個資法因應與準備

李維斌

逢甲大學
資訊處資訊長
資通安全研究中心主任
資訊工程學系教授

背景

- 個資法於2010年4月27日立法院三讀通過，2010年5月26日總統公布。
- 「個人資料保護法」，除第6條、第54條外，其餘條文定自2012年10月1日施行。
- 「個人資料保護法施行細則」，自2012年10月1日施行。

個人資料保護法

- 共六章 56條
  - 第一章　總則(第1條至第14條)
  - 第二章　公務機關對個人資料之蒐集、處理及利用總則(第15條至第18條)
  - 第三章　非公務機關對個人資料之蒐集、處理及利用(第19條至第27條)
  - 第四章　損害賠償及團體訴訟(第28條至第40條)
  - 第五章　罰則(第41條至第50條)
  - 第六章　附則(第51條至第56條)

立法精神

行爲規範

立法目的與精神

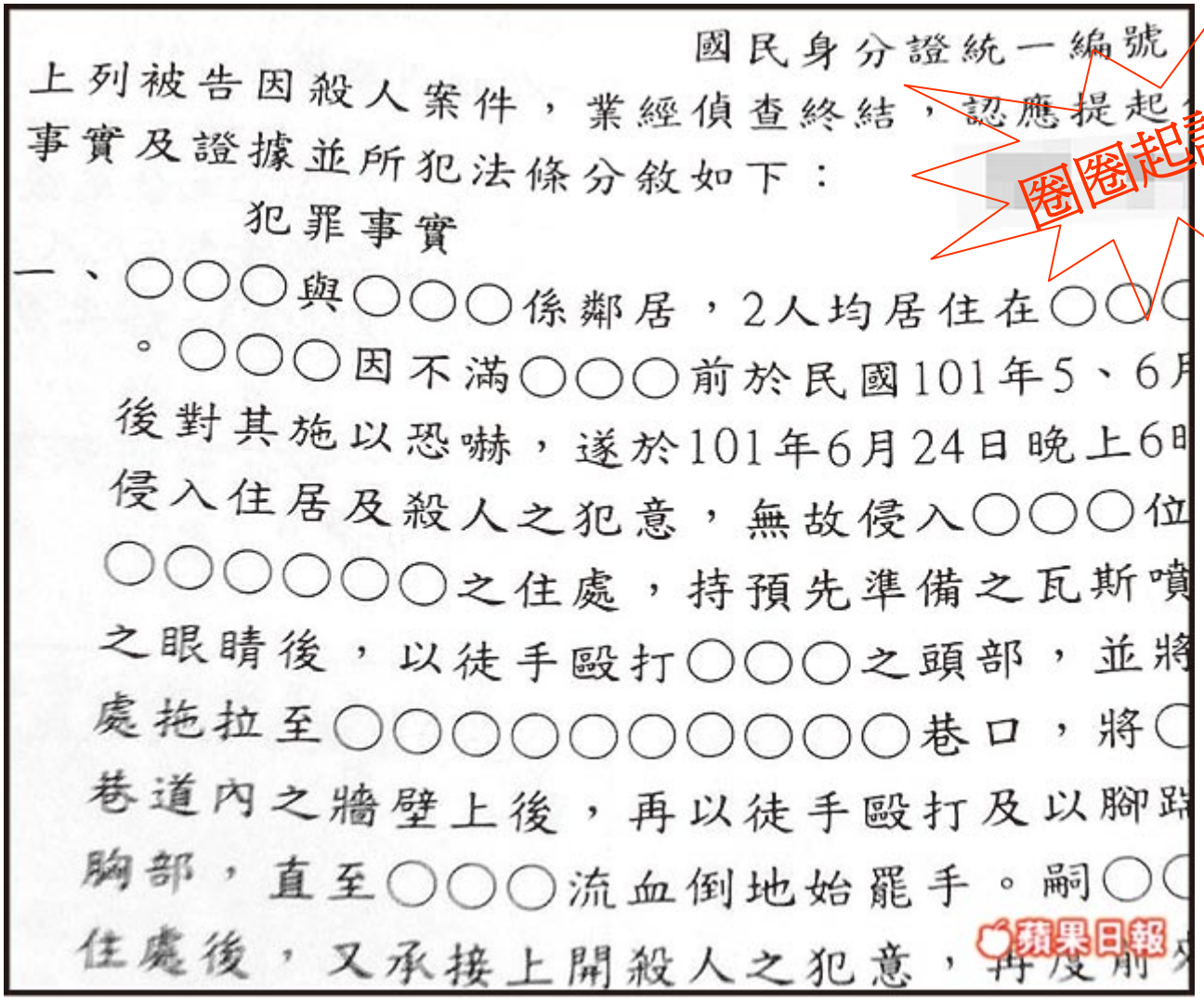
- (第1條)為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之**合理利用**，特制定本法。

