個人資料保護法衝擊與因應

2013.02.27/2013.03.06
王俊凱 協理
NII 產業發展協進會

個人資料，無所不在

電信/網路
服務提供業者

帳單地址
電子郵件信箱
帳戶資料

開立帳戶資料
保單資料
貸款徵信資料
會員資料
周年慶抽獎券

銀行/證券/保險公司
百貨公司/大賣場

信用卡資料
客戶資料
宅配地址
教育程度

學籍資料
人事資料
註冊/報名資料
家長會聯絡

線上購物/ 網拍
社群網站

身分證號碼
結婚登記
報稅資料
駕照申請/換發

監理/ 戶政
財稅等政府單位

健檢報告
病歷資料
診斷書

醫院 / 診所
健康檢查中心

學校 / 補習班
社區活動中心

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」。

暫緩實施的第六條與第五十四條條文

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:

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。

個資法第五十四條:

本法修正施行前非由當事人提供之個人資料，依第九條規定應於處理或利用前向當事人為告知者，應自本法修正施行之日起一年內完成告知，逾期未告知而處理或利用者，以違反第九條規定論處。

如何降低個資法之風險？

1. §18 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。

2. §28 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力者，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。

3. §29 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。

4. §50 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定（§47,48,49縣市政府及目的事業主管機關）受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

5. §31 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。

6. 施行細則第十二條第二項說明「落實安全維護措施」有十一項。

5

施行細則第十二條第二項的來源

1. **法務部施行細則第十二條說明了「適當安全防護措施」，基本上就是英國BS10012的做法。為了避免違反個資法，透過機制來建立防護措施，不是為驗證而已。（過去ISO27001只集中於資訊部門）**
2. 個資法第2條第2款：「個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。」：個資盤點不能只在資訊部門（資訊部門可以協助確認），因為個資法客體含「各種形式含個資的檔案（如紙張等）」
3. 盤點個資時應注意個資生命週期（蒐集、處理、利用、傳輸、銷毀）的關聯性：各階段的合法性，必須回到蒐集時的特定目的與範圍。「蒐集合法」，不表示其他階段合法。

6

施行細則第十二條說明

措施1：配置管理之人員及相當資源

企業必須指派一位人員出任個資管理代表，也就是專門處理個資相關事項的專員。另外，依據執行時的需要，企業必須提供相關的經費、人力等資源，來協助管理人員實施各項管理程序。

措施2：界定個人資料之範圍

也就是所謂的個資盤點，目的是要找出企業內部所有的個人資料。企業可依據個資的資料流來設計盤點表，讓各部門逐一清查，找出各部門中存放個資的載體，例如可能儲存個資的文件、手冊或系統等。

措施3：個人資料之風險評估及管理機制

企業可進行風險評鑑或是隱私權衝擊分析，從這兩項作業中了解資產的價值、可能遭遇的風險以及有哪些較為敏感的個資。

措施4：事故之預防、通報及應變機制

企業應建立起事故應變的通報程序，也就是發生了事故後，該通知誰，該如何處理，都要有相對應的方法。此外，要從發生的事故中找出對應的預防措施。

措施5：個人資料蒐集、處理及利用之內部管理程序

企業要制定出一套合法的業務流程，對於蒐集、處理及利用這三項有明確的流程規範，並將其制定成程序書，以便員工查閱。

措施6：資料安全管理以及人員管理

企業要將資料分級，並依據不同職位的員工設定存取權限，而存放資料的位置，要採取防護措施，像是資料加密、防火牆、入侵偵測系統等等。

措施7：認知宣導及教育訓練

企業應定期對全體員工舉辦教育訓練，內容包括法令宣導、內部規範宣導等等。而且企業必須要保存這些教育訓練或認知宣導的實施記錄，作為未來證明自己的確有善盡良善管理之責的證明。

措施8：設備安全管理

針對各式各樣的設備，如：USB、隨身硬碟、行動裝置等，要有明確的使用規範，才不會因為使用這些載具而造成個資外洩。

措施9：資料安全稽核機制

企業可聘請專業顧問公司定期稽核個資保護的流程，或是舉辦內部稽核活動，可以從報告中找出缺失或潛在的問題。

措施10：使用紀錄、軌跡資料及證據保存

經由各項程序所產生的任何形式記錄，企業皆需妥善保存，以利日後舉證之用。依個資法的規範，發生個資損害事件後的5年內都可求償，這也意味著企業相關個資記錄至少要保存5年。

