個資法說明與因應

吳國維
CEO, NIIEPA

大綱

- 個資法修正與何時實施？
- 個資法架構與部分條文
- 施行細則說明（部分）
- 該做甚麼？與案例說明
- 結語

大綱

- 個資法修正與何時實施？
- 個資法架構與部分條文
- 施行細則說明（部分）
- 該做甚麼？與案例說明
- 結語

個資法國際發展趨勢

1890年 隱私權的提倡

個人可不被打擾，安靜獨處生活的權利（the right to be alone)

1980年 隱私與個資保護開始受到國際組織重視

OECD提出「隱私保護與個人資料跨境流通指導原則」

1995年 歐盟提出個人資料保護指令

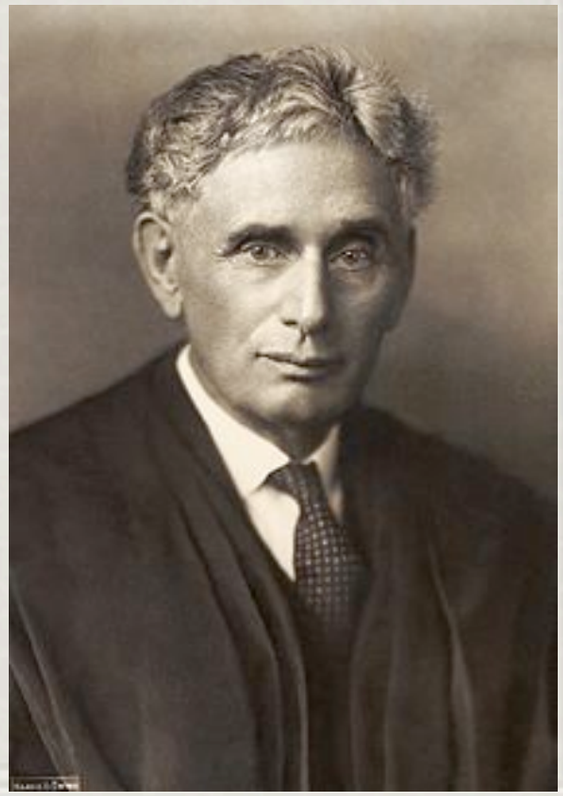
歐盟個人資料保護指令，影響包含我國在內之各國立法工作

2007年 APEC推動跨境隱私保護實驗計畫

我國為APEC成員之一，直接面臨來自國際上的壓力

Louis D. Brandeis :
(11.13, 1856 ~ 10.5, 1941)

- "snapshot photography"
-"the right to be left alone"
- The right offered by the Fourth Amendment which disallowed unreasonable search and seizure.



資料參考來源：資策會

“個人資料保護法”
與
” 電腦處理個人資料管理辦法 “

- 電腦處理個人資料保護法：84年8月11日制定公佈
- 個人資料保護法：99年5月26日修正公佈。
- 99年5月26日總統公佈日起，廢止許可登記制度。
- 其他法條施行日期，由行政院定之。
- 施行細則，由法務部定之。

何時施行？

- 總統於99年5月26日公佈
- 法務部預定完成施行細則之期間
  - 11月25日之目標是否可以達成？
- 將由行政院訂定施行日期
  - 今年十二月？明年六月？
- 自公佈日起，原有證照制度立即廢除
  - 金融業目前已無個資法執照

保護個人資料的其他法律

- 民法18、195（侵害人格權）
  - 財產上的損害賠償
  - 精神慰撫金
  - 回復名譽的適當處分
- 刑法315、315-1、318-1（妨害秘密罪）
  - 有期徒刑 -> 三年以下
  - 罰金 -> 三萬元以下
- 通訊保障及監察法19、24、25（秘密通信自由）
  - 損害賠償
  - 有期徒刑 -> 五年以下

新法修正重點

- 擴大適用主體：
  - 現行法：公務機關與非公務機關（醫院、學校、電信業、金融業、證卷業、保險業、大眾傳播業、徵信業等八類行業
  - 新法：打破行業別限制，包含各行各業及個人
- 擴大保護客體：
  - 現行法：使用電腦或類似設備處理之個人資料檔案。
    蒐集　：為建立個人資料檔案而取得個人資料
  - 新法　：以任何方式（包含紙本）留存的資料
    蒐集　：以任何方式取得的個人資料

