



南投縣101年度各國民中、小學 個人資料保護法研討會

個人資料保護法與案例介紹

日期：2012/10/04(四)

時間：13:30~16:30

講師：張力允

第一階段課程大綱

- 個人資保護法介紹
- 個人資料保護法部分條文

- 個人資料保護法介紹
- 個人資料保護法部分條文

個人資料，無所不在



個人資料保護法

全國法規資料庫入口網站 - Windows Internet Explorer
 http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

Windows Live Bing 好友動向 個人檔案 郵件 相片 行事曆 MSN 分享

全國法規資料庫入口網站

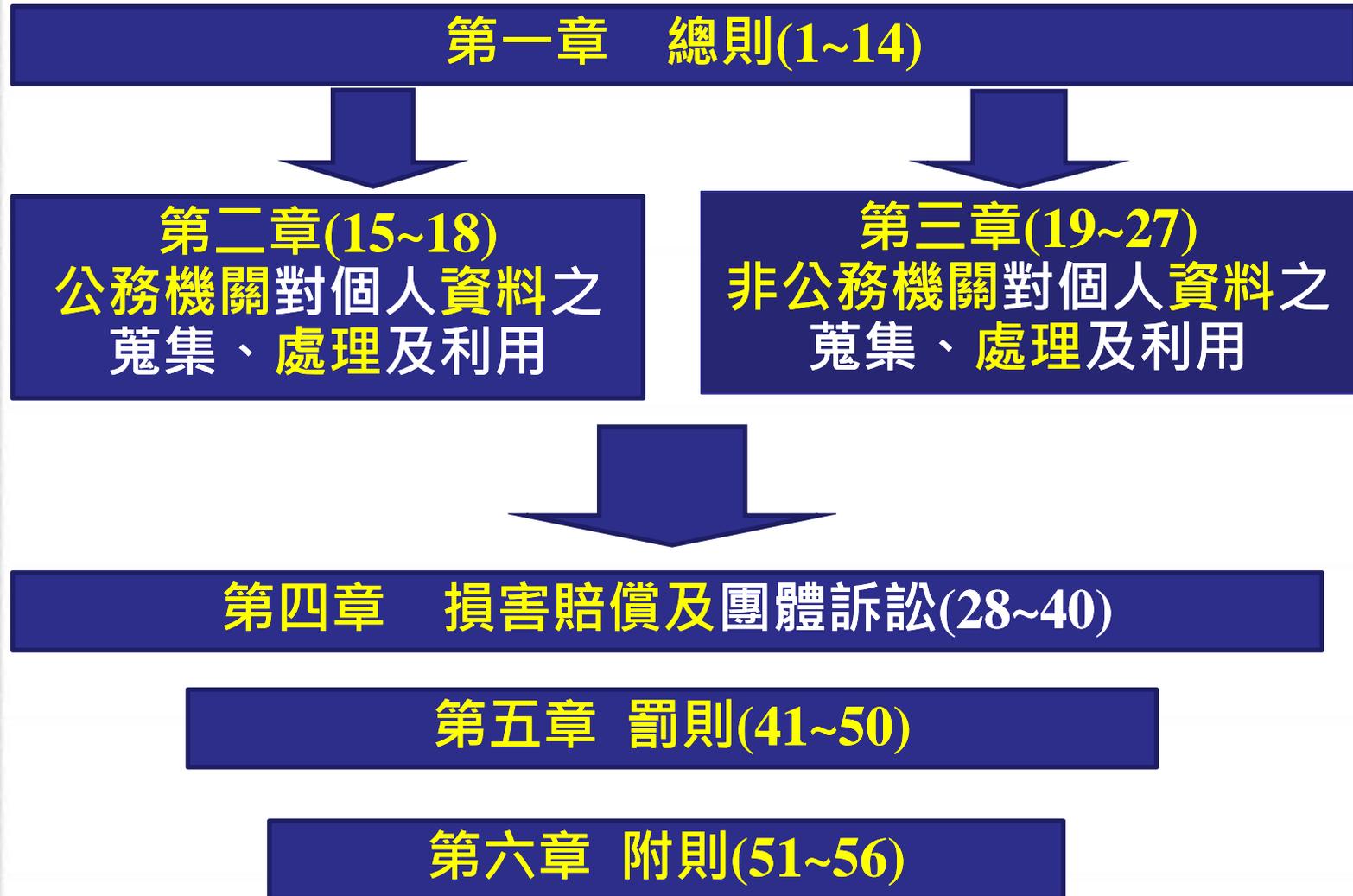
全國法規資料庫
Laws & Regulations Database of The Republic of China

最新訊息 法規類別 法規檢索 司法判解 條約協定 兩岸協議 綜合查詢

現在位置：[首頁](#) > [法規](#) > 條文內容

所有條文	
名稱	個人資料保護法 <small>英</small>
修正日期	民國 99 年 05 月 26 日
生效狀態	※本法規部分或全部條文尚未生效 本法 99.05.26 修正公布之全文施行日期，由行政院定之。但現行條文第 19~22、43 條之刪除，自公布日施行。
第一章 總則	
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。
第 2 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。

個人資料保護法架構圖



個人資料保護法(續)

- 立法院於99年4月27日，將電腦處理個人資料保護法，修訂並三讀通過為「個人資料保護法」
- 個人資料保護法於99.05.26 修正公布之全文施行日期，由行政院定之。
- 修訂方向：
 - 擴大保護客體
 - 普遍適用主體
 - 增修行為規範
 - 強化行政監督
 - 妥適調整罰則
 - 促進民眾參與

個人資料保護法(續)

- 擴大適用主體：
 - 現行法：
 - 公務機關 (依法行使公權力之中央或地方機關)
 - 非公務機關：醫院、私立學校、電信業、金融業、證券業、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，包括各行各業及個人。
 - 受委託蒐集、處理或利用個人資料者，視同委託機關。
- 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 (包括紙本) 留存的資料。
 - 蒐 集：以任何方式取得個人資料。
 - 個 人：生存之特定或得特定之自然人。

個人資料保護法(續)

- 增訂告知義務：
 - 直接蒐集及間接蒐集之告知義務。
 - 資料違法外洩之通知義務。

個人資料保護法(續)

- 調整賠償義務及罰則：
 - 民事賠償：新台幣2千萬元→2億元。
 - 刑事處罰：新台幣5萬元→100萬元。
 - 有期徒刑：3年以下→5年以下。
 - 意圖營利犯罪者，非告訴乃論。
 - 行政處罰：新台幣10萬元→50萬元。
- 主管機關並得為下列處分：
 - 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。
 - 公布違法情形及其姓名或名稱與負責人。

個人資料保護法(續)

- 99年5月26日總統公布日起，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。
- 預計將於101年10月1日實施新法，同時將採兩階段修法，第1階段「小修」部分，預計7月送立法院；第2階段大修預計1年內提出。

何謂個人資料?? (個資法第二條第一款)

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

一般
資料



特種
資料

- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

更嚴
格

其他
資料

- 得以直接或間接方式識別該個人之資料

我們對其資料有什麼權利??

- 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。

上述權利，不得請求當事人預先拋棄，也不得以特約限制之。

個人資料的基本保護原則

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

立法理由：

避免資料蒐集者巧立名目或理由，任意蒐集、處理或利用個人資料，明定個人資料之蒐集、處理或利用，應與蒐集目的有正當合理關聯，不得與其他目的作不當聯結。

個人資料的基本保護原則(續)

- 不要因為擔心違反個資法，導致過度地「避免或迴避」必要資料之蒐集與使用。
- 個人資料保護的重點在於「保持個人資料的正確性，並且告知當事人所蒐集資料的特定目的，以及安全處理與使用方式與範圍，並作好適當的刪除與銷毀工作」。

哪些人應遵守個資法??