措施11：個人資料安全維護之整體持續改善

企業的管理高層應該定期開會，或是有重大事故時召開會議，評估個資保護制度落實的程度，並持續改善。同樣的，這些改善會議或企業個資保護措施的改善作為也都需要記錄。

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

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

手機號碼、住家電話、聯絡地址等

薪資、帳戶、資金來源…

原則不得蒐集、處理或利用

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

特種個資內容（已被暫緩實施）

- 特種個人資料，包括醫療、基因、性生活、健康檢查、犯罪前科
  - 特種個人資料除個資法第 6 條（目前凍結）所定情形外，不得蒐集、處理或利用。

類別	內容（施行細則§4）
醫療	指包含病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。
基因	由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。
性生活	指性取向或性慣行之個人資料 。
健康檢查	指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料 。
犯罪前科	指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄 。

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

個資法基本認知

一.個人資料法緣由

二.個人資料法立法目的

三.個人資料法進展

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

資料參考來源：資策會

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.

14

經濟合作暨發展組織 (OECD)

- 個人資料保護8大原則

限制蒐集原則	經本人同意，以合法、公正手段於適當場所蒐集.
品質確保原則	符合資料使用之目的，並確保資料之正確性、完整性和時效性.
目的明確原則	進行蒐集的目的必須在蒐集的當時就闡述明確，爾後使用也必須受限於當初所訂目的，不得他用.
限制目的外使用原則	非經本人同意不得作蒐集目的外利用.
安全確保原則	資料必須採取合理安全保護措施，以免資料遭遺失、盜用、毀損、竄改或揭露的風險.
公開原則	對個人資料之開發、運用、政策等必須採取一般的公開政策.
個人參與原則	確認資料存在、資料內容、請求刪除或更正.
責任明確原則	資料管理者必須確保落實組織政策與執行措施以遵守上述各項原則.

15

新法修正重點

- 擴大適用主體：
  - 舊法：公務機關與非公務機關（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）
  - 現行法：打破行業別限制，包含各行各業及個人
- 擴大保護客體：
  - 舊法：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
  - 現行法　：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