新法修正重點（續）

- 增訂告知義務：
  - 直接搜集及間接搜集之告知義務
    - 修正施行前非由當事人提供之個人資料，應自本法修正施行之日起一年內完成告知。
    - 當事人拒絕行銷之權利
  - 資料違法外洩之通知義務
- 加重罰則：
  - 民事賠償：新台幣二千萬元->二億元
  - 刑事處罰：新台幣伍萬元->一百萬
    有期徒刑：三年以下->五年以下

大綱

- 個資法修正與何時實施？
- 個資法架構與部分條文
- 施行細則說明（部分）
- 該做甚麼？與案例說明
- 結語

個資法架構

第一章　總則（14）

第二章（4）
公務機關對個人資料之
蒐集、處理及利用

第三章（9）
非公務機關對個人資料之
蒐集、處理及利用

第四章　損害賠償及團體訴訟（13-1,1,11 ）

第五章　罰則（10 - 1,4,5）

第六章　附則（6）

何謂個人資料？

一般資料

自然人的
- 姓名
- 出生年月日
- 身分證號碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 病歷
- 聯絡方式
- 財務情況
- 社會活動

特種資料

- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

其他資料

- 得以直接或間接方式識別該個人之資料

特種資料蒐集、處理與利用

1. （個資法第六條）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：
    1. 法律明文規定。
    2. 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。
    3. 當事人自行公開或其他已合法公開之個人資料。
    4. 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。
    5. 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。

第二章：公務機關

1. 個資法第十五條：公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
    1. 執行法定職務必要範圍內。
    2. 經當事人書面同意。
    3. 對當事人權益無侵害。

第二章：公務機關（續）

1. 個資法第十六條：公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
    1. 法律明文規定。
    2. 為維護國家安全或增進公共利益。
    3. 為免除當事人之生命、身體、自由或財產上之危險。
    4. 為防止他人權益之重大危害。
    5. 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，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
    6. 有利於當事人權益。
    7. 經當事人書面同意。

第二章：公務機關（續）

1. 個資法第十七條：公務機關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：
    1. 個人資料檔案名稱。
    2. 保有機關名稱及聯絡方式。
    3. 個人資料檔案保有之依據及特定目的。
    4. 個人資料之類別。
2. 個資法第十八條：公務機關保有個人資料檔案者，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。

第三章：非公務機關

1. 個資法第十九條：非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
    1. 法律明文規定。
    2. 與當事人有契約或類似契約之關係。
    3. 當事人自行公開或其他已合法公開之個人資料。
    4. 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
    5. 經當事人書面同意。
    6. 與公共利益有關。
    7. 個人資料取自一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

    蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

第三章：非公務機關（續）

1. 個資法第二十一條：非公務機關對國際傳輸個人資料，而有下列情形之一者，中央目的事業主管得限制之：
    1. 涉及國家重大利益。
    2. 國際條約或協定有特別規定。
    3. 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。
    4. 以迂迴方式向第三國（地區）傳輸個人資料規避本法。

第四章：損害賠償及團體訴訟

1. 個資法第二十八條：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，復損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
    1. 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，並得請求為回復明與之適當處分。
    2. 依前二項情況，如被害人不易或不能證明其實際損害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。
    3. 對於同一原因事實造成多數當事人權利受害者之事件，經當事人請求損害賠償者，其合計最高總額以二億元為限。但因該原因事實所涉利益超過二億元者，以該所涉利益為限。
    4. ....
2. 個資法第二十九條：非公務機關違反本法規定，置個人資料遭不法蒐集、處理、利用或其他侵害當事人權力者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

第四章：損害賠償及團體訴訟

1. 個資法第三十條：損害賠償請求權，自請求權人知有損害及賠償義務人者起，因二年間不行使而消滅，自損害發生時起，逾五年者，亦同。
2. 個資法第三十一條：損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。
3. 個資法第三十二條：依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：
   I. 財團法人之登記財產總額達新台幣一千萬元或社團法人之社員人數達一百人。
   II. 保護個人資料事項於其章程所定目的範圍內。
   III. 許可設立三年以上。

第五章：罰則

1. 違法蒐集、處理或利用個人資料，足生損害與他人者：處二年以下有期徒刑、拘役或併科新台幣貳拾萬元以下罰金（告訴乃論：41）。
2. 意圖營利犯前項之罪者：處五年以下有期徒刑，得併科新臺幣一百萬以下罰金（無須告訴，檢察官得依職權訴追：41）。
3. 意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害他人者：處五年以上有期徒刑、拘役或科或併科新台幣一百萬元以下罰金（無須告訴， 檢察官得依職權訴追：42）。
4. 公務員假借職務之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