- 電腦處理個人資料保護法（現行法）：
 - 公務機關：依法行使公權力之中央或地方機關。
 - 非公務機關：醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業、徵信業等八類行業。
- 個人資料保護法（由行政院決定施行日）：
 - 公務機關：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：前款以外之自然人、法人或其他團體。

哪些行為受個資法規範??

- 蒐集：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。

哪些行為受個資法規範??(續)

- 處理：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。
 - 內部傳送：公務機關將資料傳送給國外辦事處，總公司將資料傳送給分公司。

哪些行為受個資法規範??(續)

- 利用：將個人資料為處理以外之使用。
 - 直接對當事人使用其個人資料，例如對當事人從事行銷。
 - 將資料提供當事人以外之第三人。

哪些行為受個資法規範??(續)

- 國際傳輸：將個人資料作跨國（境）之處理或利用。
 - 向大陸地區傳輸個人資料(法務部94年8月26日法律字第0940029553號)。
 - 外國在台分公司將客戶資料傳遞予外國總公司(法務部90年4月27日法律決字第014746號)。

個人資料保護法免責條款

- 媒體基於新聞報導公益目的重新回到免為告知範。
- 非公務機關使用或處理個人資料，如果與公共利益有關，或是個人資料取自於一般可得來源，且使用該資料有比保護資料更重大利益，則不需要經過當事人同意即可使用；不過當事人可以主動請求刪除、停止使用相關個人資料。
- 單純的個人或家庭活動，以及在公開場所或公開活動中，所蒐集、處理或利用的個人影音資料，只要沒有與其他個人資料結合，都不適用個資法。

- 個人資料保護法介紹
- 個人資料保護法部分條文

基本原則：
不得逾越特定目的

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。(§5)



電腦處理個人資料保護法之特定目的

民國 85 年 08 月 07 日公發布

人身保險業務 (依保險法令規定辦理之人身保險相關業務)	人事行政管理
土地行政	公立與私立慈善機構之目標
公共衛生	公共關係
火災預防與控制	戶政及戶口管理
不動產服務	公職人員財產申報業務
立法或立法諮詢	民政
代理與仲介之管理	犯罪預防、型事偵查、執行、矯正、保護處分或更生保護事務
外匯管理	生態保育
合法性審計	交通運輸
刑案資料管理	存款與匯款業務管理
行銷 (不包括直銷至個人)	行銷 (包括直銷至個人)
有價證券之承銷、自營買賣或代客買賣業務管理	有價證券與有價證券持有人登記
住宅政策	兵役行政
社會行政	社會服務或社會工作
投資管理	供水與排水服務

電腦處理個人資料保護法之特定目的

資訊與資料庫管理	會員 (籍) 管理 (含會員指派之代表)
農產品交易	農產品推廣資訊
募款	發照與登記
傳播行政與管理	華僑資料管理
經營郵政業務郵政儲匯保險業務	經營電信業務與電信增值網路業務
債權整貼現及收買	漁業行政、管理
僱用服務管理	輔助性與後勤支援
學生資料管理	徵信
學術研究	選舉、罷免事務
衛生行政	營建業之行政管理
輻射公害	輻射防護
環境保護	糧食行政、管理
保健醫療服務	警政
護照、簽證及文件證明處理	觀光旅館業及旅行業管理業務
其他中央政府	其他公共部門
其他司法行政業務	其他地方政府事務
其他合於營業登記項目或章程所定業務之需要	其他金融業務管理
其他財政收入	其他財政服務
其他諮詢與顧問服務	

電腦處理個人資料保護法之特定目的

科技管理	法律服務
法院執行業務	法院審判業務
放射性廢棄物收集與處理	金融監理
客戶管理	信用卡或轉帳卡之管理
訂位、住宿登記與購票事項	政府福利金或救濟金給付行政
信託業務管理	計畫與管制考核
退撫基金或退休金管理	保險監理
個人資料之交易	捐供血服務
畜牧行政、管理	財產保險業務 (依保險法令規定辦理之財產保險相關業務)
財產管理	借款戶與存款戶存借作業綜合管理
消費者保護與交易準則	核貸與授信業務
教育或訓練行政	授信業務管理
國稅與地方稅稽徵	商業與技術資訊
票據交換管理	採購與供應管理
救護車服務	統計調查與分析
就業安置、規劃與管理	著作權行政
會計與相關服務	電信監理業務

電腦處理個人資料保護法之特定目的及 個人資料之類別修正草案對照表

修正代號〇〇二至〇〇六、〇〇八至一〇一；增訂代號一〇二至一八一。

個人資料類別

修正代號C〇〇一、C〇一一、C〇〇三、C〇三三、C〇二三、C〇三四、C〇五二、C〇五七、C〇六一、C〇六六、C〇八五、C〇八九、C一一一、C一一四；增訂C〇五八。

公務機關個人資料之蒐集、處理及利用

特定目的內(\$15)

- 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。

特定目的外 (\$16)

- 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，且資料經過處理後或依其揭露方式無從識別特定當事人。
6	有利於當事人權益。
7	經當事人書面同意

非公務機關個人資料之蒐集、處理及利用

特定目的內(§19)

- 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	個人資料取自於一般可得之來源。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。

非公務機關個人資料之蒐集、處理及利用

特定目的外 (§20)

- 非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，應於蒐集之特定目的必要範圍內為之。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，且資料經過處理後或依其揭露方式無從識別特定當事人。
6	經當事人書面同意。

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。

非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

直接蒐集個人資料的告知義務

何時應該告知? 向當事人蒐集之前

應告知事項

1	機關名稱。
2	蒐集目的。
3	個人資料類別。
4	利用期間、地區、對象及方式。
5	當事人依第3條規定得行使之權利及方式： (1) 查詢或請求閱覽。 (2) 請求製給複製本。 (3) 請求補充或更正。 (4) 請求停止蒐集、處理或利用。 (5) 請求刪除。 上述權利，不得預先拋棄或以特約限制。
6	如當事人得自由選擇提供個人資料，不提供將對其權益之影響。

得免為告知之情況

1	依法律規定得免告知
2	個人資料之蒐集係公務機關執行法定職務所必要
3	告知將妨害公務機關執行法定職務
4	告知將妨害第三人之重大利益
5	當事人明知應告知之內容

間接蒐集個人資料的告知義務

何時應該告知？處理或利用當事人的個資前

應告知事項

1	機關名稱。
2	蒐集目的。
3	個人資料類別。
4	利用期間、地區、對象及方式。
5	當事人依第3條規定得行使之權利及方式： (1) 查詢或請求閱覽。 (2) 請求製給複製本。 (3) 請求補充或更正。 (4) 請求停止蒐集、處理或利用。 (5) 請求刪除。 上述權利，不得預先拋棄或以特約限制。
6	個人資料來源。

得免為告知之情況

1	依法律規定得免告知。
2	個人資料之蒐集係公務機關執行法定職務所必要。
3	告知將妨害公務機關執行法定職務。
4	告知將妨害第三人之重大利益。
5	當事人明知應告知之內容。
6	當事人自行公開或其他已合法公開之個人資料
7	不能向當事人或其法定代理人為告知。
8	基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
9	大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

- 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。(§12)



個人資料之安全保護相關規定

- 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(§18)。
- 非公務機關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 (§27)。

