

Name	楊家豪 (Jerry Yang)
Position	安侯企業管理股份有限公司 高級顧問師
Certificate	■ ISO 27001 Lead Auditor Certificate ■ ISO 20000 Lead Auditor Certificate ■ BS 25999 Certificate ■ ITIL Foundation Certificate ■ EC-Council Certified Security Specialist ■ EC-Council Certified Ethical Hacker Certificate (V5.0)
Experience	■ ISMS 專案建置輔導暨驗證 — 行政院衛生署中南區醫療聯盟 (共 6 間醫院) — 立法院維護輔導暨驗證 (專案經理) — 財團法人電信技術中心 — 北區區域網路中心 (共 14 個單位) — 北區縣市網路中心 (共 23 個單位) — 台北市立聯合醫院建置輔導暨驗證 (共 9 間分院) — 財政部臺灣省北區國稅局建置輔導暨驗證 — 財政部高雄市國稅局建置輔導暨驗證 — 財政部臺灣省中區國稅局建置輔導暨驗證 — 行政院勞工委員會職業訓練局建置輔導暨驗證 — 富邦媒體科技股份有限公司建置輔導暨驗證 — 統一速達股份有限公司建置輔導暨驗證 ■ ITSM 專案建置輔導暨驗證 — 行政院國家資通安全會報技術服務中心建置輔導暨驗證 ■ 技術風險評鑑(電腦與網路弱點掃描暨滲透測試) — 行政院衛生署中南區醫療聯盟電腦與網路弱點掃描 (共 6 間醫院) — 財政部高雄市國稅局電腦與網路弱點掃描 — 立法院電腦與網路弱點掃描 — 行政院衛生署國民健康局電腦與網路弱點掃描 — 中央健保局電腦與網路弱點掃描 — 清雲科技大學電腦與網路弱點掃描 — 雲林科技大學電腦與網路弱點掃描 — 台北市立聯合醫院無線網路弱點掃描暨滲透測試 (共 9 間分院) — 財政部臺灣省北區國稅局電腦與網路弱點掃描 ■ 稽核審查 — 行政院研究發展考核委員會憑證註冊授權作業(Registration Authority Operator)稽核 — 行政院研究發展考核委員會憑證(MOICA/MOEACA)稽核 — 蘇格蘭皇家銀行資訊安全管理第三方稽核 — 超過 30 個單位資訊安全主導稽核經驗



PERFORMANCE AND TECHNOLOGY

台北海洋技術學院 悠遊個人資料保護法研習

楊家豪, 高級顧問師
安侯企業管理股份有限公司
2011/02/16

ADVISORY

課程大綱

- 個資法重點說明
- 個人資料保護法之因應之道
- Q&A

個資外洩嚴重

- 資料外洩以及個人隱私被侵犯情況嚴重

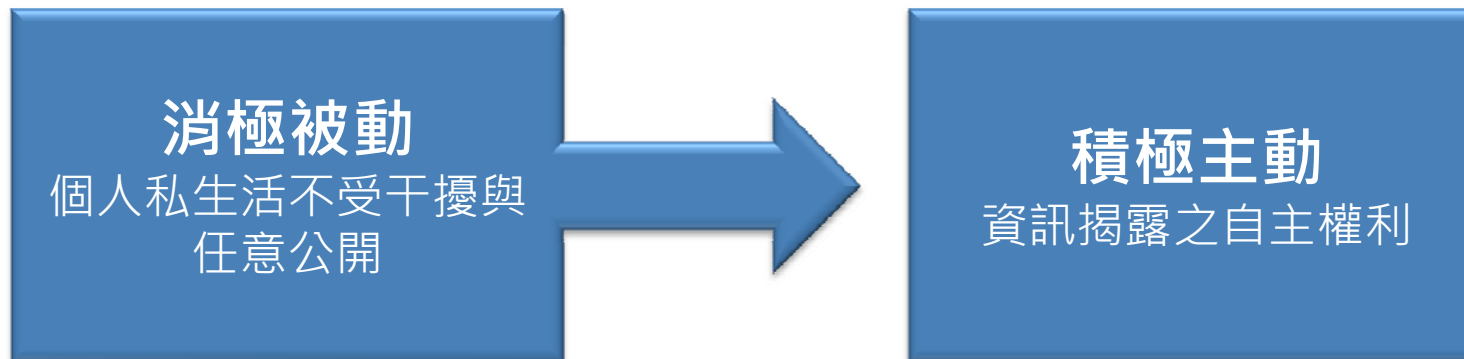
- ◆ 刑事警察局犯罪預防科根據2009年的統計資料指出，165反詐騙諮詢專線接獲詐騙投訴電話，排名第一的是個資外洩詐騙事件，占總數的35%，未收到網購產品的詐騙事件則名列第二
- ◆ 詐騙問題在十大民怨調查當中高居第二