“個人資料保護法”
與
” 電腦處理個人資料管理辦法 “

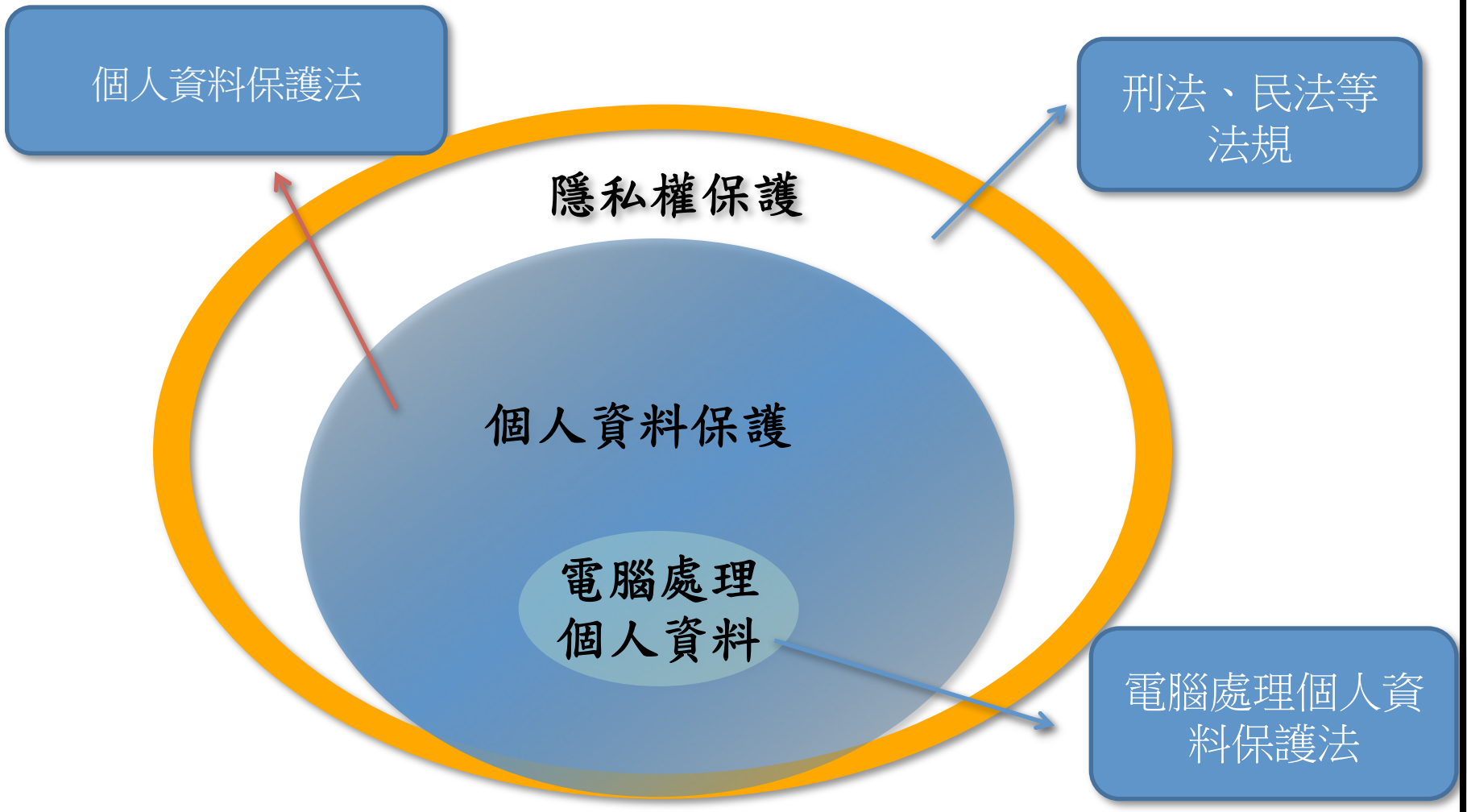
- 電腦處理個人資料保護法：84年8月11日制定公佈。
- 個人資料保護法：99年5月26日修正公佈。
  - 99年5月26日總統公佈日起，廢止許可登記制度。
  - 100年11月25日的目標已經展延
  - 101年9月26日公佈施行細則
  - 個資法終於在101年10月1日宣佈實施

個人資料保護法之立法目的

避免人格權侵害

促進個人資料合理利用

隱私權與個人資料保護？



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

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

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）

第五章　罰則（10）

第六章　附則（6）

個人資料保護法的適用於個人嗎?

個資法適用對象

- 包括各行各業及個人 (§2)
- 受委託蒐集、處理或利用個人資料者，視同委託機關 (§4)

個資法保護客體

- 以任何方式（包括紙本）留存的資料
- 任何方式取得個人資料 (§2)
- 生存之特定或得特定之自然人

公務與非公務之定義：

§2&7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。
§2&8非公務機關：指前款以外之自然人、法人或其他團體。

資料蒐集、處理或利用與特定目的之關聯：

§5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

教育部來函轉知

公立學校如係各級政府依法令設置實施教育之機構，而具有機關之地位，應屬個資法之公務機關。非由各級政府設置之私立學校，則屬本法之非公務機關。

26

直接蒐集個人資料的告知義務（§8）

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（§9）

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。

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

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

特定目的之內(§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
8	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	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。
7	經當事人書面同意：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。

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) 。

個資法規定的安全保護相關規定有哪些?