個資法施行細則草案所列的安全維護事項

保護標的：

防止個人資料被竊取、竄改、毀損、滅失或洩漏

1	成立管理組織，配置相當資源。
2	界定個人資料之範圍。
3	個人資料之風險評估及管理機制。
4	事故之預防、通報及應變機制。
5	個人資料蒐集、處理及利用之內部管理程序。
6	資料安全管理及人員管理。
7	認知宣導及教育訓練。
8	設備安全管理。
9	資料安全稽核機制。
10	必要之使用紀錄、軌跡資料及證據之保存。
11	個人資料安全維護之整體持續改善。



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。



此11項安全措施內容為參照英國BS10012:2009及日本JISQ15001:2006等個人資料管理系統之規範，以P-D-C-A循環之概念予以建立。

公務機關(公立學校)之法律責任

刑事責任

違法蒐集處理或利用敏感性資料

違法蒐集及處理個人資料

違法利用個人資料

違法進行國際傳輸

非法妨害個人資料正確性

非意圖營利：
兩年以下有期徒刑

意圖營利：
五年以下有期徒刑

五年以下有期徒刑

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)

民事責任

最高賠償總額 2 億元

非財產損害得請求賠償相當金額

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。(§28)

非公務機關(私立學校)之法律責任

刑事責任

違法蒐集處理或利用敏感性資料

違法蒐集及處理個人資料

違法利用個人資料

違法進行國際傳輸

非法妨害個人資料正確性

非意圖營利：
兩年以下有期徒刑

意圖營利：
五年以下有期徒刑

五年以下有期徒刑

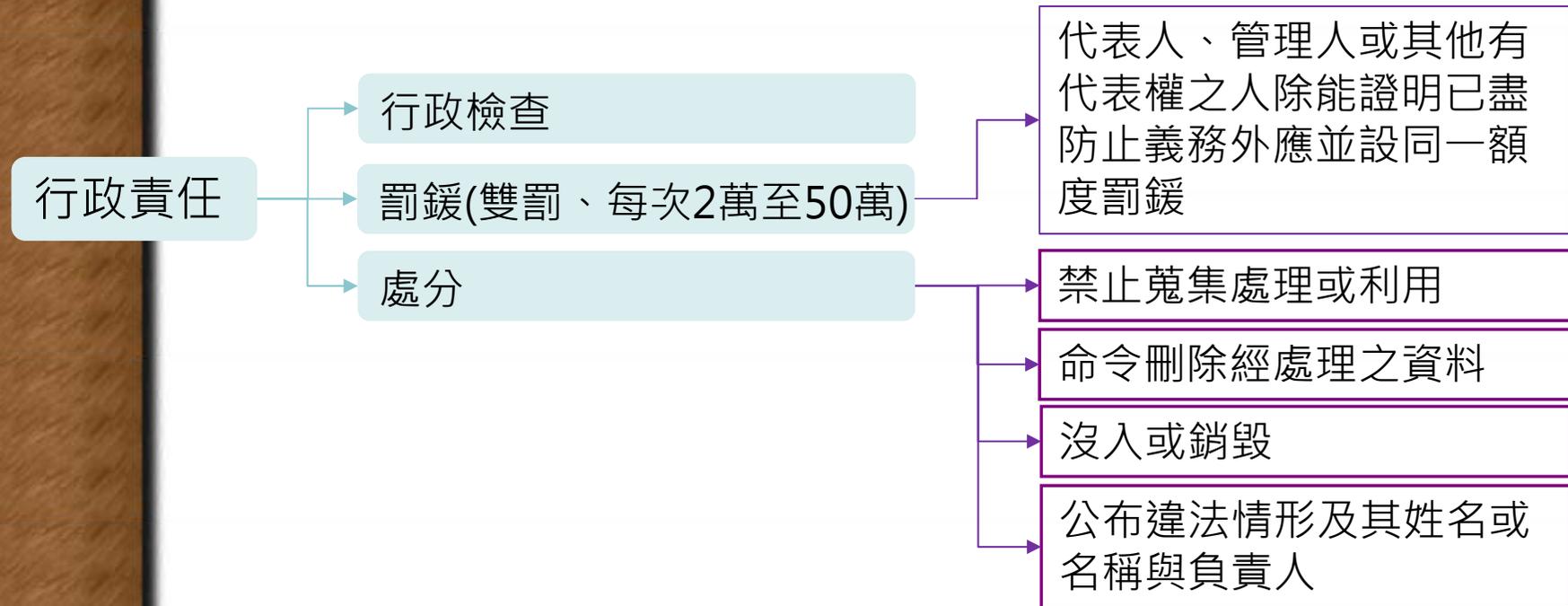
民事責任

最高賠償總額 2 億元

非財產損害得請求賠償相當金額

非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。但能證明其無故意或過失者，不在此限。(§29)

非公務機關(私立學校)之法律責任 (續)



第二階段課程大綱

- 個人資料流之重要性
- 個人資料保護暨實施
- 個人資料生命週期與風險管理

- 個人資料流之重要性
- 個人資料保護暨實施
- 個人資料生命週期與風險管理

個人資料流之重要性

- 個資保護對組織而言是風險管理的議題
 - 個資外洩引起的威脅
 - 調查和訴訟
 - 負面宣傳
 - 運營中斷
 - 計劃外預算
 - 對企業信任產生懷疑。
- 企業/組織在個人資料保護的策略層應建立一個基於風險管理的資料保護策略方法，而非僅依賴周邊的安全。也就是將個人資料的安全保護直接加在資料本身。

個人資料流之重要性

- 前不久爆發的少將洩密案，政府的補救措施
 - 徹底清查洩密案所帶來的損失外
 - 追查資料外洩流向
 - 調查該名少將在任職內還看過哪些檔案
 - 這些機密檔案曾被哪些人閱覽過
 - 是否還潛在著資料外洩的風險
 - 有沒有任何管理流程上的漏洞
- 唯有描繪出完整資料流，才能從中找出缺失及防堵方式，避免日後相同情況再度上演。

個人資料流之重要性

- 發生資料外洩後，第一件要做的就是描繪出完整的資料流向。
 - 瞭解這份檔案日常的使用者、維護者及檔案使用狀況；
 - 清查檔案曾經被哪些員工閱覽過，這些員工又看過哪些其他的檔案；
 - 追查除了外洩檔案外，洩密者還看過哪些檔案。

個人資料流之重要性

- 描述和分析組織目前的業務流程架構，基本上，任何的業務活動都會牽涉到資訊的管理，並且包括四項元素，分別為：資訊蒐集、交易流程、交易結果和以上三者所留下的記錄。

個人資料流之重要性

- 在資料流分析過程中，至少要識別出業務流程主要的元件，如人員、設備及個人資料處理過程使用之相關紙本化表單或自動化方式等，以及個人資料如何透過業務流程被蒐集、處理、利用、揭露和保存，建議以清楚易懂的方式來呈現彼此的關聯(如圖形或簡易的表格方式)。

- 個人資料流之重要性
- 個人資料保護暨實施
- 個人資料生命週期與風險管理

資料蒐集、處理、利用之自我檢查五步驟

步驟一：清點所有個人資料



步驟二：清查蒐集個人資料之途徑與方式



步驟三：確認是否須履行告知義務並建立告知機制



步驟四：確認蒐集、處理、利用之特定目的



步驟五：檢視利用的範圍與方式

取得個人資料的來源

- 直接蒐集

- 由當事人提供

- 間接蒐集

- 自第三人取得

- 經由公開管道取得

個人資料來源-直接蒐集(告知)