突顯個人資料外洩嚴重影響到民眾與消費者之財產
安全與生活品質

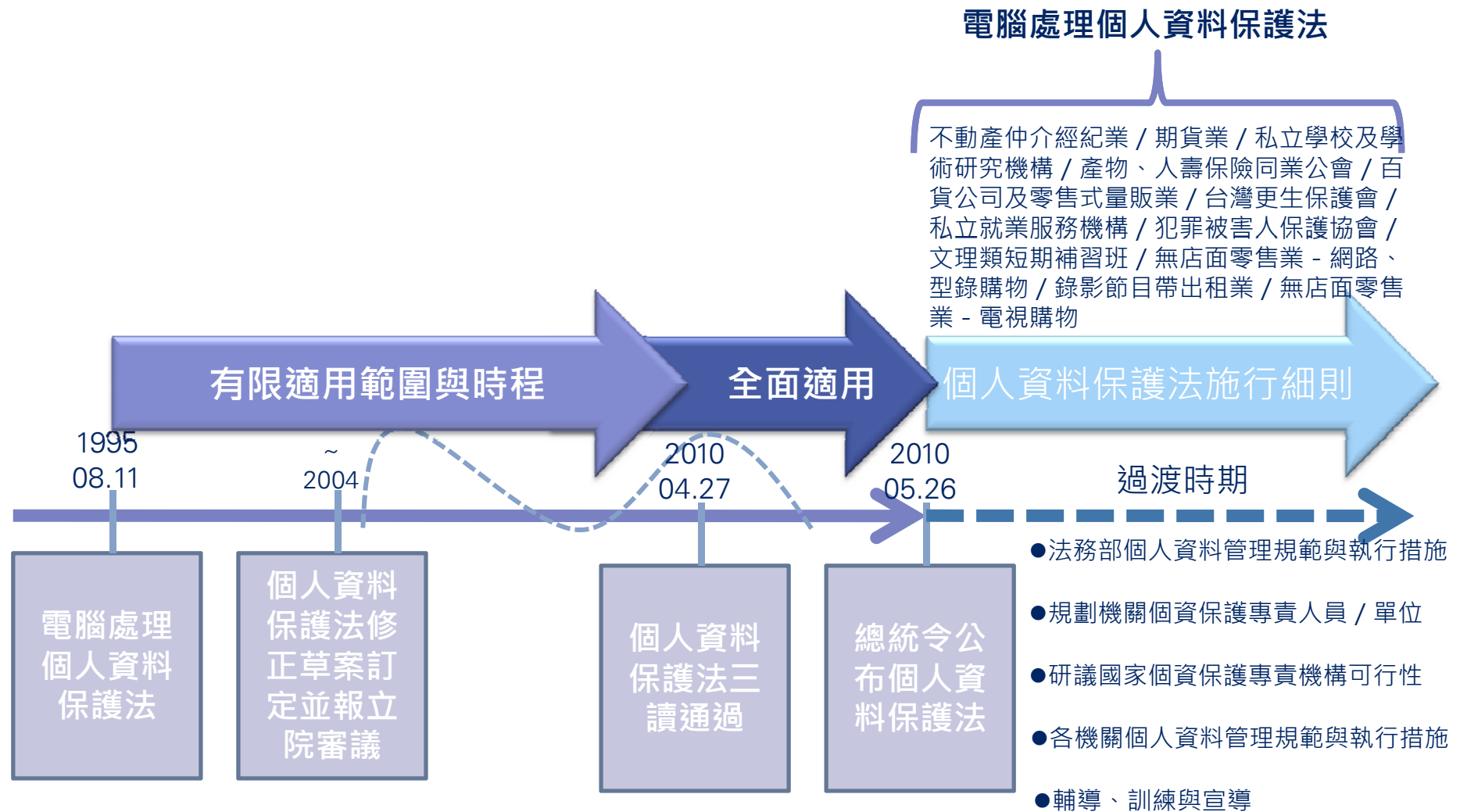
資訊隱私權的概念

● 資訊隱私權

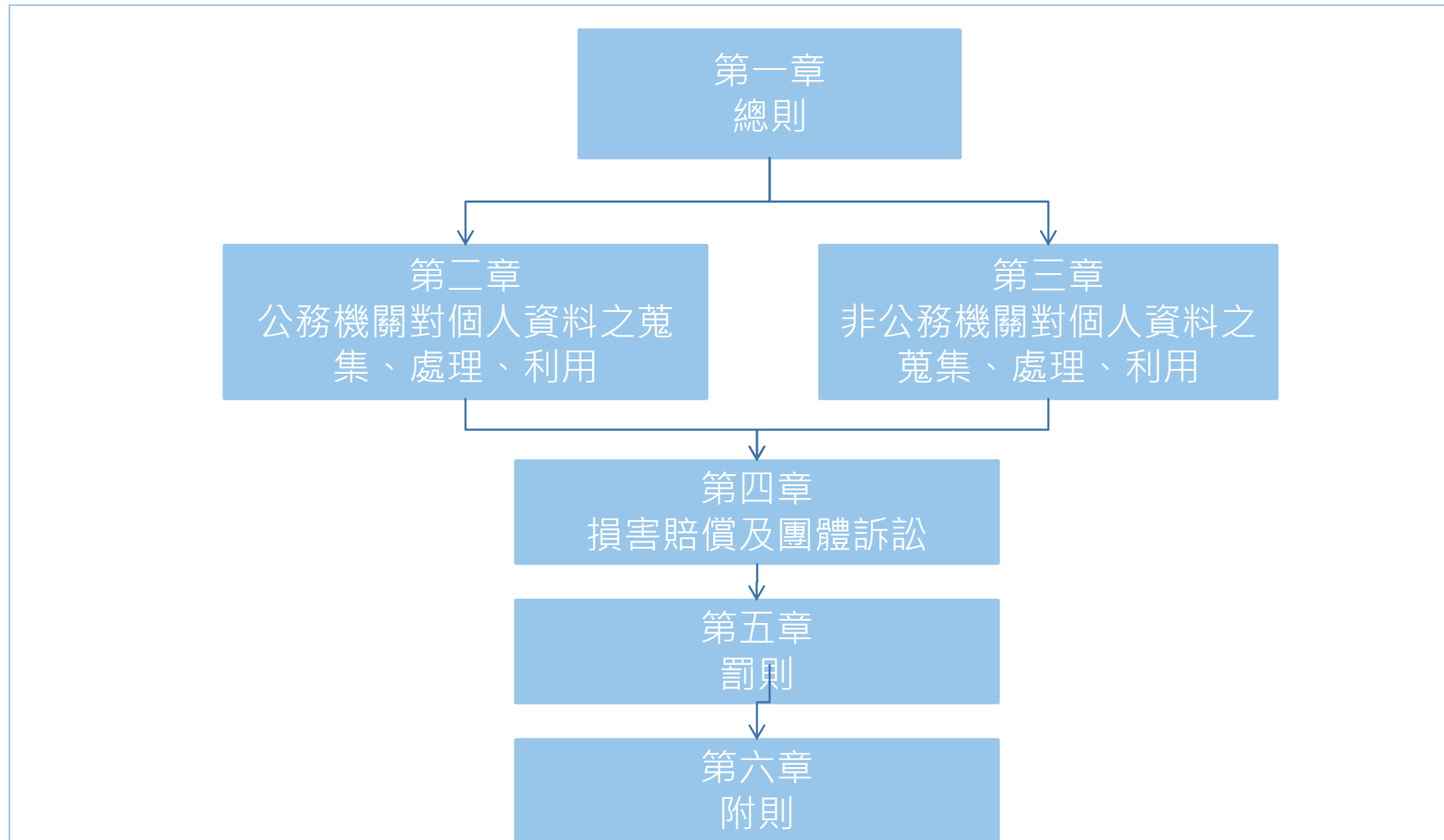
- ◆個人自主控制個人資料之權利 (資訊自決權)
- ◆個人有決定是否接露個人資料、及在何種範圍內、於何時、以何種方式、向何人接露之決定權
- ◆個人對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。
(釋字第603號)