大綱

- 個資法修正與何時實施？
- 個資法架構與部分條文
- 施行細則說明（部分）
- 該做甚麼？與案例說明
- 結語

施行細則

- 本法第二條第二款所稱個人資料檔案，包括備份檔案及軌跡資料
  - 軌跡資料係指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（Log Files），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑...等，可用於比對、查證資料存取之適當性。因此，為符合本法個人資料保護與個人資料合理利用之立法意旨，個人資料檔案除備份檔案外，亦應保括軌跡資料在內，爰增訂如上。

施行細則（續）

- 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、滅失或洩露，採取技術上或組織上之必要措施。
  - 前項必要措施，應包括下列事項：（一）成立管理組織，配置相當資源。（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）必要之使用記錄、軌跡資料及證據之保存。（十一）個人資料安全維護之整體持續改善。：（PIMS）
- 第一項必要措施，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。

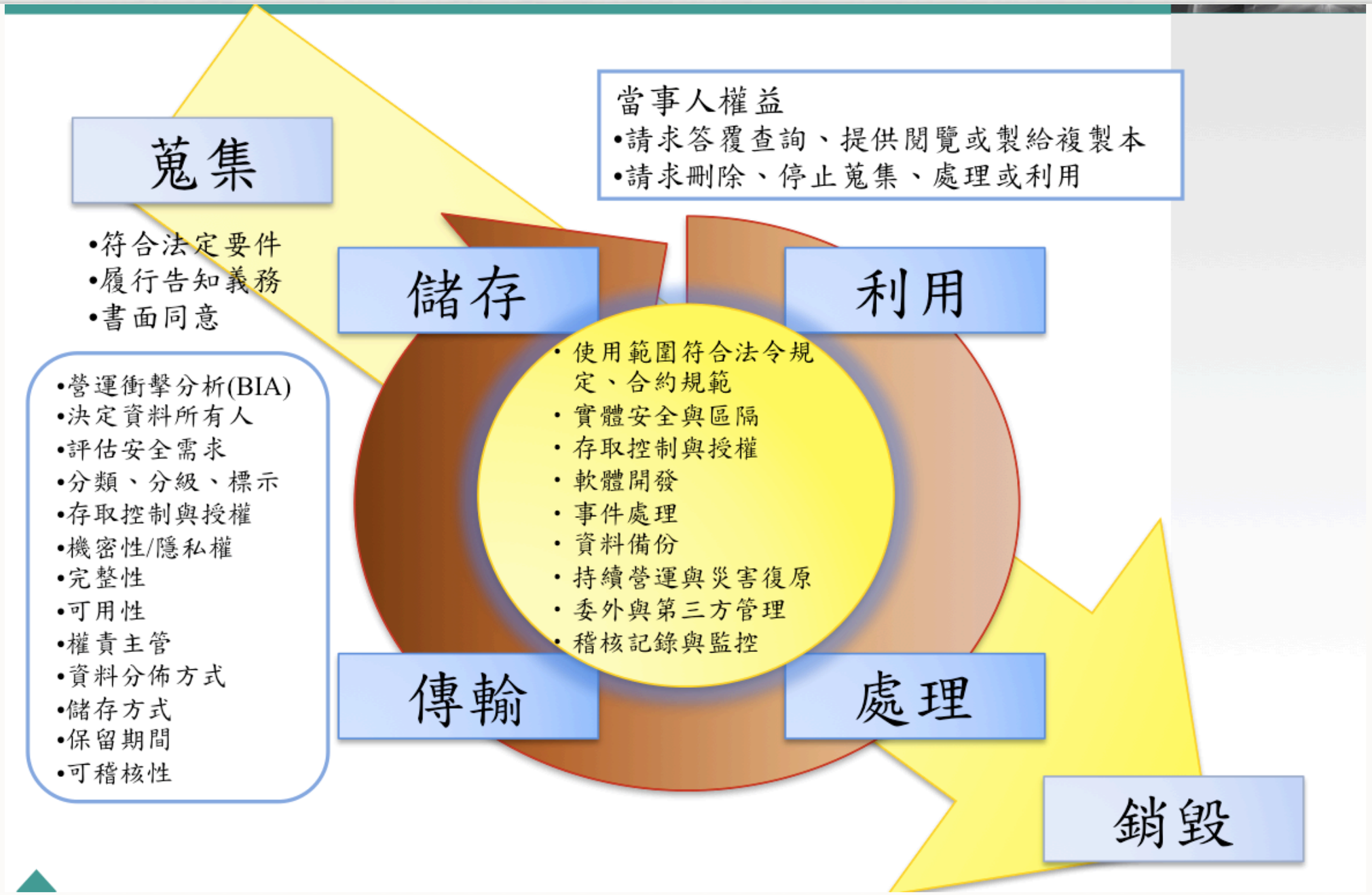
施行細則（續）

- 公務機關保有個人資料檔案者，應訂定個人資料安全維護規定，其內容應包括前項所定事項。
- 本法第十八條所稱專人，指具有管理及維護個人資料檔案之專業能力，且足以擔任機關檔案資料安全維護經常性工作之人員。公務機關為使專人具有辦理安全維護事項之能力，應經常或使專人接受相關專業之教育訓練。

大綱

- 個資法修正與何時實施？
- 個資法架構與部分條文
- 施行細則說明（部分）
- 該做甚麼？與案例說明
- 結語

個人資料生命週期管理


當事人權益
•請求答覆查詢、提供閱覽或製給複製本