告知時點：向當事人蒐集前

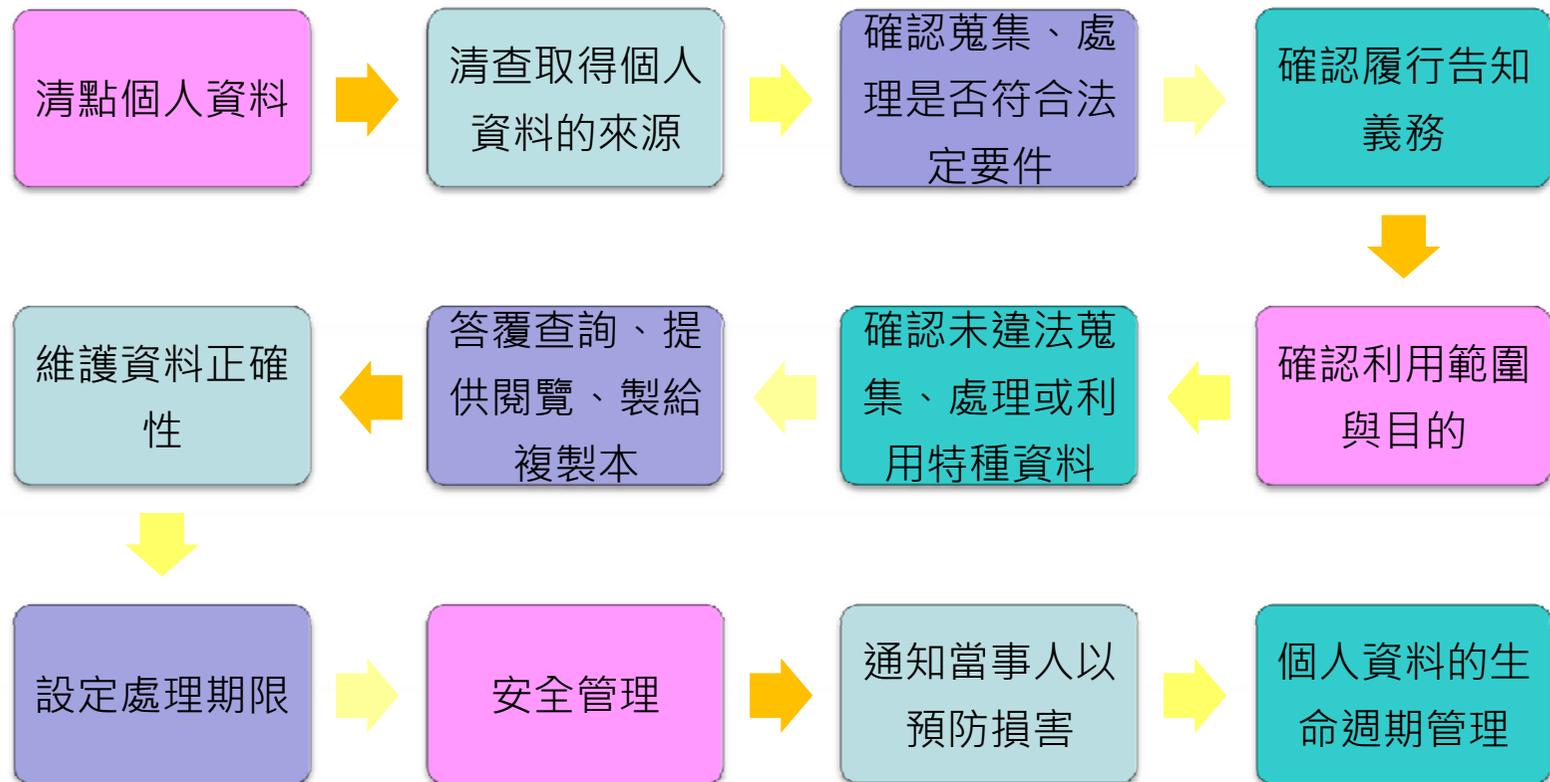
應告知事項	得免為告知之情況
公務機關名稱	依法免告知
蒐集之目的	履行法定義務所必要
個人資料之類別	告知將妨害公務機關執行法定職務
利用之期間、地區、對象及方式	告知將妨害第三人重大利益
當事人得行使之權利	當事人明知應告知內容
當事人得自由選擇提供個人資料時，不提供對其權益之影響	

個人資料來源-間接蒐集(告知)

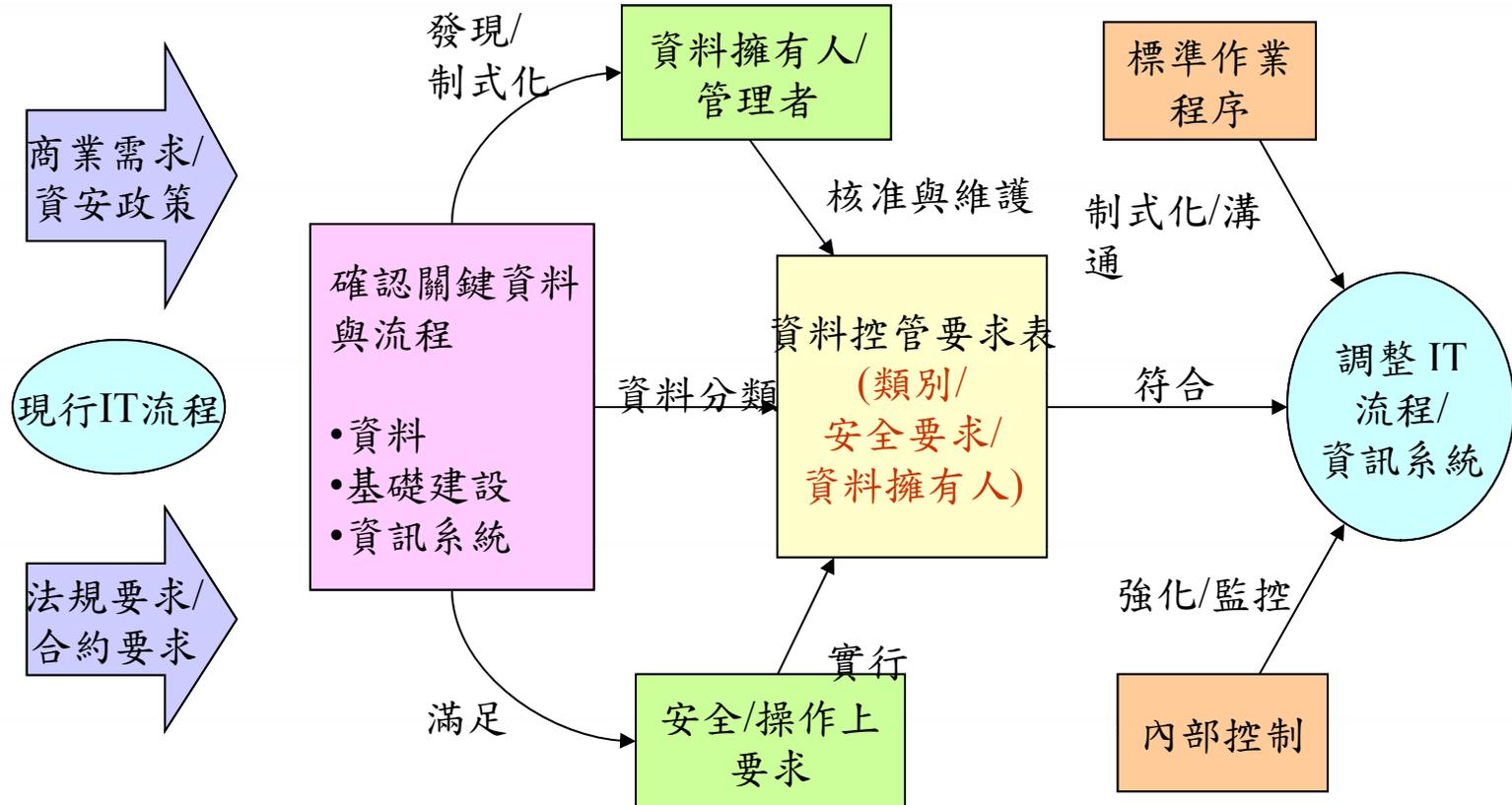
告知時點：處理或利用前

應告知事項	得免為告知之情況
公務機關名稱	依法免告知
蒐集之目的	履行法定義務所必要
個人資料之類別	告知將妨害公務機關執行法定職務
利用之期間、地區、對象及方式	告知將妨害第三人重大利益
當事人得行使之權利	當事人明知應告知內容
	當事人自行公開或其他已合法公開
	學術機構機於公益或學術研究之目的，且資料經處理或無從辨識當事人
	不能向當事人或其法定代理人告知
	大眾傳播業者基於新聞報導之公益目的