個人資料保護法修正歷程



個人資料保護法整體架構



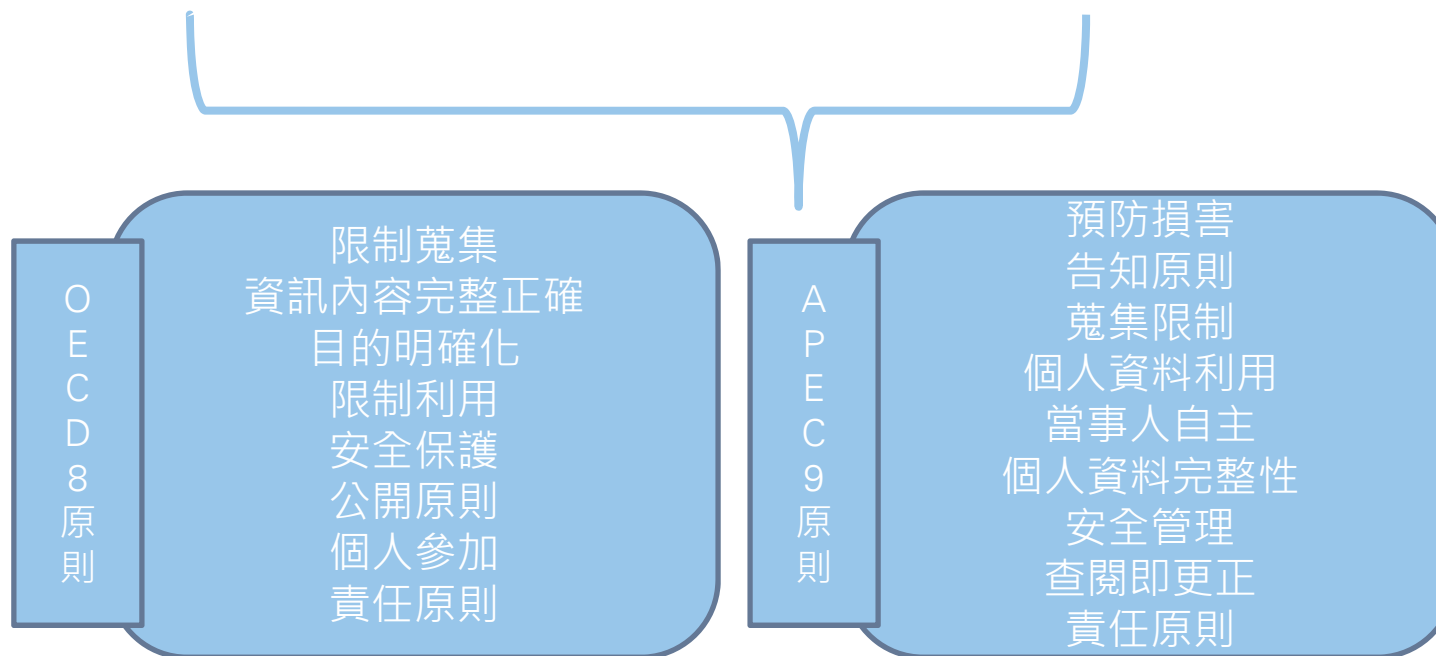
立法目的與原則

● 立法目的(§1)

