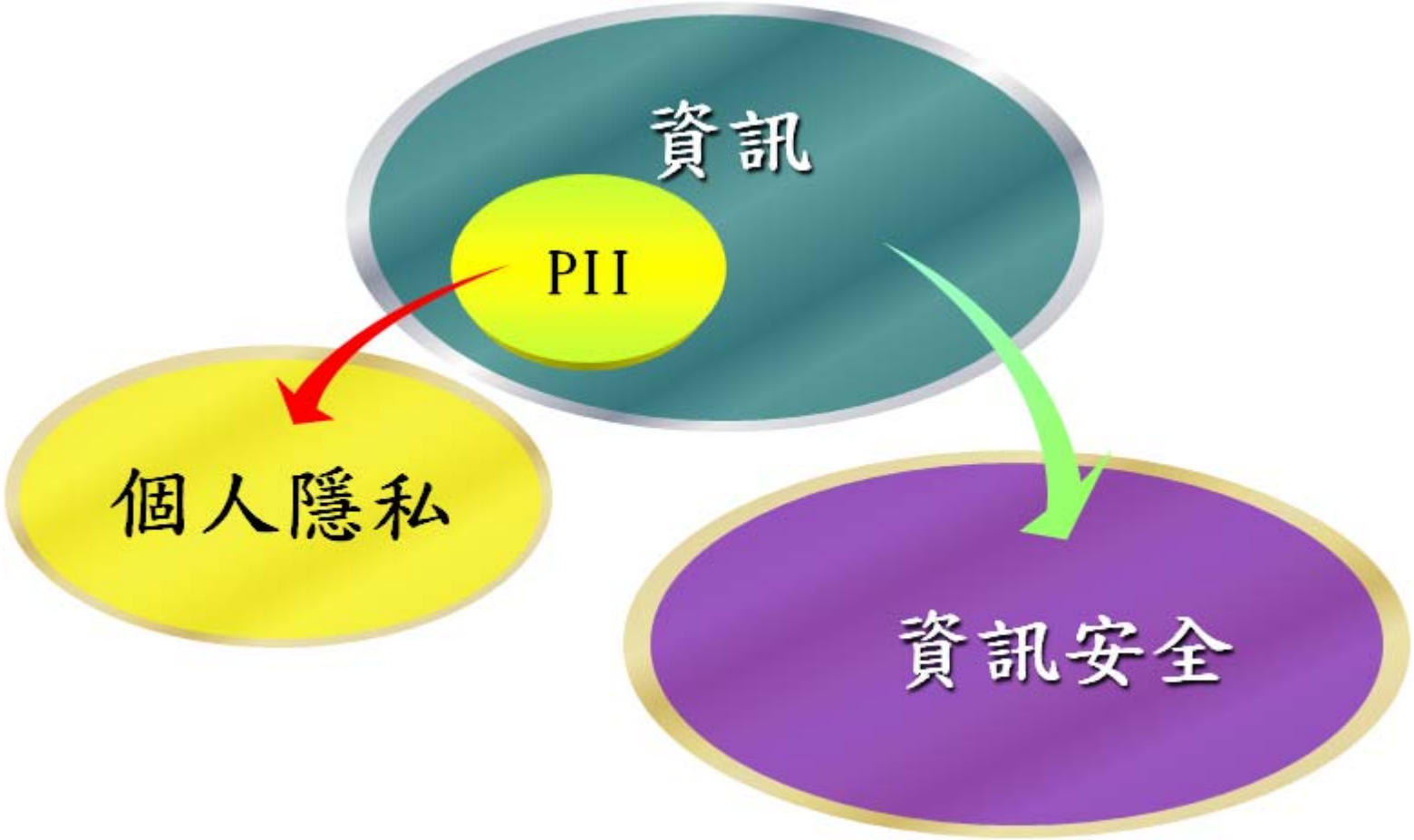
責任規範-民事賠償(2/3)

個人資料保護法	電腦處理個人資料保護法
第二十八條　公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。 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	第二十七條　公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。 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。 前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。 基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。 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。

責任規範-行政檢查(3/3)

個人資料保護法	電腦處理個人資料保護法
第二十二條　中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。 中央目的事業主管機關或直轄市、縣(市)政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。 對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。 參與檢查之人員，因檢查而知悉他人資料者，負保密義務	第二十五條　目的事業主管機關，認有必要時，得派員攜帶證明文件，對於應受其許可或登記之非公務機關，就本法規定之相關事項命其提供有關資料或為其他必要之配合措施，並得進入檢查。經發現有違反本法規定之資料，得扣押之。 對於前項之命令、檢查或扣押，非公務機關不得規避、妨礙或拒絕。

資訊安全與個人隱私之關係



*** (PII-個人可辨識資訊Personally identifiable information)**

個資法通過後之影響評估(1/2)