個人資料盤點與作業流程識別



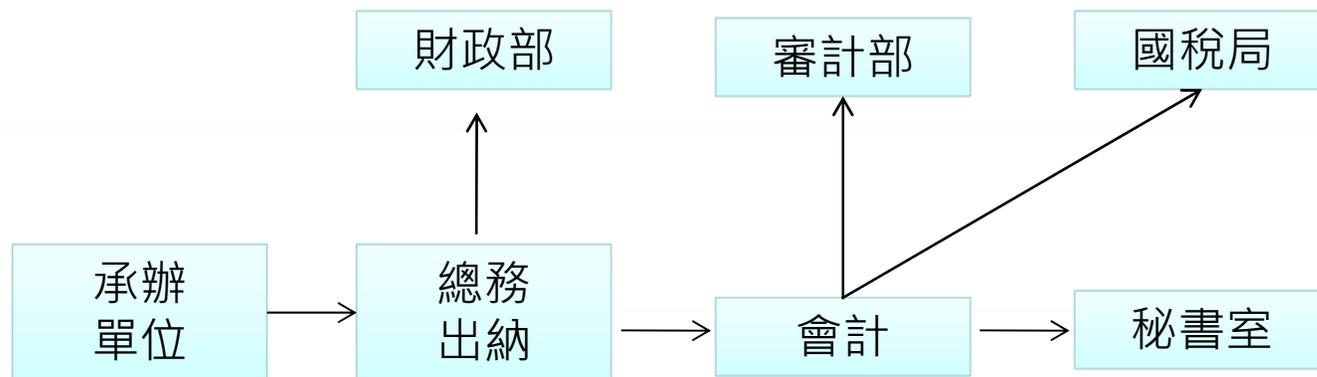
個人資料管理流程圖



By Rafael Etges, CISA, CISSP, And Karen McNeil, NII 整理

個人資料保護作業程序(Example)

- 「邀請專家學者出席會議請領車馬費作業」



- 一個資範圍：姓名、單位、身分證統一編號、戶籍地址、帳號、連絡電話等

個人資料保護暨實施

推動個人資料保護及管理制度

ISMS(Information Security Management System)
PIMS(Personal Information Management System)
More...

實施個人資料管理及保護教育訓練

訓練、訓練、再訓練
宣導、宣導、再宣導

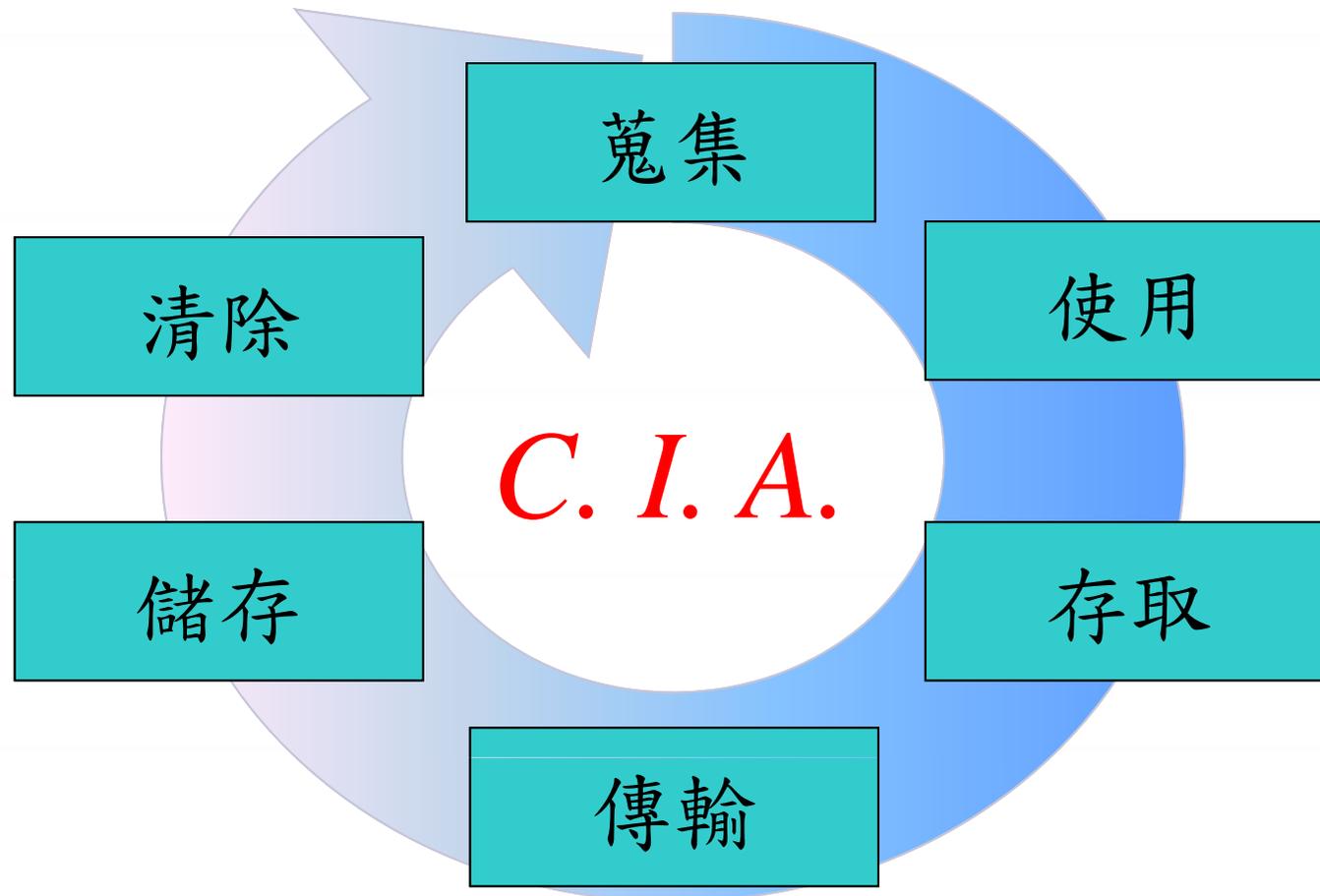
評估可行之個人資料管理
及保護之技術方案

DLP(Data Loss Prevention)
資產管理技術
More...