- ◆為規範個人資料之蒐集、處理及利用，以**避免人格權受侵害**，並促進個人資料之合理利用

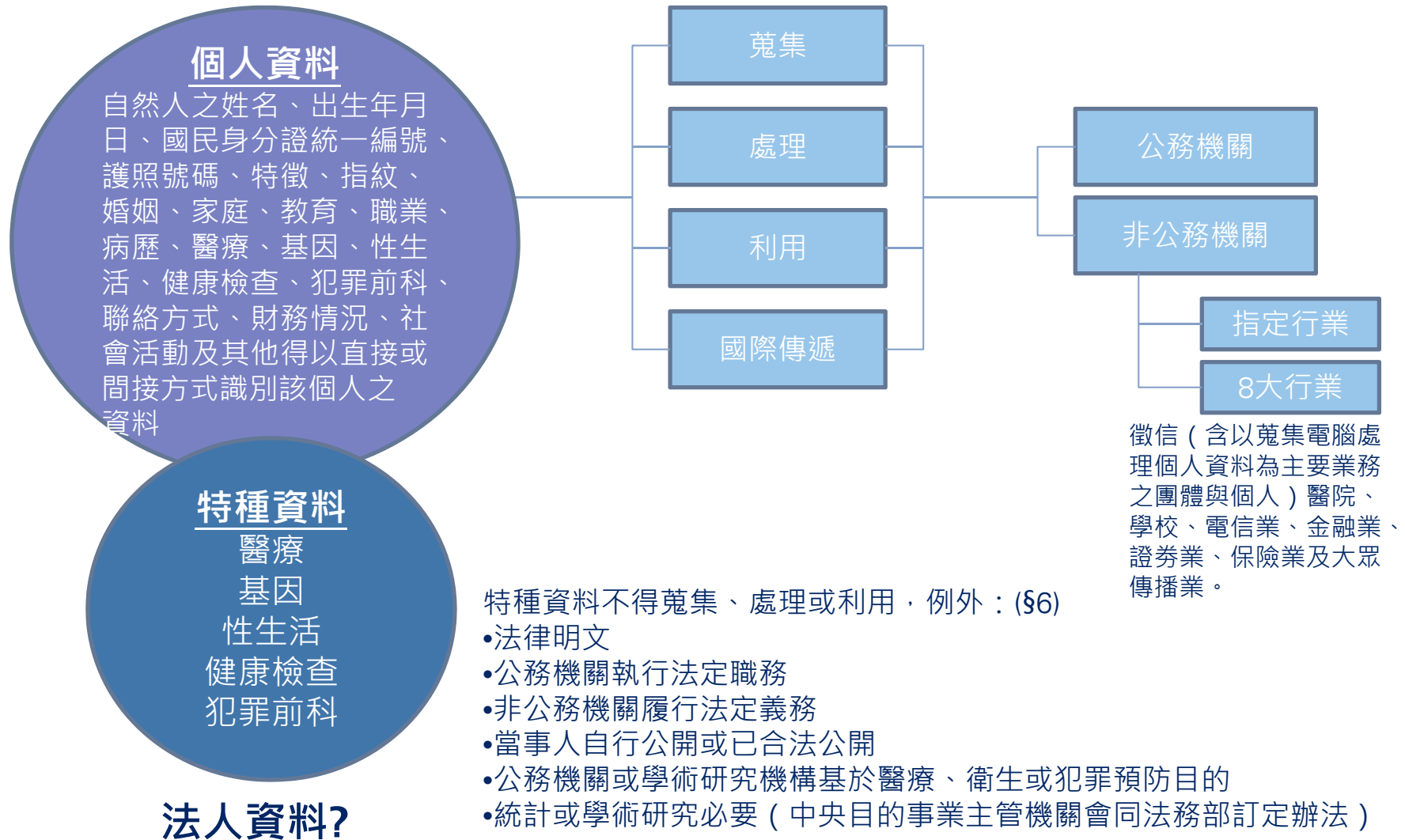
● 立法原則：

- ◆新法：歐盟隱私保護指令及APEC隱私保護綱領9原則

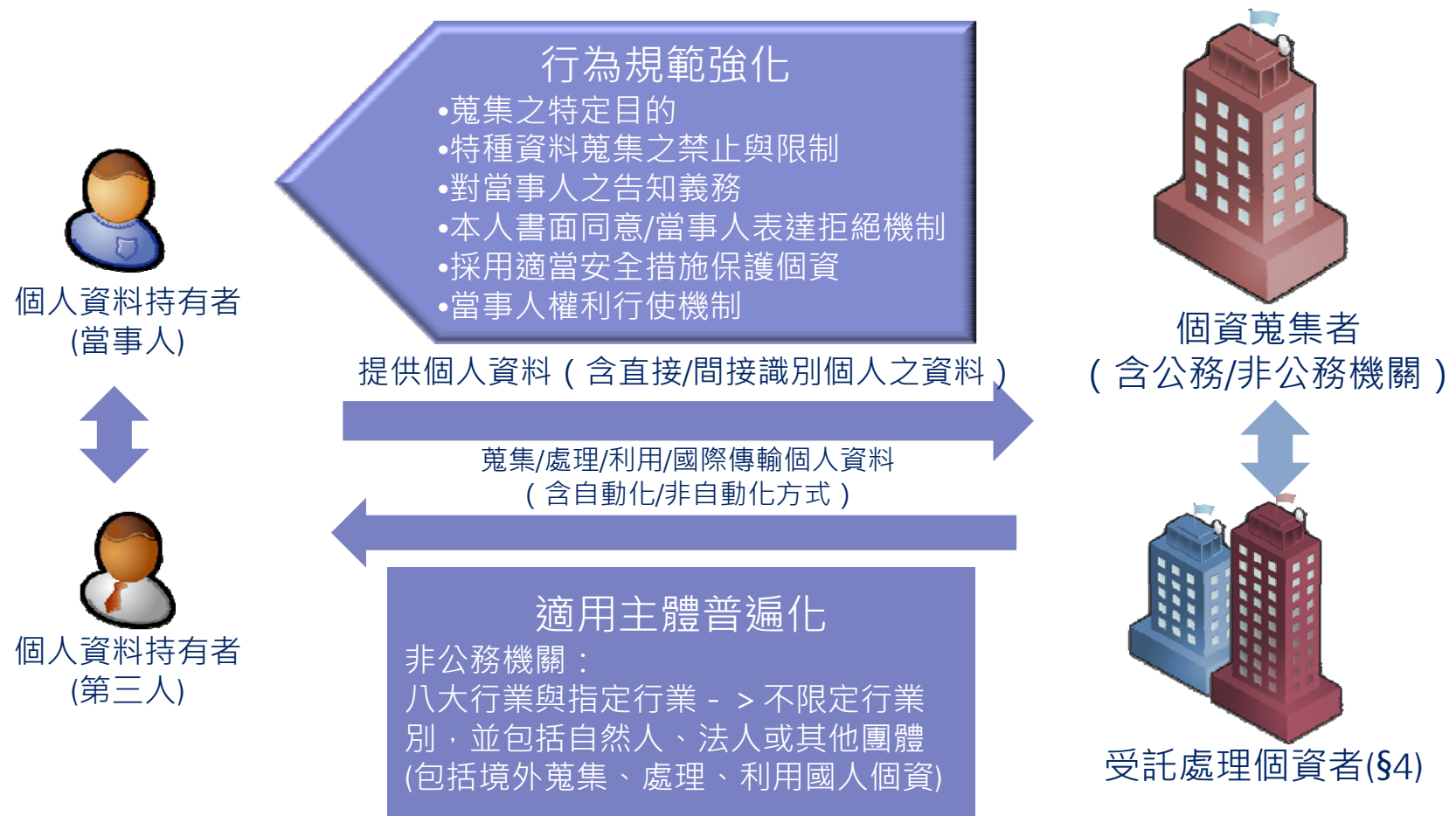


納入國際規範重點，促使法制接軌，減少產業跨境個資傳輸障礙

個資保護的現在



規範主體定義



自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料者？

規範行為定義

- 蒐集

- ◆ 為建立個人資料檔案而取得個人資料
- ◆ 取得方式不限，任何方式取得皆為蒐集
- ◆ 包括「直接蒐集」與「間接蒐集」

- 處理

- ◆ 為建立或利用個人資料檔案所為之紀錄、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

- ◆ 將蒐集之個人資料為「處理」外之使用

- 組織內部資料傳送 - 處理
- 將個資提供第三人 - 利用

- 國際傳輸

- ◆ 將個人資料作跨國(境)之處理或利用

當事人權利

- 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之： (§3)
 - ◆查詢或請求閱覽
 - ◆請求製給複製本
 - ◆請求補充或更正
 - ◆請求停止蒐集、處理或利用
 - ◆請求刪除
- 下列情形之一者，不在此限： (§10)
 - ◆妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益
 - ◆妨害公務機關執行法定職務
 - ◆妨害該蒐集機關或第三人之重大利益

當事人權利 (cont'd)

- 申請查詢、提供閱覽或製給複製本(§13)

- ◆應於受理後15日內為准駁之決定
- ◆必要時得延長，延長期限不得逾15日
- ◆延長原因應以書面通知當事人

- 申請刪除、停止處理或利用(§13)

- ◆應於受理30日內為准駁之決定
- ◆必要時得延長，延長期限不得逾30日
- ◆延長原因應以書面通知當事人
- ◆申請查詢、閱覽、複製本

公務機關或非公務機關得酌收必要成本費用(§14)



個人資料蒐集者告知之義務

- 公務機關或非公務機關向當事人蒐集個人資料時，應明確告知當事人下列事項：(§8 I)
 - ◆公務機關或非公務機關名稱
 - ◆蒐集之目的
 - ◆個人資料之類別
 - ◆個人資料利用之期間、地區、對象及方式
 - ◆當事人依第三條規定得行使之權利及方式
 - ◆當事人得自由選擇提供個人資料時，不提供將對其權益之影響

個人資料蒐集者蒐集與處理之義務

- 公務機關對個人資料之蒐集或處理，應有特定目的，並符合下列情形之一者： (§15)
 - ◆ 執行法定職務必要範圍內
 - ◆ 經當事人書面同意
 - ◆ 對當事人權益無侵害
- 非公務機關對個人資料之蒐集或處理，應有特定目的，並符合下列情形之一者： (§19)
 - ◆ 法律明文規定
 - ◆ 與當事人有契約或類似契約之關係
 - ◆ 當事人自行公開或其他已合法公開之個人資料
 - ◆ 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人
 - ◆ 經當事人書面同意

個人資料蒐集者利用之義務

- 公務機關特定目的外之利用： (§16)

- ◆ 法律明文規定
- ◆ 為免除當事人之生命、身體、自由或財產上之危險
- ◆ 為防止他人權益之重大危害
- ◆ 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人
- ◆ 經當事人書面同意
- ◆ 為維護國家安全或增進公共利益
- ◆ 有利於當事人權益

- 非公務機關特定目的外之利用： (§20)

- ◆ 同公務機關前五項

非公務機關依前項規定利用個人資料行銷者，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。非公務機關應於首次行銷時，免費提供當事人表示拒絕之方式 (§20 五)

個人資料蒐集者保護之義務

● 公務機關

◆公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同： (§17)

- ✓個人資料檔案名稱
- ✓保有機關名稱及聯絡方式
- ✓個人資料檔案保有之依據及特定目的
- ✓個人資料之類別

◆公務個人資料檔案者，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。 (§18)

● 非公務機關

◆個人資料保護計畫： (§27)

- ✓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

個資蒐集者告知義務之免除

- 蒐集由當事人提供的資料(§8II)

- ◆ 依法律規定免告知
- ◆ 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
- ◆ 告知將妨害公務執行
- ◆ 告知將妨害第三人重大利益
- ◆ 當事人明知告知內容

- 蒐集非由當事人提供的資料(§9II)

- ◆ 前述(§8II)情形
- ◆ 當事人自行公開或是已合法公開的資料
- ◆ 不能向當事人或其法定代理人為告知
- ◆ 基於公共利益或學術研究目的，但須無從識別當事人
- ◆ 大眾傳播業基於新聞報導之公益目的而蒐集

國際傳輸

- 非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之： (§21)
 - ◆ 涉及國家重大利益
 - ◆ 國際條約或協定有特別規定
 - ◆ 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞
 - ◆ 以迂迴方法向第三國（地區）傳輸個人資料規避本法

行政檢查權

- 中央目的事業主管機關或直轄市、縣(市)政府對非公務機關執行行政檢查權：**(§22)**
 - ◆得率同資訊、電信或法律等專業人員共同為之
 - ◆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
- 非公務機關之異議權**(§24)**
 - ◆對於檢查時所為之沒入、扣留、複製等等處分，得聲明異議
- 補償措施：**(§26)**
 - ◆中央目的事業主管機關或直轄市、縣(市)政府檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果

處罰

- 非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣(市)政府除依本法規定裁處罰鍰外，並得為下列處分：(§25)
 - ◆禁止蒐集、處理或利用個人資料
 - ◆命令刪除經處理之個人資料檔案
 - ◆沒入或命銷燬違法蒐集之個人資料
 - ◆公布非公務機關之違法情形，及其姓名或名稱與負責人

損害賠償

- 違反本法規定(§28) (§29)

- ◆公務機關與非公務機關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侵害當事人權利者，負損害賠償責任