- 共通影響
  - 現行各組織體蒐集、處理、利用個資之機制需要配合調整
    - 個資特定目的規範強化、當事人書面同意與告知義務要求，將影響現行公務與非公務機關蒐集、處理、利用個人資料之流程與管理機制。
- 公務機關
  - 特種資料之蒐集處理利用規範需由各中央目的事業主管機關自行訂定。
  - 目的事業主管機關輔導責任與壓力提高
    - 非公務機關適用行業範圍擴大、行政檢查權及裁罰金額之提高、以及目的事業主管機關指定特定事業訂定個資安全維護計畫及服務終止個資處理方法等責任，將增加輔導之責任與壓力。

個資法通過後之影響評估(2/2)

- 無過失責任使得機關內部管理規則之建立與專人責任之強化成重點。
- 非公務機關
  - 未適用舊法之非公務機關，將需重新建立內部個人資料管理制度與流程，已符合法制要求並降低風險。
  - 適當安全措施之要求，將提高產業進行個資保護必要投入之成本。
  - 個資保護法律責任風險提高，如何有效舉證釐清關聯業者所負責任，有其重要性。

因應策略 (1/5)

- 新個資法下可採行之初步因應措施
- 首要步驟：盤點，確認組織可能擁有之個人資料
  - 個人資料取得來源。
  - 資料種類。
  - 特定目的。
  - 有無設定保存期限。
- 建立適當之資料安全機制
  - 將個人資料保護重點納入組織內部管理政策。
  - 指派專人或單位負責個人資料保護事。
  - 建立個人資料保護計畫（從資料蒐集開始到資料銷毀為止）。

因應策略 (2/5)

- 對於個人資料傳輸、儲存、處理等流程，建立適當之資訊安全機制，防止個人資料遭受竊取、竄改、毀損、滅失或洩漏。
- 接觸、處理與應用個人資料之內部規則、管理相關流程與應變流程，須予以建立。

- 強化人員認知並建立訓練機制
  - 正職人員、派遣人員。
  - 其他-廠商 /合約。
- 建立當事人同意流程
  - 當事人書面同意機制之設置
    - 紙本書面/電子文件。
    - 員工契約內容/蒐集個資文件之同意條款。

因應策略 (3/5)

- 蒐集之特定目的說明機制/文件之建立。
- 特定目的範圍外利用，書面同意之取得機制。

- 建立當事人權利主張機制
  - 建立個人資料當事人得以主張權利之機制與流程
    - 查詢或請求閱覽。
    - 請求製給複製本。
    - 請求補充或更正。
    - 請求停止搜集、處理或利用。
    - 請求刪除。
  - 妥善處理來自當事人（個人資料之本人）之客訴及抱怨。

因應策略 (4/5)

- 確認是否有必須對當事人補充告知義務之情事
  - 若有，則若要繼續利用各該個人資料，須於一年內補行告知。
- 一般企業更應關注主管機關公告項目，配合進行個人資料保護管理
  - 目的事業主管機關可能指定特定非公務機關訂定個人資料檔案安全維護計畫，須關注公告項目。
  - 定期檢查個人資料管理作業程序是否符合法令要求。
- 訂定隱私保護政策及相關內部規範。
- 設置專人及開發個人資料管理制度。

因應策略 (5/5)