•請求刪除、停止蒐集、處理或利用
蒐集
•符合法定要件
•履行告知義務
•書面同意
儲存
利用
•營運衝擊分析(BIA)
•決定資料所有人
•評估安全需求
•分類、分級、標示
•存取控制與授權
•機密性/隱私權
•完整性
•可用性
•權責主管
•資料分佈方式
•儲存方式
•保留期間
•可稽核性
•使用範圍符合法令規定、合約規範
•實體安全與區隔
•存取控制與授權
•軟體開發
•事件處理
•資料備份
•持續營運與災害復原
•委外與第三方管理
•稽核記錄與監控
傳輸
處理
銷毀

學校個資之種類

教職員、學生資料

姓名、電話、地址、
家長姓名、學生證號碼

校務行政資料

姓名、學生證號碼、成績單、操行等

健康資料

姓名、健康資料記錄

薪資資料

姓名、身分證字號、地址、電話、薪資、級別

檢視個資蒐集的合法性

確認是否爲個人資料？

↓

個人資料來源：直接從當事人取得
或自第三人間接取得

↓

是否取得書面同意或符合蒐集、處理
之其他例外規定

↓

在特定目的內之使用或符合特定目
的之例外規定（單獨書面同意）

↓

是否完成告知義務或符合免告知之例外情形？

法務部預計與施行細則中訂定之十二項安全維護事項

1. 必要之組織
2. 界定個人資料之範圍
3. 個人資料搜集、處理或利用之程序
4. 當事人行使權利之處理程序
5. 資料安全
6. 資料稽核
7. 人員管理及教育訓練
8. 記錄及證據之保存
9. 設備管理
10. 緊急應變措施及通報
11. 改善建議措施
12. 其他安全維護事項

個資保護，你可以作什麼？

定期備份

- 個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩露。

設定範圍

- 個人資料輸入、輸出、更新或註銷時，應該釐定使用範圍，以及調閱或存取的權限。

帳號密碼

- 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識之登入通行碼。個人資料檔案使用完畢後，應即退出應用程式，不得留置與電腦中。