個人資料行為規範

- 蒐集：指以任何方式取得個人資料。
- 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。
  - 國際傳輸：指將個人資料作跨國(境)之處理或利用。
- 利用：指將蒐集之個人資料為處理以外之使用。

安全維護措施

個資法來了...



國民身分證統一編號

上列被告因殺人案件，業經偵查終結，認應提起
事實及證據並所犯法條分敘如下：

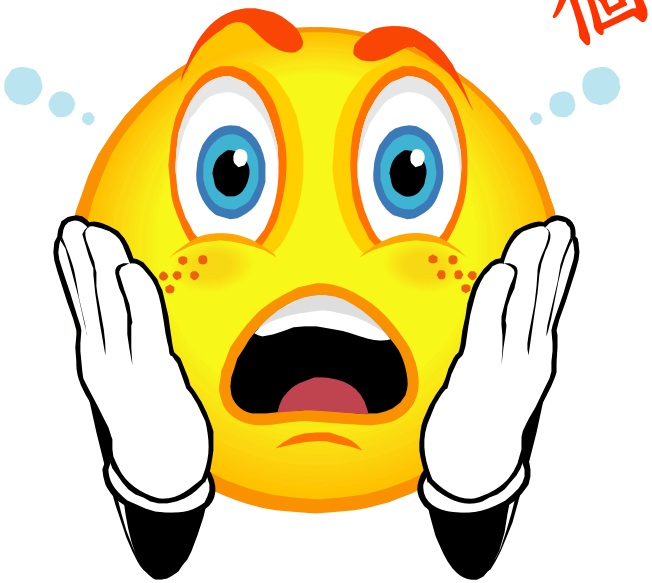
犯罪事實

一、○○○與○○○係鄰居，2人均居住在○○○
。○○○因不滿○○○前於民國101年5、6月
後對其施以恐嚇，遂於101年6月24日晚上6時
侵入住居及殺人之犯意，無故侵入○○○位
○○○○○○之住處，持預先準備之瓦斯噴
之眼睛後，以徒手毆打○○○之頭部，並將
處拖拉至○○○○○○○○○○巷口，將○
巷道內之牆壁上後，再以徒手毆打及以腳踢
胸部，直至○○○流血倒地始罷手。嗣○○
住處後，又承接上開殺人之犯意，再度前

圈圈起訴書

蘋果日報

個資恐慌症



必須展現學校對個人資料保護之決心，做好各項安全維護措施，

善盡保管人之責任。

誰是苦主？

IT部門的宿命

- 高度資訊化
- ISMS的先遣部隊
- 電腦處理個人資料保護法
- …

http://www.douban.com/photos/photo/716411968/

先前來了個 ISMS
現在又來了 PIMS

我是 C_{areer}I_sO_{ver}

萬事起頭難...

- 簡單的物理學！
- 通過相關認證？
- 回歸法律觀點！

修正條文...

- 增訂本法第十二條所稱適當方式通知之內涵及應包括之內容
- 一、本條新增。
- 二、本法所稱適當安全維護措施、安全維護事項、適當之安全措施，參考德國聯邦個人資料保護法第九條規定，應係指技術上及組織上之措施，爰為第一項規定。
- 三、為確保個人資料檔案之合法且正當蒐集、處理或利用，辦理安全維護之適當措施內容宜予規範，爰為第二項規定。其目的為與國際接軌，乃以 P-D-C-A方法論予以建立，使各企業得參考所列之十一款內容，考量組織規模與保有個人資料之數量或內容，依比例原則建立技術上與組織上之措施。