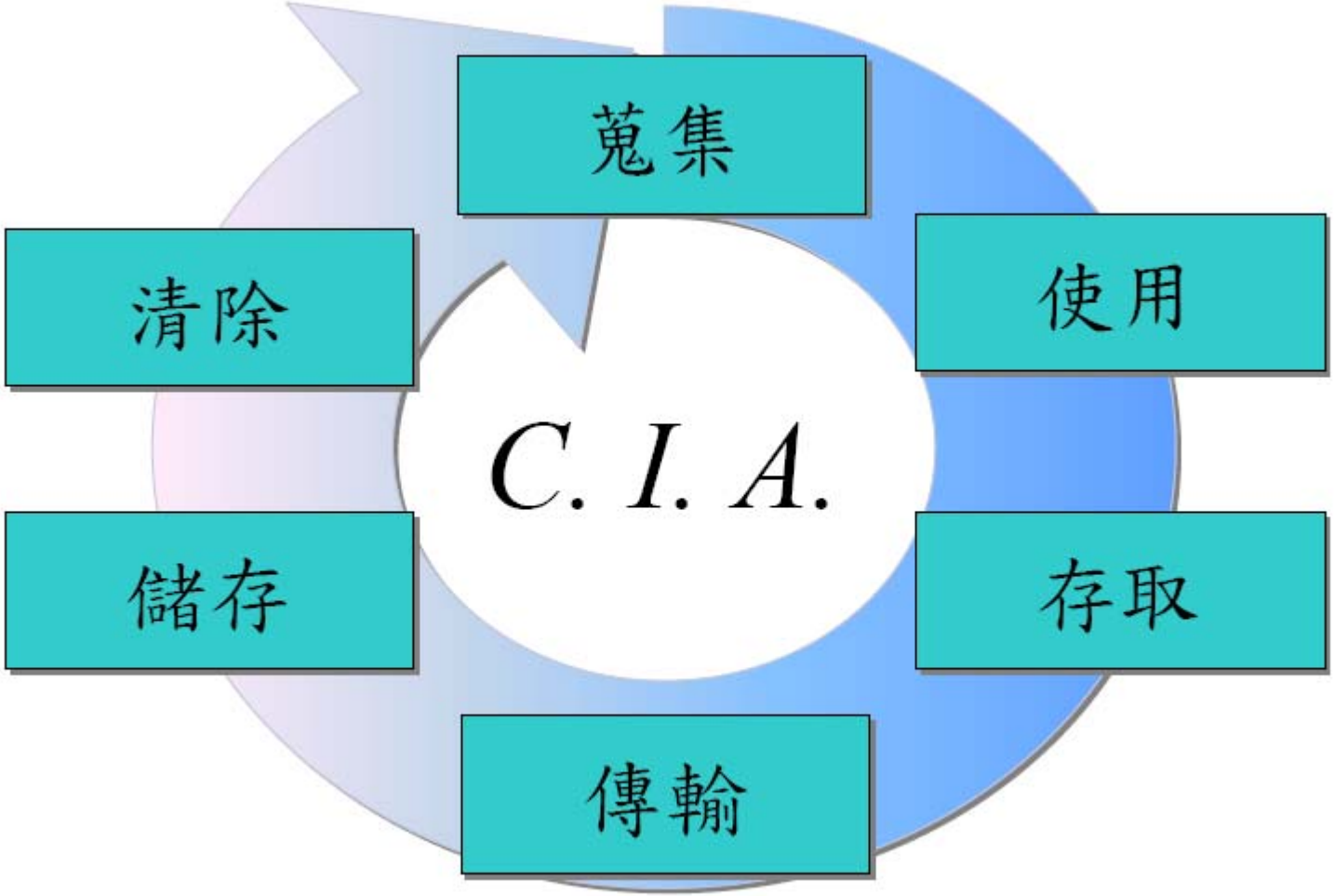
- 隨時評估隱私風險及訂定避免損害擴大之程序。
- 建置層級化之個資安全管理措施。
- 最小限度蒐集與利用及損賠預估與保險。
- 定期員工教育訓練及強化客服資訊諮詢功能。
- 加強與目的事業主管機關之協調聯繫。
- 注意國際隱私發展及隱私權標章驗證機制。

營運資料

- 各行業都的營運資料：
  - 製程流程與參數、財務資料、員工個人資料、客戶個人資料…

行業別	營運秘密	個人資料
科技及製造業	製程流程與參數、設計資訊、未公開產品規格、軟體原始碼、營運及業務、財務、人事資訊	雇員個人資訊
金融行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	雇員個人資訊、客戶個人資訊、信用卡或帳戶資訊
醫療行業	實驗數據、業務、財務、人事資訊	雇員個人資訊、病患個人資訊、病歷資訊、健康檢查資訊
教育行業	研究報告、業務、財務、人事資訊	教職員資訊、學生及家長個人資訊、學生學習紀錄
政府及軍事	軍事機密資訊、內部調查資料、未公開規劃、稅務資訊、情報資訊	國民、市民資訊、個人稅務及財務資訊、
零售行業	交易資訊、未公開營運資訊、業務、財務、人事資訊	會員資訊、信用卡或帳戶資訊

個人資料生命週期管理



個人資料管理重點(1/2)

- 蒐集
  - 符合法律之蒐集個人資料之理由、方法與告知義務。
  - 確認個人資料之正確性及內容是否符合法律之定義「得以直接或間接方式識別該個人之資料」。
- 利用
  - 符合法律及申報之使用規範。
  - 符合組織政策之內部使用規範(含交叉行銷)。
- 存取處理
  - 存取個人資料之權限管理(含第三方人員)。
  - 維護、委外或外包廠商之資訊安全管理。

個人資料管理重點(2/2)

- 傳遞
  - 個人資料傳輸過程中之安全設計（加密或安全網路）。
- 儲存
  - 個人資料新增及修改之安全作業程序及管理。
  - 存放個人資料之場所及設備之安全管理。
  - 備份或歸檔後之資料安全。
- 清除
  - 個人資料刪除或報廢之安全處理程序。
- 其它
  - 客訴、法律、懲處程序。