滿足基本
個人資料保護

- 個人資料流之重要性
- 個人資料保護暨實施
- 個人資料生命週期與風險管理

個人資料生命週期管理(Personal Data Life Management)



個人資料生命週期管理(Personal Data Life Management)

- **蒐集**
 - 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為法律定義之「得以直接或間接方式識別該個人之資料」
- **使用**
 - 符合法律之使用規範
 - 符合組織政策之內部使用規範(例如：交叉行銷)
- **存取**
 - 存取個人資料之權限管理
 - 委外或外包廠商之資訊安全管理

個人資料生命週期管理(Personal Data Life Management)

- **傳輸**
 - 個人資料傳輸過程中之安全(加密或安全網路)
- **儲存**
 - 個人資料新增及修改之作業程序
 - 存放個人資料場所及設備之安全管理
 - 備份或歸檔後之資料安全
- **清除**
 - 個人資料刪除或銷毀之安全處理程序
- **其它**
 - 客訴、法律糾紛、懲處程序

與個資法相關的資安管理機制

	ISO27001	BS10012	JISQ15001:2006
優點	<ol style="list-style-type: none"> 1.國際ISO標準 2.國家CNS標準 3.國內熟習機制 4.人才與經驗足 5.法務部接受 	<ol style="list-style-type: none"> 1.專門個資標準 2.英國國家標準 3.已推廣年多 	<ol style="list-style-type: none"> 1.專門個資標準 2.日本國家標準 3.日本案例豐富 4.台日交流數年
缺點	<ol style="list-style-type: none"> 1.資料收集缺 2.殺雞用牛刀？ 	<ol style="list-style-type: none"> 1.沒有經驗案例 2.無國際認證書 3.人才經驗缺乏 4.與英國法律緊密結合 	<ol style="list-style-type: none"> 1.只有日本使用 2.目前國內還無 3.無法取得認證 4.與日本法律緊密結合

個人資料業務流程分析

- 流程確認目的
 - 瞭解同仁本身個資相關業務處理方式，及所使用之相關資訊(如紙本(電子)表單或系統等)。
- 參考適用之法令、法規或主管機關要求，可鑑別現行作業是否符合要求。

個人資料業務流程分析

- 作業訪談內容範例，識別流程名稱

流程名稱	檔案名稱	資料形式	法律依據	特定目的	揭露			現有控制
					對象	方式目的	個資範圍	
教育訓練報名作業	研討會 廣宣名 單	DA	合約	053 教育或訓練行政	無	無	無	本機 帳密 保護

個人資料業務流程分析

- 重點說明單位目前個資處理方式

蒐集		處理		利用			保存		銷毀		揭露		現有控制			
來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率		對象	方式目的	個資範圍
寄送報名表請與會人員填寫資料	<input checked="" type="checkbox"/> 直接 <input type="checkbox"/> 間接	X X組	本機作業 Excel表	X X組	無	台灣	X X組	報名通訊聯繫	X X組 XXXX-XXXX # XXX	教育訓練執行期間	無	無	無	無	無	本機帳密保護

個人資料業務流程分析

- 重點說明單位目前個資利用與保存方式

蒐集			處理		利用				保存		銷毀		揭露		現有控制	
來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象	方式目的		個資範圍
寄送報名表請與會人員填寫資料	<input checked="" type="checkbox"/> 直接 <input type="checkbox"/> 間接	X X組	本機作業 Excel表	X X組	無	台灣	X X組	報名通訊聯繫	X X組 XXXX-XXXX # XXX	教育訓練執行期間	無	無	無	無	無	本機帳密保護

個人資料業務流程分析

- 重點說明單位目前個資銷毀方式

蒐集			處理		利用			保存		銷毀		揭露		現有控制		
來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象		方式目的	個資範圍
寄送報名表請與會人員填寫資料	<input checked="" type="checkbox"/> 直接 <input type="checkbox"/> 間接	X X組	本機作業 Excel表	X X組	無	台灣	X X組	報名通訊聯繫	X X組 XXXX-XXXX # XXX	教育訓練執行期間	無	無	無	無	無	本機帳密保護

個人資料業務流程分析

- 作業訪談所得資料彙整於個人資料清冊：

單位	流程	個資檔案	格式	個人資料流				
				蒐集	處理	利用	儲存與銷毀	揭露
業務單位	員工聯絡資料維護作業	員工聯絡資料名冊	DA	業務單位	業務單位	業務單位	業務單位	無
總務	採購作業	採購案契約書數份	DA	業務單位	業務單位	總務	總務	無
會計	付款作業	憑證用紙 (出差費、 講師鐘點費)	DC	會計	會計	會計	會計	查帳 主管 機關

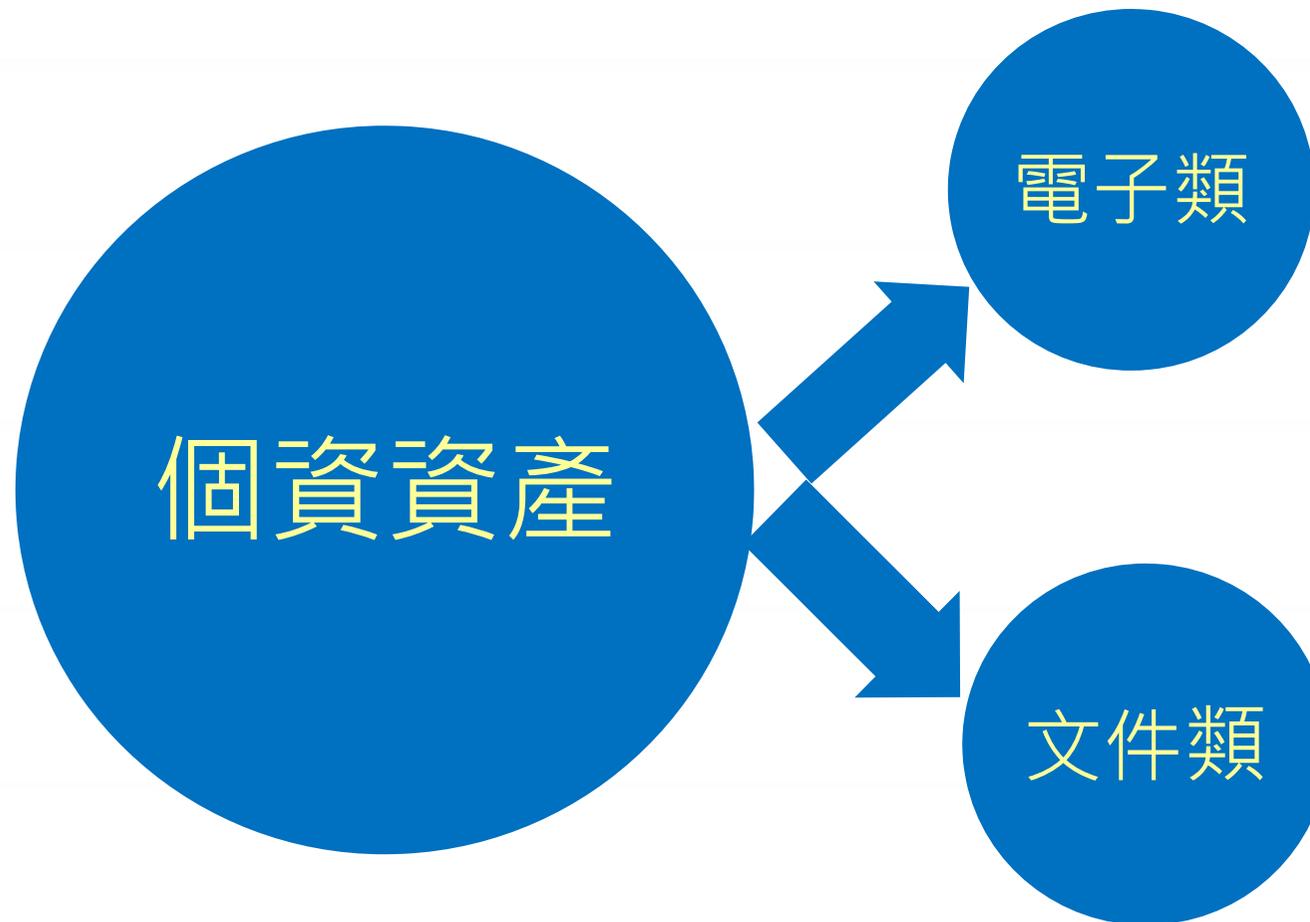
個人資料檔案清冊(範例)