個資保護，你可以作什麼？（續）

建立程序

- 含有個人資料的紙本，運用於申請、列印、存檔、轉交及銷毀等行爲，應建立相關之授權、監督及行爲記錄的機制。

彌封加密

- 內部傳遞或其他機關交換個人資料時，應在實體文件密封袋上，加上彌封，或對電子資料檔案壓縮加密，並加以記錄檔案的流向。

紀錄追蹤

- 對於調閱個人資料的人，加以記錄其調閱身份及行爲。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

審核公布

- 機關學校單位管理之網站或網頁內容，於確有必要公佈個人資料時，須經所屬單位主管核准，且依相關法律及規範處理，才能公佈。

個資保護你可以作什麼？：設備管理

專人處理

- 應指定專人負責管理儲存個人資料的設備及設施，並檢查、處理設備的異常事件。

安全隔離

- 儲存個人資料的設備，應置放於安全區域，例如：門禁控管的辦公區域、機房等，避免有心人士或非授權人員存取。

委外監督

- 外部人員及個人，更新或維修電腦設備時，應指派專人在場，確保個人資料之安全，以及防止個人資料外洩。

徹底刪除

- 儲存個人資料之電腦或相關設備，如需報廢或移轉他用時，應確實刪除該設備所儲存的個資檔案。

個資保護，你可以作什麼？：人員管理

持續訓練

- 機關學校應對處理個人資料的人員，施與教育訓練，並定期與單位內宣導個資隱私保護之重要性。

帳密更換

- 處理個人資料之人員，其職務如有異動，應將所保管之資料移交。而接辦人員應重置通行碼，也應視需要更換使用者識別帳號。

權限取消

- 處理個人資料之人員，應簽訂保密切結書，並確認與離職或合約終止時，取消其使用者識別帳號，且收繳其通行證及相關證件。

國際資訊安全、個資防護管理系統標準
– ISO 27001/PIMS

11領域、39控制目標、133控制要點

資訊安全政策

資訊安全組織

資訊資產分類與管理

人員安全

實體與環境安全

通訊與操作管理

存取控制

系統發展與維護

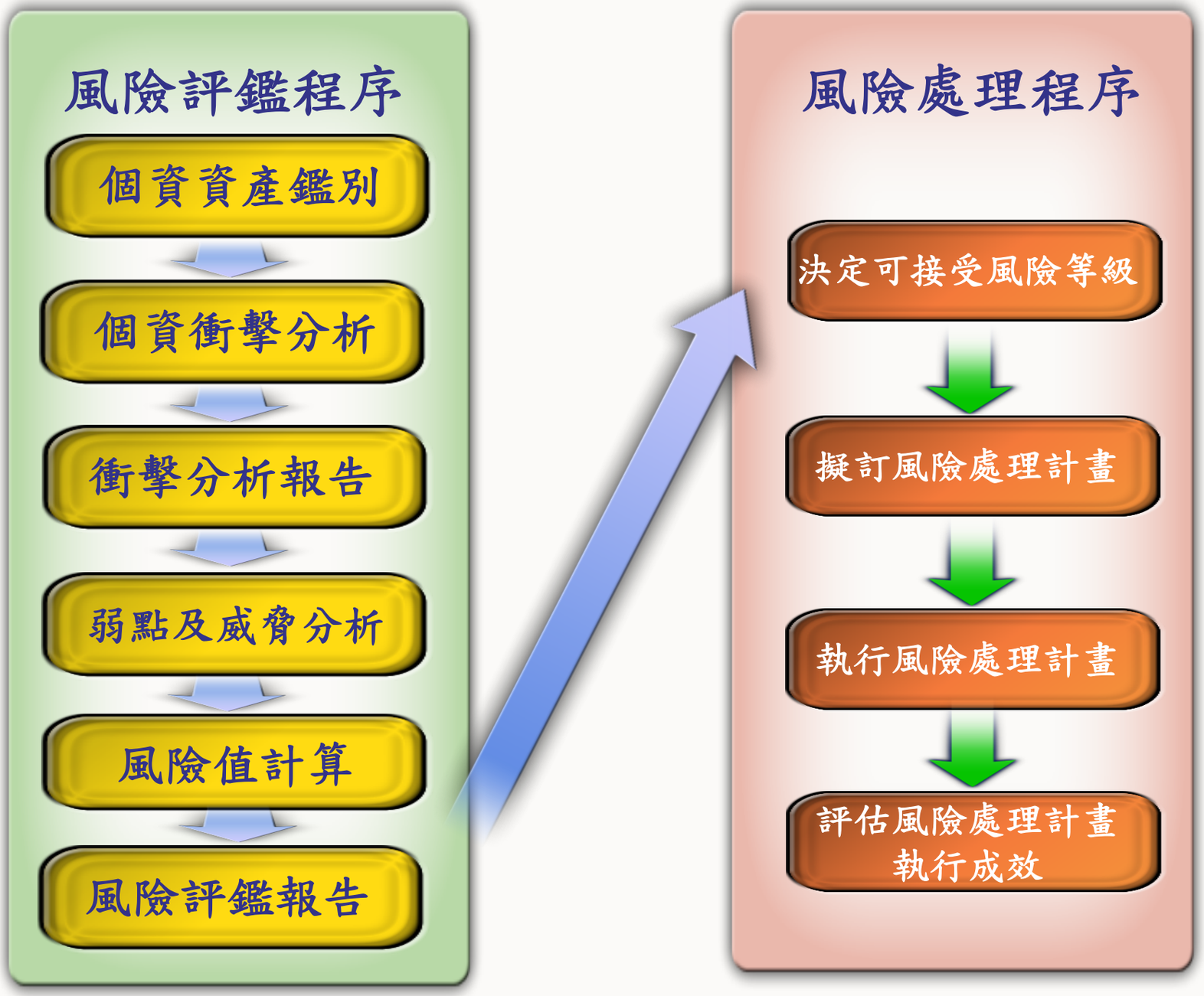
資訊安全事件管理

業務持續運作管理

法令規章之遵循

資訊安全管理稽核

個人資料風險管理程序
– PIMS



案例

1. 學校活動（含社團）是否可透過信件寄發給所有學生？誰可以寄發或使用？
   - 學校或社團辦活動可以透過信件寄發通知給學生，因爲此舉符合學校教育及成立社團之特定目的。
   - 學校辦活動之單位、以及社團都可以寄發及使用學生的個人資料。
   - 若學校活動是廠商的行銷活動，即有爭議空間，學校不可以把學生資料給合辦活動的廠商來使用。
   - 學校須評估學校使用學生個人資料之用途與目的，確認是否符合學校只「教育興學」目的，更謹慎的作法爲與教育部討論，請教育部依學校教學需求，請法務部增修「特定目的」。