- 損害賠償總額

- ◆以每人每一事件新臺幣伍佰元以上二萬元以下計算
- ◆最高總額以新臺幣二億元為限

- 不在此限之情節

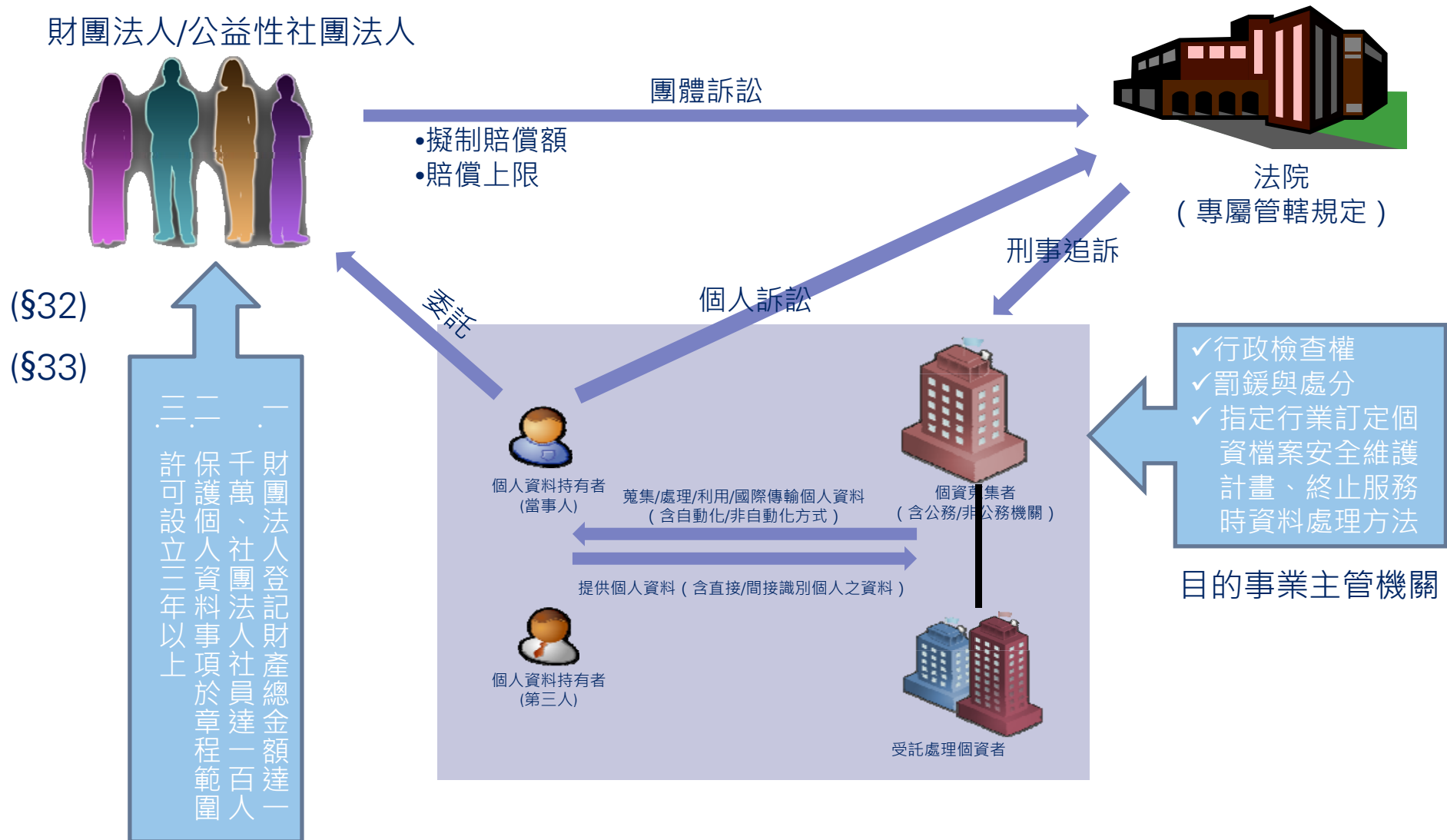
- ◆公務機關損害因天災、事變或其他不可抗力所致者
- ◆非公務機關能證明其無故意或過失者

舉證責任轉換!

- 損害賠償請求權(§30)

- ◆自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同

監督 / 救濟 / 處罰



罰則

● 刑事責任

- ◆違反第六條、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者：
 - ◆基本刑罰：(§40)
 - ✓2年以下有期徒刑、拘役或科或併科新臺幣20萬元以下罰金
 - ◆加重處罰：(§41)
 - ✓意圖營利(五年以下有期徒刑、得併科100萬元以下罰金)
 - ✓意圖為自己或為第三人不法之利益或損害他人利益(同上)
 - ✓公務員假藉職務上之權力、機會或方法犯罪，加重其刑至1/2 (§44)

重要時程

- **施行細則： (§54)**

- ◆由法務部定之

- **公布施行日： (§55)**

- ◆由行政院定之

- **公布前非經當事人提供之個人資料： (§53)**

- ◆須於修正施行之日起一年內補行告知義務

- ◆逾期未告知而處理、利用者，以違反第9條規定論處 -

- ✓ 依據第48條規定，限期改正，若未改正，則按次處新臺幣2萬元以上，20萬元以下罰鍰。

個人資料保護法修正重點

適用範圍	個人資料保護法
擴大保護客體	為落實對個人資料之保護，將保護客體予以擴大，將非經電腦處理之個人資料(即人工資料)一併納入保護
普遍適用主體	•刪除非公務機關行業別之限制，使任何自然人、法人或其他團體，除為單純個人或家庭活動之目的而蒐集、處理或利用個人資料外，皆須適用本法 •公務機關及非公務機關，在中華民國領域外對中華民國人民蒐集、處理或利用個人資料者，亦適用本法
增修行為規範	增訂醫療、基因、性生活、健康檢查及犯罪前科等五類資料為特種資料，除符合法定要件外，原則上不得蒐集、處理或利用書面同意內涵明確化，特定目的外利用個人資料需當事人書面同意者，應另以單獨書面同意方式為之不論是直接或間接蒐集資料，除符合得免告知情形者外，均須明確告知當事人蒐集機關名稱、蒐集目的、資料類別、利用方式、資料來源等相關事項違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除或停止蒐集、處理或利用其個人資料從事商品行銷之非公務機關，應於首次行銷時免費提供當事人表示拒絕之方式
促進民眾參與	為結合民間力量，發揮本法保護個人資料之功能，財團法人或公益社團法人符合本法規定者，得提起團體訴訟，以協助隱私權益遭侵害之當事人進行民事或行政救濟

個人資料保護法修正重點 (cont'd)