編號 項目	個人資料 檔案名稱	保有依據	特定目的	個人資料識別	保管單位
1	公教人員履歷資料(含公教人員基本資料、現職學歷、考試、訓練家屬、經歷、考績獎懲、銓審等人事資料)	人事管理條例、行政院暨所屬各機關人事行政資訊化統一發展要點、行政院及所屬各機關人事資料統一管理要點。	002人事行政管理	C001辨識個人者、C003政府、C021家庭情形、C023家庭其他成員之細節、社會情況(C031住家及設施、C038職業、C039執照或其他許可)、教育、技術或其他專業(C051學校紀錄、C052資格或技術C054職業專長)、受僱情形(C061現行之受僱情形、C062僱用經過、C063離職經過、C064工作經驗、C065工作紀錄、C068薪資與預扣款、C071工作之評估細節、C072受訓紀錄)	人事室
2	教職員工聯絡資訊	行政院及所屬機關人事資料統一管理要點	002人事行政管理	C001識別個人者；受僱情形	人事室
3	待遇資料	全國軍公教員工待遇支給要點、公立學校教職員敘薪辦法、勞動基準法及其施行細則、各機關學校聘僱人員離職儲金給與辦法	002人事行政管理	C061現行之受僱情形	人事室

個人資料檔案清冊(範例)

編號 項目	個人資料 檔案名稱	保有依據	特定目的	個人資料識別	保管單位
10	大雄國小 學生基本 資料	臺北市國民中小學 學生學籍管理辦法	079學生資料管 理	COO1辨識個人者、C003政府資料中之 辨識者、C011個人描述、C057學生紀 錄	訓導處 生教組
11	志工保險 名冊	臺北市國民小學交通導護 志工隊設置要點	096其他地方 政府業務	COO1辨識個人者、C003政府資料中之 辨識者、C011個人描述、C052資格或 技術	訓導處 生教組
12	環境教育 教職員名 冊	環境教育法施行細則第10 條	087環境保護	C001辨識個人者、C003政府資料中之 辨識者、C062僱用經過、C088保險細 節	訓導處 衛生組
13	清寒學生 午餐 補助名冊	臺北市政府教育局安心就 學溫馨輔導計畫	040政府福利金 或救濟金給付 行政	C001辨識個人者、C002辨識財務者、 C003政府資料中之辨識者、C011個人 描述	午餐中心
14	國小學生 健康資訊 系統web版	學校衛生法第九條	089保健服務	C001辨識個人者、C003政府資料中之 辨識者、C011個人描述、C012身體描 述、C111健康紀錄	健康中心
15	國小學生 健康檢查 記錄卡	學校衛生法第九條	089保健服務	C001辨識個人者、C003政府資料中之 辨識者、C011個人描述、C012身體描 述、C111健康紀錄	健康中心
16	國小學生 體適能成 績資料檔	學校衛生法施行細則	089保健服務	C001辨識個人者、C003政府資料中之 辨識者、C011個人描述、C012身體描 述、C111健康紀錄	訓導處 體育組

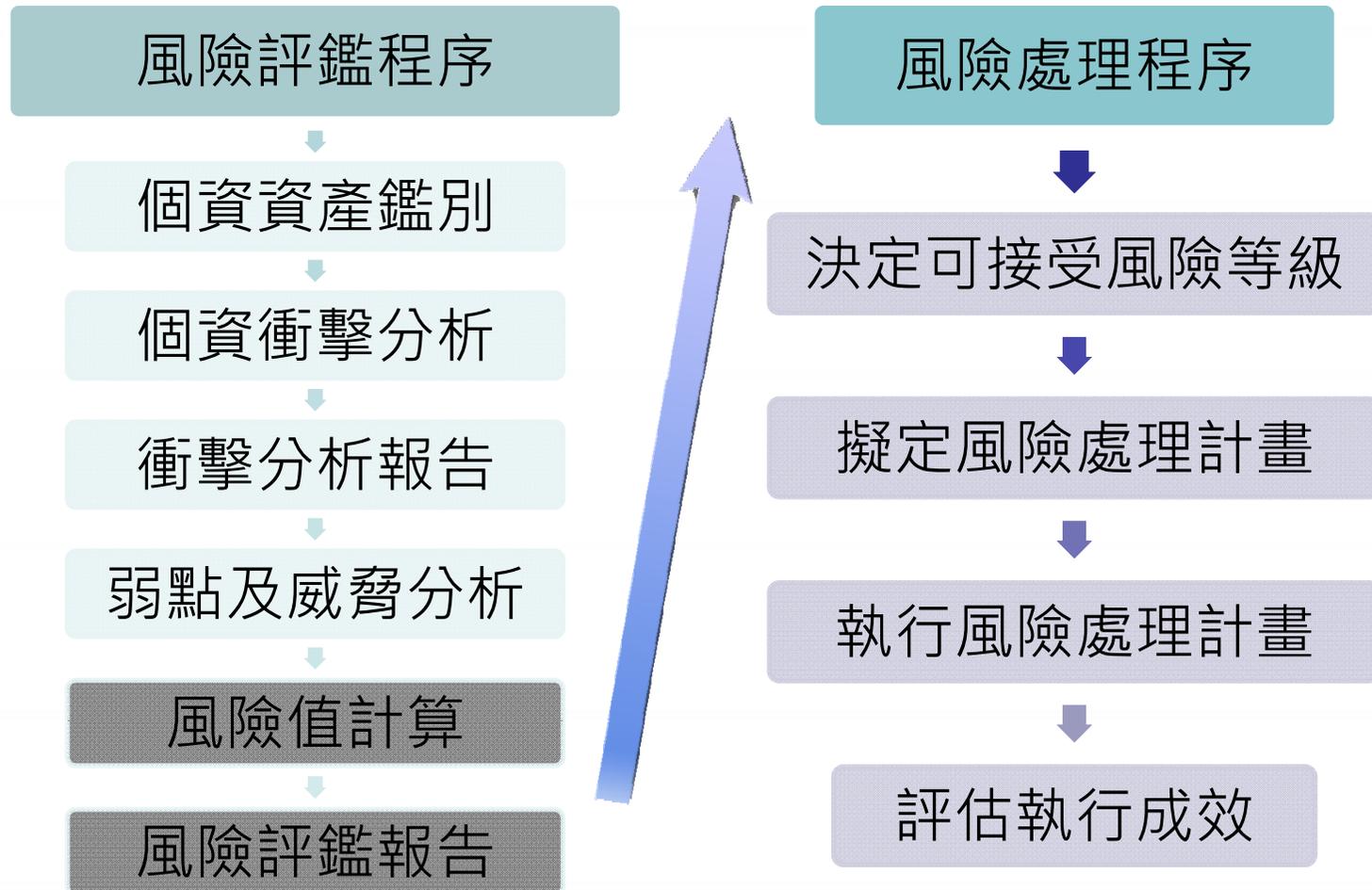
個人資訊資產分類



個人資訊資產分類

- 電子 (Data)
 - 儲存於硬碟、磁帶、光碟、唯讀記憶體等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔。
- 文件 (Document)
 - 以紙本形式存在之文書資料，包含公文、報表、表單、計畫書、合約、外來文件等。