個資法施行細則§12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	成立管理織人員及相當資源
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	使用紀錄、軌跡資料及證據保存
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。

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

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)

個人資料保護法之特定目的

民國 101 年 10 月 01 日公告生效　（共182項）

人身保險	文化行政
人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）	文化資產管理
入出國及移民	水利、農田水利行政
土地行政	火災預防與控制、消防行政
工程技術服務業之管理	代理與仲介業務
工業行政	外交及領事事務
不動產服務	外匯業務
中小企業及其他產業之輔導	民政
中央銀行監理業務	民意調查
公立與私立慈善機構管理	犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務
公共造產業務	生態保育
公共衛生或傳染病防治	立法或立法諮詢
公共關係	交通及公共建設行政
公職人員財產申報、利益衝突迴避及政治獻金業務	公民營（辦）交通運輸、公共運輸及公共建設
戶政	仲裁

個人資料保護法之特定目的(續)

全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險	兩岸暨港澳事務
刑案資料管理	券幣行政
多層次傳銷經營	宗教、非營利組織業務
多層次傳銷監管	放射性物料管理
存款保險	林業、農業、動植物防疫檢疫、農村再生及土石流防災管理
存款與匯款	**法人或團體對股東、會員（含股東、會員指派之代表）、董事、監察人、理事、監事或其他成員名冊之內部管理**
有價證券與有價證券持有人登記	法制行政
行政執行	法律服務
行政裁罰、行政調查	法院執行業務
行銷（包含金控共同行銷業務）	法院審判業務
住宅行政	社會行政
兵役、替代役行政	**社會服務或社會工作**
志工管理	金融服務業依法令規定及金融監理需要，所為之蒐集處理及利用
投資管理	金融爭議處理
災害防救行政	金融監督、管理與檢查
供水與排水服務	青年發展行政

個人資料保護法之特定目的(續)

非公務機關依法定義務所進行個人資料之蒐集處理及利用	借款戶與存款戶存借作業綜合管理
保健醫療服務	原住民行政
保險經紀、代理、公證業務	捐供血服務
保險監理	旅外國人急難救助
信用卡、現金卡、轉帳卡或電子票證業務	核子事故應變
信託業務	核能安全管理
契約、類似契約或其他法律關係事務	核貸與授信業務
客家行政	海洋行政
建築管理、都市更新、國民住宅事務	消費者、客戶管理與服務
政令宣導	消費者保護
政府資訊公開、檔案管理及應用	畜牧行政
政府福利金或救濟金給付行政	財產保險
科技行政	財產管理
科學工業園區、農業科技園區、文化創業園區、生物科技園區或其他園區管理行政	**財稅行政**
訂位、住宿登記與購票業務	退除役官兵輔導管理及其眷屬服務照顧
計畫、管制考核與其他研考管理	退撫基金或退休金管理
飛航事故調查	商業與技術資訊
食品、藥政管理	國內外交流業務
個人資料之合法交易業務	借款戶與存款戶存借作業綜合管理

個人資料保護法之特定目的(續)

國家安全行政、安全查核、反情報調查	發照與登記
國家經濟發展業務	稅務行政
國家賠償行政	華僑資料管理
專門職業及技術人員之管理、懲戒與救濟	訴願及行政救濟
帳務管理及債權交易業務	貿易推廣及管理
彩券業務	鄉鎮市調解
授信業務	傳播行政與管理
採購與供應管理	債權整貼現及收買業務
救護車服務	募款（包含公益勸募）
教育或訓練行政	廉政行政
產學合作	**會計與相關服務**
票券業務	會議管理
票據交換業務	經營郵政業務郵政儲匯保險業務
陳情、請願、檢舉案件處理	經營傳播業務
勞工行政	經營電信業務與電信加值網路業務
博物館、美術館、紀念館或其他公、私營造物業務	試務、銓敘、保訓行政
場所進出安全管理	**資（通）訊服務**
就業安置、規劃與管理	**資（通）訊與資料庫管理**
智慧財產權、光碟管理及其他相關行政	**資通安全與管理**

個人資料保護法之特定目的(續)

農產品交易	衛生行政
農產品推廣資訊	**調查、統計與研究分析**
農糧行政	**學生（員）（含畢、結業生）資料管理**
遊說業務行政	**學術研究**
運動、競技活動	憑證業務管理
運動休閒業務	輻射防護
電信及傳播監理	選民服務管理
僱用與服務管理	選舉、罷免及公民投票行政
圖書館、出版品管理	營建業之行政管理
漁業行政	環境保護
網路購物及其他電子商務服務	證券、期貨、證券投資信託及顧問相關業務
蒙藏行政	警政
輔助性與後勤支援管理	護照、簽證及文件證明處理
審計、監察調查及其他監察業務	體育行政
廣告或商業行為管理	觀光行政、觀光旅館業、旅館業、旅行業、觀光遊樂業及民宿經營管理業務
影視、音樂與媒體管理	其他中央政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
徵信	其他公共部門（包括行政法人、政府捐助財團法人及其他公法人）執行相關業務
標準、檢驗、度量衡行政	其他公務機關對目的事業之監督管理