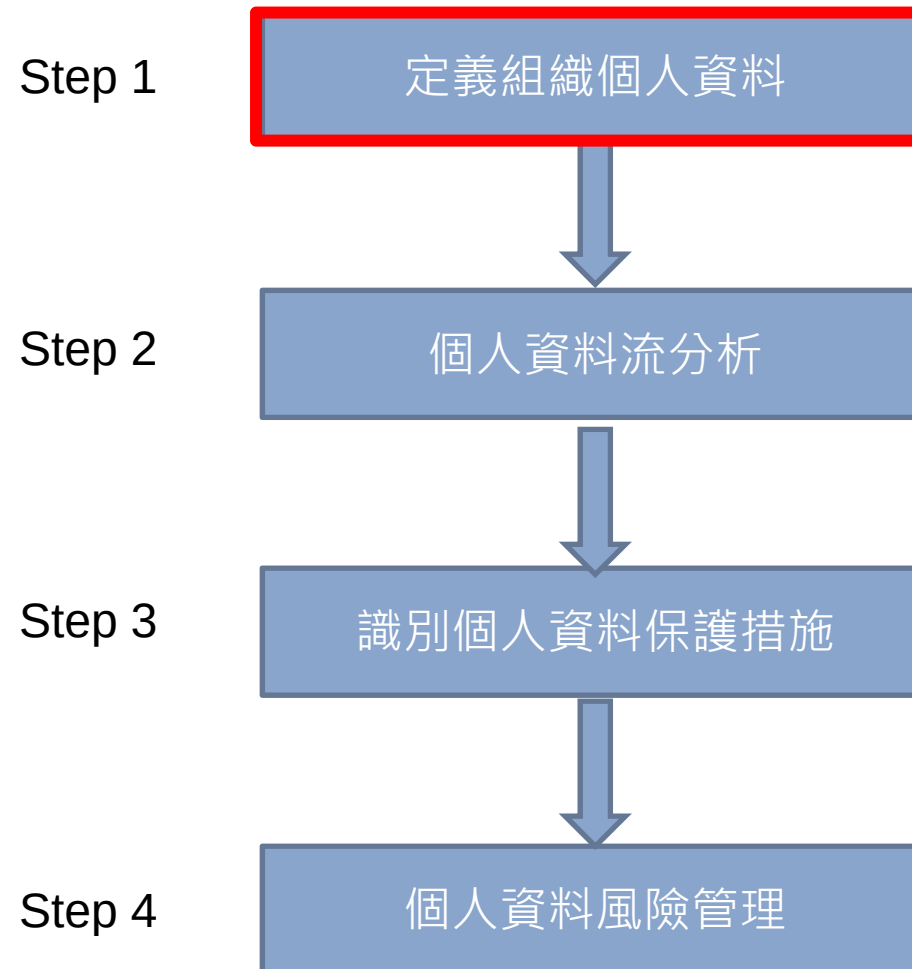
適用範圍	個人資料保護法
強化行政監督	為加強防制個人資料之濫用，中央目的事業主管機關或直轄市、縣（市）政府，發現非公務機關違反本法規定或認有必要時，得派員攜帶執行職務證明文件，進入檢查，如發現有違法情事，並得採取必要處分
調整責任內涵	•民事責任：提高基於同一原因事實應對當事人負損害賠償責任之總額2億(被害人不易或不能證明其實際損害額時，得請求法院依侵害情節以新臺幣5 百元以上2 萬元以下計算) •刑事責任：非「意圖營利」者得科處2年以下有期徒刑(告訴乃論)；「意圖營利」者得科處5年以下有期徒刑(非告訴乃論) •行政責任：非公務機關之代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，並應課以同一額度之罰鍰，以加強其監督之責任
隱私保護與新聞自由之平衡	本法乃個人資料保護之基本法律，惟新聞自由的尊重，乃現代民主國家的重要表徵，為期兼顧「個人隱私」與「新聞自由」之平衡，對於大眾傳播業者基於新聞報導之公益目的而蒐集個人資料，自得免為告知當事人；另外，與公共利益有關或個人資料取自於一般可得之來源者，非公務機關對個人資料亦得為蒐集或處理

課程大綱

- 個資法重點說明
- 個人資料保護法之因應之道
- Q&A

實作面策略_個人資料保護程序

- 個資抓漏



個人資料盤點

● 組織個人資料作業流程表

◆X軸：解構組織各部門個人資料流程

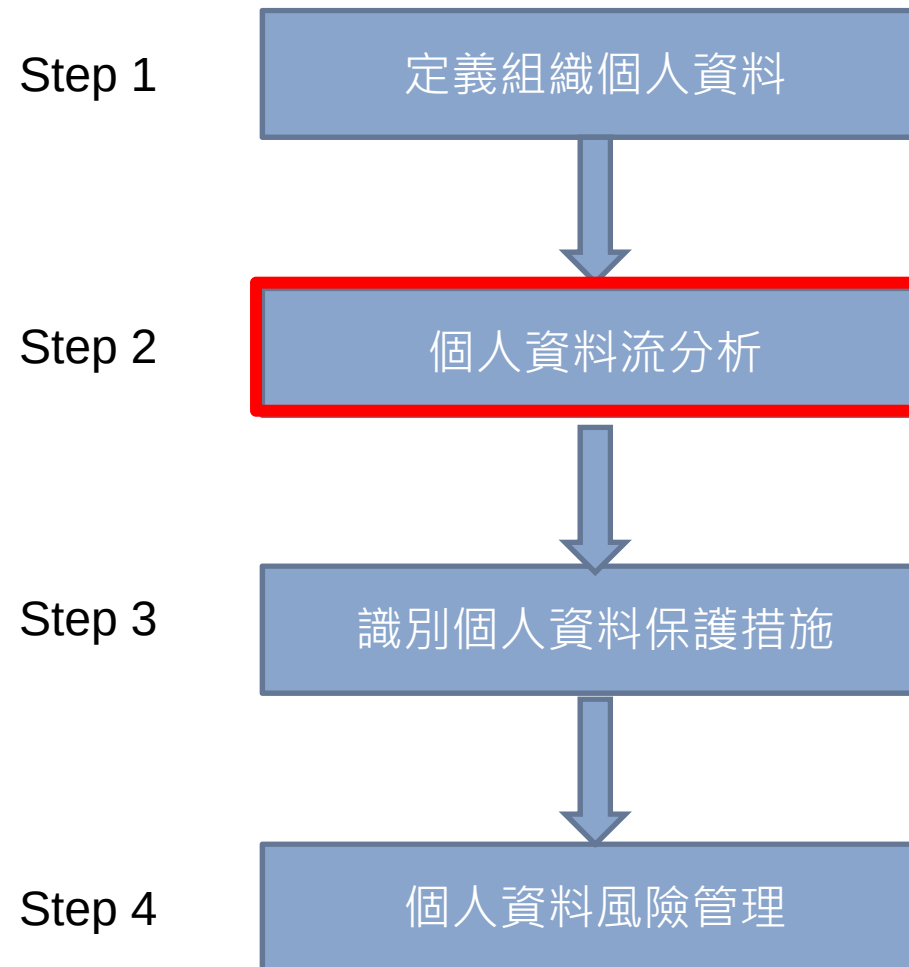
◆Y軸：解構組織擁有的個人資料種類

部門類別 個資種類	教務處	學務處	註冊組	總務處	衛保組	圖資中心	業務部	人資部	資訊部	會計室	...
學生基本資料	C、P、U	C、P、U	C、P、U		P、U	P、T					
教師基本資料	C、P、U	C、P、U		C、P、U		P、T		C、U			
職員基本資料	C、P、U	C、P、U		C、P、U		P、T					
學生學籍資料	C、P、U	C、P、U	C、P、U			P、T					
註冊資料			C、P、U	P、U		P、T					
薪資資料				P、U		P、T					
...											