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

- 資訊安全管理系統(ISMS)是否能夠滿足個資法要求？
- 資訊安全管理系統(ISMS)與個人資訊管理系統(PIMS)的差異何在？

10

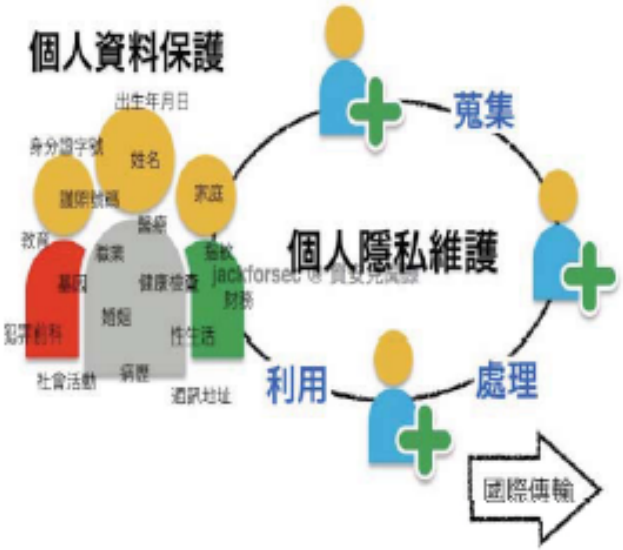
個資保護行為規範

蒐集
- 告知
- 特定目的
- 書面同意

處理
- 安全維護措施

利用
- 不逾越特定目的

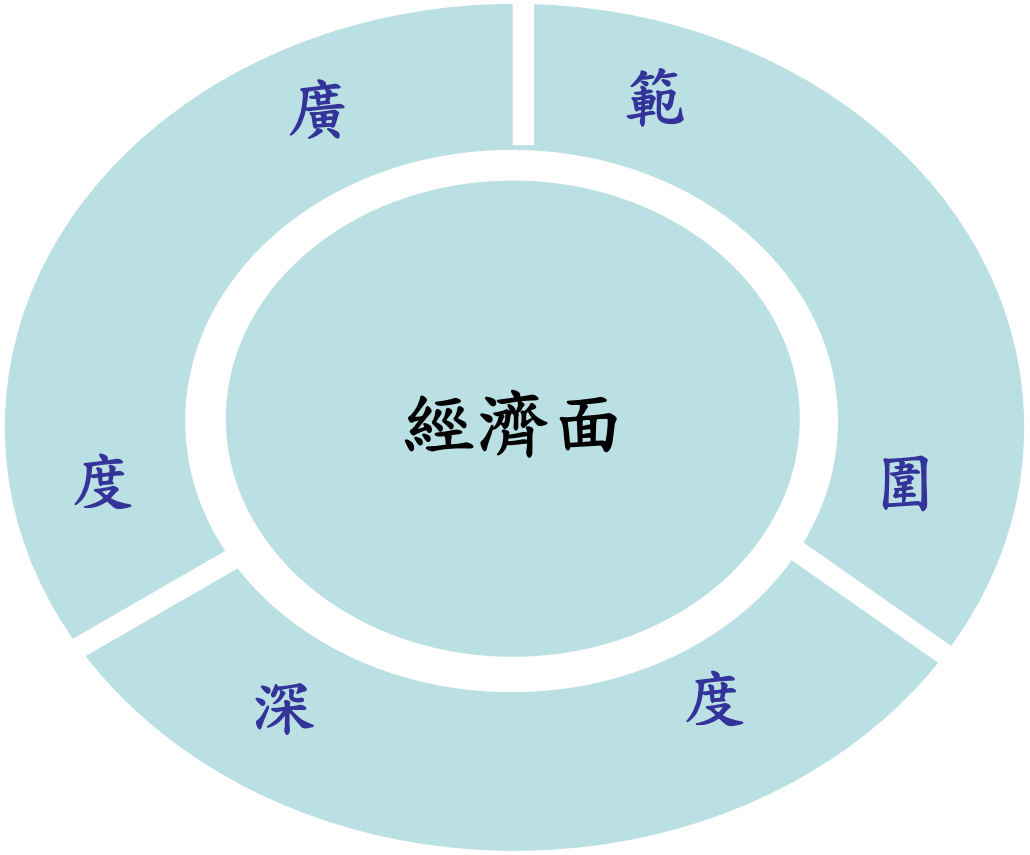
- 損害賠償
- 罰責



raising standards worldwide™

BSI

ISMS vs PIMS



持續性的工作

- 很夠力的個資小組
- 全面性的個資盤點
- 流程適法性的調整
- 個資觀念宣導教育
- 證據保存的證據力
- …

管理、操作、技術

主動出擊 克服最大靜摩擦力
借力使力 力道加倍
跨域學習 提升影響力

敬請指教