個人資料風險管理程序



個人資料盤點

- 個資盤點是管理制度中相當重要的作業，唯有全面性進行清查，才能了解相對應之風險，並施以適切的控制措施。
- 根據法規要求個資之定義，重新檢視所有已蒐集之資訊。
- 鑑別出所有與個人資料相關之營運流程。
- 針對各個流程細項了解其流程架構。
 - 各個活動執行時，資料輸入輸出之說明。
 - 資料流向。

第三階段課程大綱

- 案例分析與討論
- 個人資料保護，我們可以做甚麼
- 結語

- 案例分析與討論
- 個人資料保護，我們可以做甚麼
- 結語

校務行政相關的個人資料

- 學生學籍資料
- 學生申請補助資料
- 學生清寒家庭身分
- 學生成績資料
- 學生獎懲及違規紀錄
- 學生家庭狀況
- 保健室病歷紀錄
- 學生家長或緊急連絡人聯絡方式
- 教職員健康檢查資料
- 教職員人事資料
- 教職員出缺勤紀錄
- 教職員通訊錄
- 畢業校友資料
- 畢業紀念冊
- 圖書館借還書記錄

案例 1

新生訓練是否為恰當時機讓學生知道學校可能利用其個人資料的狀況，學校也可一併在新生訓練或註冊時取得其同意授權？

No!

除非學校使用個人資料有可能超過教育行政之特定目的，否則是不需要學生額外授權的。

但因為新法增加了「告知」的義務，因此在學生入學時應立刻履行告知義務，詳述學校使用個人資料之範圍用途等。

More

如果學校對於學生的個人資料有逾越特定目的之利用，應及早告知學生並取得其「書面同意」。

案例 2

學生畢業後是否仍可寄發活動通知？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如何管理才符合個資法？

Yes!

學校使用校友個人資料還須符合「教育行政」之特定目的，若超過特定目的則不能使用，可能需要在畢業前取得學生授權。

More

一般人並不會反對辦校友活動會超過特定目的，但學校應與教育部、法務部溝通，確保學校能繼續使用校友資料。

此外，學校應建立控管機制避免校友資料外洩。

案例 3

學校是否可寄發與銀行合作發行的校園認同卡相關資料給校友？

No!

學校當初蒐集校友個人資料之特定目的為教育或訓練行政，或學生資料管理。學校寄發認同卡相關資料給校友，構成利用校友個人資料之行為，似已逾越上述特定目的，除非取得校友之書面同意，否則不得為之。

案例 4

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？

Yes!

畢業紀念冊上的學生資料是屬於個人資料。

More

過去畢業紀念冊的收集與公開並非違法行為，但因為現在有越來越多的販賣個人資料或詐騙個人資料之行為，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 5

老師擔心學生最近可能因閱讀某些讀物而造成行為偏差，所以向圖書館調閱學生的借書紀錄，請問圖書館是否可以提供？

借書紀錄含學生姓名、社會活動或其他得以識別學生之資料，此屬於個人資料之範疇。

圖書館保存借書紀錄之目的為「學生資料管理」，並不具評估學生行為偏差與否之目的。

No!

老師向圖書館調閱學生借書紀錄，固然可認為是學校內部「教育或訓練行政」目的，但仍應於該目的之必要範圍內為之，並應尊重當事人權益。

如有證據可合理懷疑某學生偏差行為與閱讀有相當關聯，老師為進一步確認而向圖書館調閱學生借書紀錄，或可被認為符合「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，全面調取學生借書紀錄，恐被認為逾越「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 6

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？

Yes!

民法規定，滿20歲為成年。未成年人包括：

- 1) 未滿7歲者，為無行為能力人：應由法定代理人代為意思表示，並代受意思表示。
- 2) 滿7歲以上者，為限制行為能力人：其為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，未成年人為書面同意，應由法定代理人代為書面同意，或得到法定代理人之允許。

More

民法規定，已經結婚之未成年人，有行為能力。換言之，已經結婚之未成年人，可以自行為書面同意，並無法定代理人代為書面同意或允許之問題。

案例 7

學校公布欄上公告曠課學生名單（學生姓名、學號）有違反個資法嗎？

No!

有關獎懲應符合學校辦理教育行政之目的，公布並不違反個資法，但須注意公布學生名單時，應僅揭露必要之個資。

案例 8

若當事人自行公開其特種個人資料，是否可以蒐集與傳播？

No!

已公開的特種個資雖然可以蒐集，但蒐集及利用仍須依個資法之特定目的範圍，也不能任意傳播。

案例 9

2008年承攬國中基測電腦閱卷、計分的業者因販售學生個人資料給補教業牟利，檢方將主要負責人共3名依背信罪及違反電腦處理個人資料保護法聲押。業者販賣給補習班的個資以光碟存放，每份售價23或35萬元，價格依地區有所不同。

Q. 蒐集與利用個資的相關業務是委外給廠商執行，若個資有外洩漏事件，應該由委外廠商負責。不是嗎？



根據個資法第4條，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。因此，雖然是外包公司洩漏個資，但是國中基測的負責單位也須負責任的。

案例 9-1

2008年承攬國中基測電腦閱卷、計分的業者因販售學生個人資料給補教業牟利，檢方將主要負責人共3名依背信罪及違反電腦處理個人資料保護法聲押。業者販賣給補習班的個資以光碟存放，每份售價23或35萬元，價格依地區有所不同。

那我要如何控制別人的公司不會外洩這些個人資料呢？



委外廠商篩選須謹慎，特別是委外蒐集與處理個資的廠商；建議應該對委外廠商的個人資料安全管理有相當的要求與管控，並應在契約條款轉嫁相關的風險。

案例 10

考績表有公司（或機關）名稱與姓名、分數等，算個人資料嗎？

Yes!

考績表是公司（或機關）內部使用，除非當事人找工作時，對方要求他將提供前一公司（或機關）相關資料，當事人可以要求過去公司（或機關）提供他過去公司考績（或者成績單），當然是當事人要求的揭露。沒有當事人的要求，我們當然沒有權利把我們手上他過去的考績或成績單提供給第三方。

案例 11

教授要求助理、行政人員或電算中心提供學生資料，在何種情形下可以提供？

Yes!
Or
No

老師因為教學所需（如與學生聯繫科業有關事項、瞭解學生家庭背景與能力等），可能會需要學生的個人資料。學校負責保管資料的人員須判斷老師索取學生資料之目的，是否逾越教學必要範圍，以判斷是否提供？
建立個人資料調閱的申請與審核機制。

案例 12

推廣中心是否可以利用報名學校的甄/筆試的考生資料，寄給落榜生推廣學分班之招生資料？

No

學校當初蒐集考生個人資料之特定目的為學生資料管理，並非行銷推廣中心之課程。推廣中心將招生資料寄給落榜生，構成利用考生個人資料之行為，逾越學生資料管理之特定目的，除非取得考生之書面同意，否則不得為之。

- 案例分析與討論
- 個人資料保護，我們可以做甚麼
- 結語

個資保護，你可以做什麼？

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，你可以做什麼？(續)

建立
程序

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

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為。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，你可以做什麼？(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，你可以做什麼？(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。

- 案例分析與討論
- 個人資料保護，我們可以做甚麼
- 結語

結語 - 給學校的建議

- 檢視法務部現有的電腦處理個人資料保護法之特定目的是否充分且符合校務推動之需求，適時向縣市教育處或其他主管機關(如教育部)提出修正或增修之建議。
- 開始進行個人資料盤點工作，瞭解學校擁有的個人資料種類、數量、保存與利用情形，以為後續風險評估與建議安全管控措施之基礎。
- 設置專人負責規劃個人資料保護相關事宜。

簡報完畢，敬請指教