- 蒐集(Collection, C)
- 處理(Process, P)
- 使用(Use, U)
- 傳輸(Transfer, T)

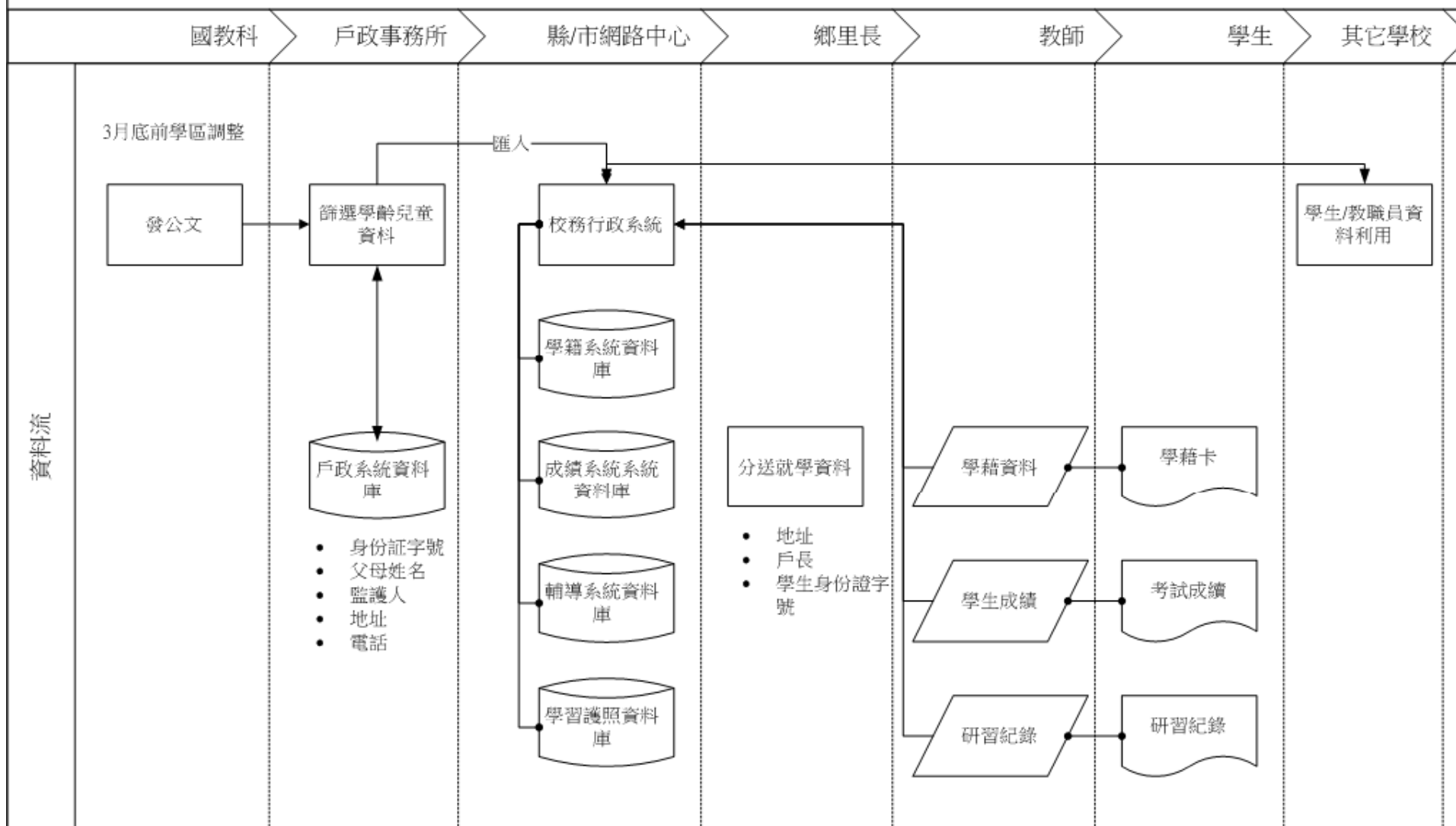
實作面策略_個人資料保護程序

- 個資抓漏



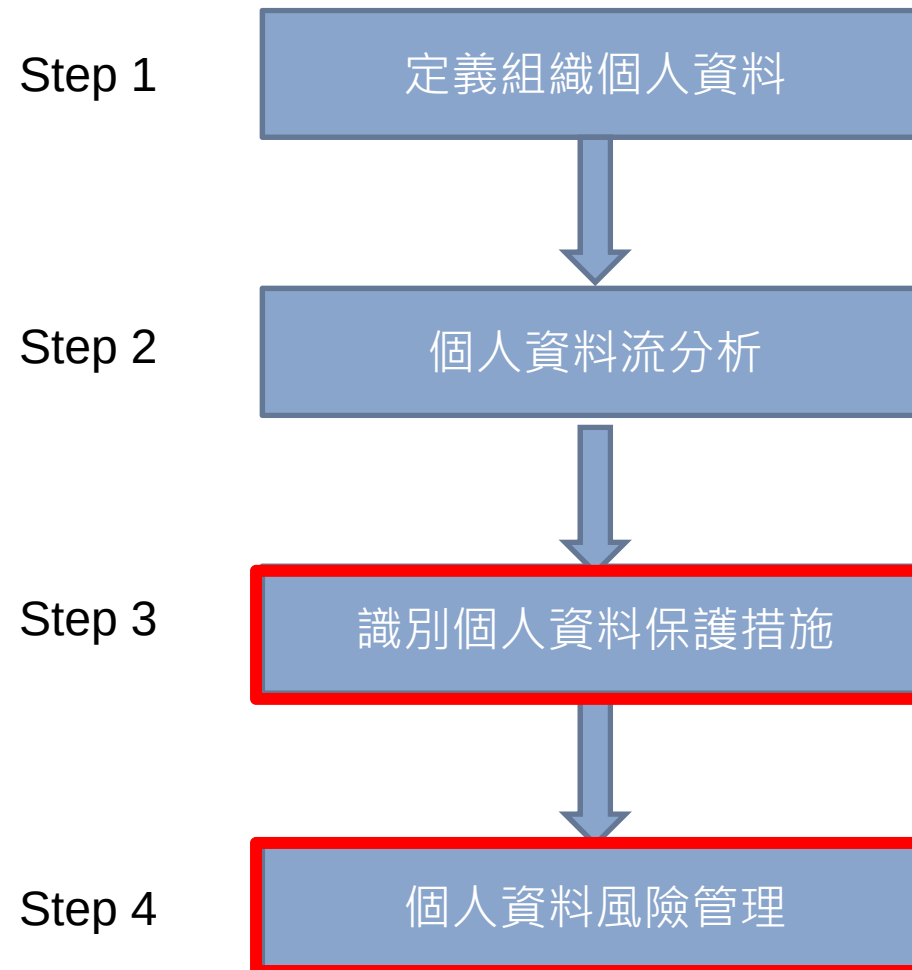
個人資料流分析-以教育單位為例

個人資料流分析-以教育單位為例



實作面策略_個人資料保護程序

- 個資抓漏



個資機密保護措施

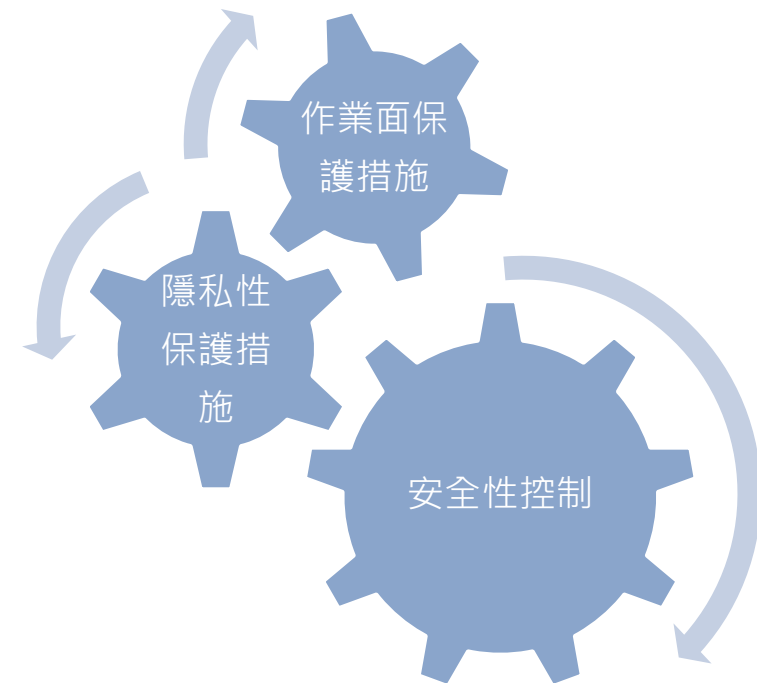
● 作業面保護措施(Operational Safeguards)

◆(一) 訂定政策與程序

1. 個資存取規範(資訊系統)
 - 個資存取控制清單(Role-based PII Access Control List)
2. 個資保存與銷毀程序
3. 個資外洩通報與處理程序
4. 系統開發流程隱私議題
 - 系統開發測試資料
 - DBA授權程序
5. 個資蒐處理利用及傳輸之使用限制
6. 懲處規範

◆(二) 宣導與教育訓練

1. 個資定義與適用法規
2. 使用與保護個資權責
3. 個資儲存與銷毀安全控制
4. ...



個資機密保護措施

- 隱私性保護措施(Privacy-specific Safeguards)

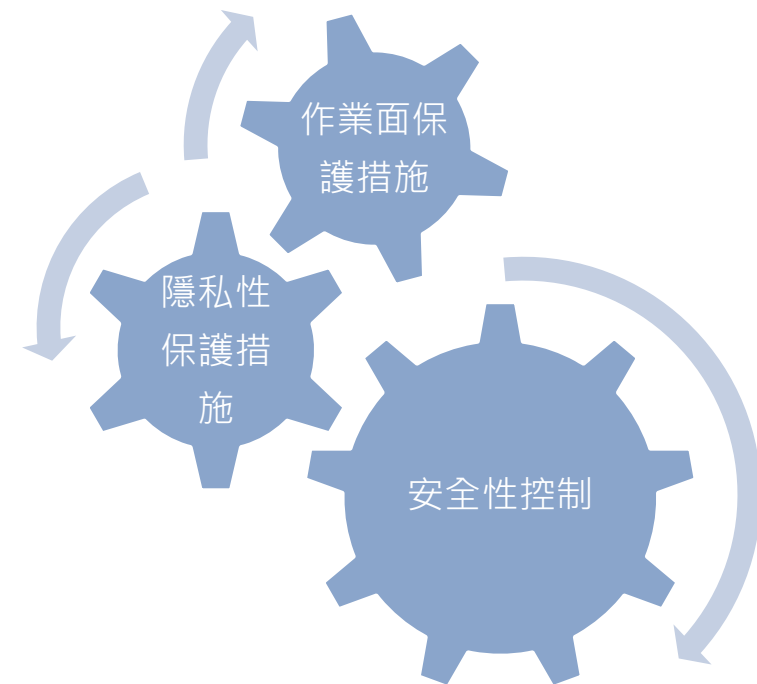
- ◆(一) 精簡蒐集、使用與持有個人資料

- ◆(二) 執行隱私衝擊評鑑

隱私衝擊評鑑(Privacy Impact Assessments, PIA)

- ◆(三) 去辨識化資訊 (可追朔)

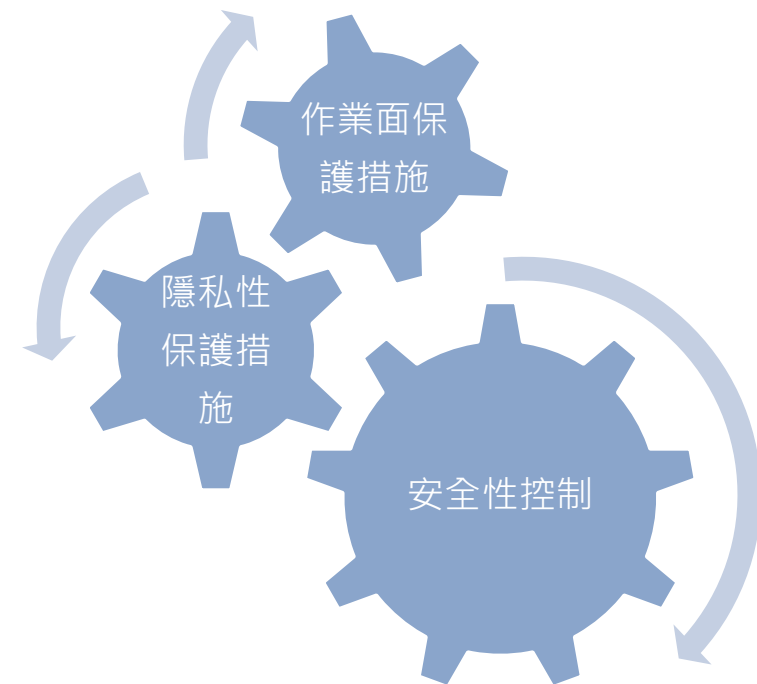
- ◆(四) 匿名化資訊 (不可追朔)



個資機密保護措施