案例（續）

2. 畢業紀念冊上的學生資料是否屬於個人資料？圖書館中陳列的歷屆畢業紀念冊是否應該管理？
   - 畢業紀念冊的學生（及家長）資料是屬於個人資料。
   - 過去畢業紀念冊的收集與公開並非違法行爲，但因爲現在越來越多的販賣個人資料或詐騙個人資料之行爲，所以學校應改變個人資料之保管方式，就能加以控管限制閱覽畢業紀念冊的人員。

案例（續）

3. 學生畢業後是否仍可以寄發活動通知？或應該在學生畢業前先取得其同意授權？歷屆畢業生個人資料應該如何管理，才符合個資法？

- 學校使用校有個人資料還須符合「教育行政」之特定目的，若超過特定目的則不能使用，可能需要在學生畢業前取得授權。
- 一般人並不會反對學校辦理校友活動是超過特定目的，但學校應與教育部、法務部溝通，確保學校能繼續使用校有資料。此外，學校應建立管控機制，避免校有資料外洩。

案例（續）

4. 若當事人尚未成年，請問個人資料蒐集需要取得當事人或監護人同意嗎？
   - 民法規定，滿20歲爲成年。未成年人包括：
     - 未滿七歲，無行爲能力人：應由法定代理人代表意思代表，並帶受意思表示。
     - 滿七歲以上，爲限制行爲能力人，其爲意思表示及受意思表示，原則上應得法定代理人之允許。
   - 依民法規定，未成年人爲書面同意，應由法定代理人代爲書面同意，或得到法定代理人之允許。
   - 雖有上述限制，但民法規定，已經結婚之未成年人，有行爲能力。換言之，已經結婚只未成年人，可以自行爲書面同意，並無法定代理人代爲書面同意或允許之問題。

案例（續）

5. 老師擔心學生因閱讀一些讀物而造成行爲偏差，是否可以向圖書館調閱學生借書記錄？

- 借書記錄含學生姓名、社會活動或其它得以識別學生之資料，此屬於個人資料之範疇。
- 圖書館保存借書記錄之目的爲「學生資料管理」，並不具評估學生行爲偏差與否只目的。
- 老師向圖書館調閱學生借書記錄，固然可認爲是學校內部「教育或訓練行程」目的，但仍應與該目的之必要範圍內爲之，並應尊重當事人權益。
- 如有證據可合理懷疑某學生偏差行爲與閱讀有關聯，老師爲進一步確認而向圖書館調閱學生借書記錄，或可被認爲符合「教育或訓練行政」目的之必要範圍。若老師在無任何證據情況下，全面調閱學生借書記錄，恐被認爲逾越「教育或訓練行政」目的之必要範圍，因而違反個資法的規定。

案例（續）

6. 在公告欄公告曠課學生名單（學生姓名、學號），有違反個資法嗎？
   - 有關獎懲應符合學校辦理「教育與訓練行政」之目的，公佈並不違反個資法。
7. 若當事人自行公開其特種個人資料，是否可以蒐集與傳播？
   - 已公開的特種資料雖然可以蒐集，但是蒐集及利用仍須依個資法織特定目的範圍，也不能任意傳播。