- 安全性控制(Security Controls)

- ◆(一) 存取控制 / 遠端存取管理
- ◆(二) 權則分工 / 權限最小化
- ◆(三) 可攜式設備管理
- ◆(四) 稽核機制
- ◆(五) 資訊系統監控管理
- ◆(六) 資料保護
- ◆ ...



管理系統（制度）導入

資訊安全管理系統(ISO 27001, ISMS)

情報資產
紙本契約書
投、得標紀錄
其他
個人資料

物理性資產
電腦
儲存硬碟
伺服器
其他

軟體資產
OS軟體
Office軟體
業務軟體
其他

服務
建物維護
Hosting
宅配
其他

個資保護管理系統(JIS Q 15001, PMS)

日本有鑑於「個人資料」保護之重要，配合日本個人情報保護法相關規定，結合管理制度概念(PDCA)，設計一套「個人資料管理系統」(JIS Q 15001, PMS)

成功導入個資管理制度(JIS Q 15001)的企業，得申請使用隱私標章，藉以彰顯企業信譽



教育部現階段之因應作為

- 正研擬個人資料保護之相關辦法，未來將要求機關學校（含公私立學校）配合遵守，亦或是由各機關學校修改、引用適當之項目
- 針對C、D級機關學校(主要是技術學院、專科學校以及高中職)已選出26所學校，後續將於99年9月到12月針對資訊安全管理與個人資料保護作業進行稽核
- 如想要更了解個人資料保護相關工作事項，建議可參考「教育機構個人資料保護工作事項」

Q & A

Presenter's contact details

Jerry Yang

KPMG Advisory Services Co., Ltd.

+886 (2) 8101 6666 ext.10258

jerryyang@kpmg.com.tw

www.kpmg.com.tw

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