案例（續）

8. 若將同仁資料提供給保險公司進行投保，那我有沒有利用（將蒐集祇個人資料爲處理以外之使用）的行爲？我算對保險公司揭露個人資料嗎？

   - 依據公司（或機關）行政處裡，的確公司（或機關）有權利提供保險公司（例如勞保局、健保局或保險公司，因爲這是公司（或機關）福利的一部分有關公司（或機關）同仁保險公司所需的資料。保險公司透過公司（或機關）人事或行政人員取得這份個人資料後，保險公司只能作爲與保險業務範圍內的應用，不得延伸做其他不符合保險業務外之行銷或其他目的之使用。

案例（續）

9. 公告欄公告曠課學生名單（學生姓名、學號）有違反個資嗎？
   - 有關獎懲之作法，應符合學校辦拉教育行政之目的，公布應不違反個人資料保護法。
10. 學校爲了保護學生，收集學生病史、健康、身份（低收入戶）資料等，有涉及特種個資嗎？
   - 有關病史、健康檢查部分，要看教育部的法規有沒有允許，務必請教育部與法務部協調、確定，以便學校單位遵行。低收入戶並非特種個資。
11. 個資法中的特種個人資料規範中，若個資擁有者自行公開，是否可以收集？是否可以拿來傳播？
   - 雖然自行公開之特種資料可以收集，但處理、利用仍要遵行各資法規定之範圍，也就是說，必須符合特定目的，並不是可以任意傳播

案例（續）

12.學校是否可以寄發校友或學校認同卡給學生或校友？

- 學校當初蒐集校友個人資料之特定目的爲「教育行政」，或學生資料管理。學校寄發認同卡給校友，構成利用校友個人資料之行爲，似乎踰越上述特定目的，除非取得校友之書面同意，否則不得爲之

13.網頁上的學生家長區，家長可以查詢學生之個人曠課、操行嗎？

- 學校將學生的缺曠課資料及操行成績提供家長查詢，似爲學校執行法定職務必要範圍，且與蒐集之特定目的（教育行政）相符。惟大學生瞭解自己的缺曠課資料及操行成績，依其年齡及身份，應爲其日常生活必需，且滿20歲之大學生已爲成年人，不論其爲意思表示或受意思表示，均無須法定代理人（家長）之允許，因此大專院校是否有必要將學生缺曠課資料及操行成績提供給家長查詢，使能達到教育行政指目的？恐有疑義，建議教育部應與法務部會同對此作出統一解釋，以便學校之所遵循，避免學生質疑。

大綱

- 個資法修正與何時實施？
- 個資法架構與部分條文
- 施行細則說明（部分）
- 該做甚麼？與案例說明
- 結語

相關案例（法務部）

- 公務機關將蒐集他人電子郵件地址資料提供他人查詢服務，如其並未與自然人之姓名等相結合，尚不足以識別該個人者，則該資料即非上開規定所稱之個人資料，並無電腦處理個人資料保護法規定之適用。
- 電話門號如未與申請人或使用人之姓名作連結，該門號僅係電話通話通訊線路之識別代碼，尚不足資識別該自然人爲何人時，自不屬本法所稱之個人資料。
- 另如該電話門號係由公司或法人名義申請，由於非屬自然人之個人資料，則根本與本法無涉。

相關案例（法務部）

- 如電信公司僅提供電話門號資料，並未揭露該門號申請人或使用人之姓名，由於未達足資識別特定當事人之程度，資無本法適用問題。
- 車輛之車牌號碼，並無法識別該車輛所屬之個人資料，非屬於本法所稱之個人資料。
- 如地方政府停車資訊公開方式（通知單單號、停車日期、停車時間、停車路段及應繳金額等），未與自然人姓名等相結合，因無從以此方式直接或間接識別該個人，故非屬上開規定所稱之個人資料，而無電腦處理個人資料保護法之適用問題。

資安與個資防護基本觀念

- 資訊安全與個資防護不是僅爲資訊人員之責任
- 資訊安全與個資防護是組織全體的責任
- 資訊安全與個資防護需要長官的大力支持
- 資訊安全與個資防護之推動不是專案形式，必須持續
- 組織每位成員都可能成爲資安與個資防護漏洞
- 管理階層應提供承諾建立、完成、監督、檢視、維護及改善資安與個資管理制度之落實

QUESTIONS?