個人資料保護法之特定目的(續)

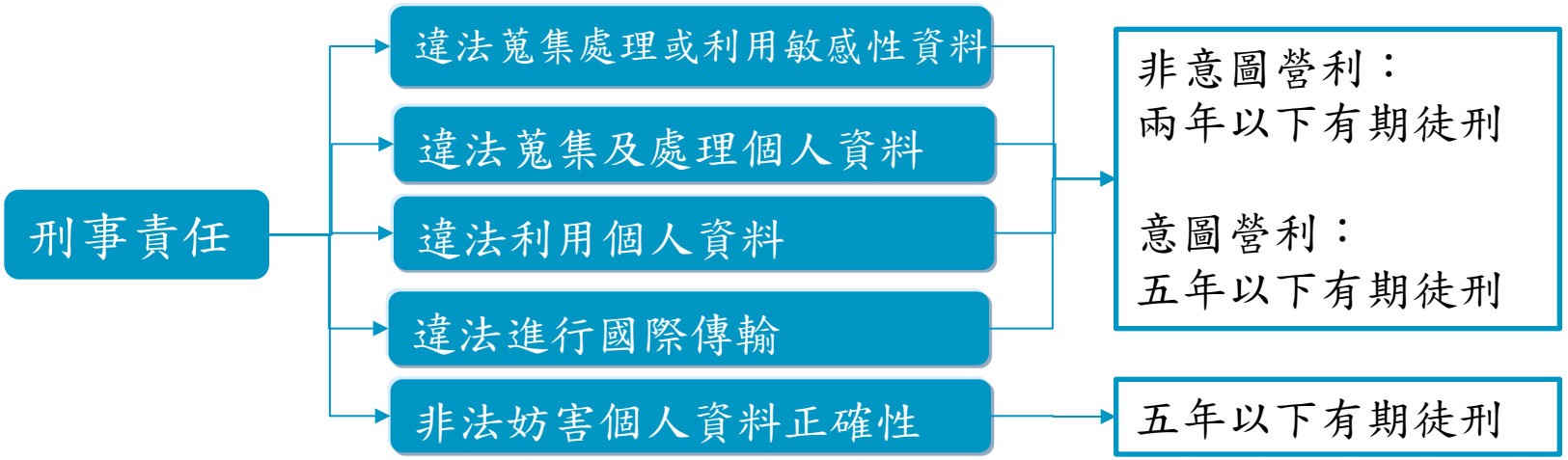
其他司法行政
其他地方政府機關暨所屬機關構內部單位管理、公共事務監督、行政協助及相關業務
其他自然人基於正當性目的所進行個人資料之蒐集處理及利用
其他金融管理業務
其他財政收入
其他財政服務
其他經營公共事業（例如：自來水、瓦斯等）業務
其他經營合於營業登記項目或組織章程所定之業務
其他諮詢與顧問服務

資料違法外洩時，一定要和當事人說嗎?

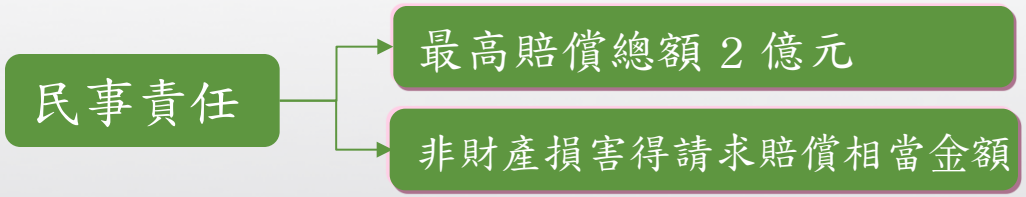
- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。(§12)

若違反個資法，只要罰錢就可以了嗎?

公務機關之法律責任

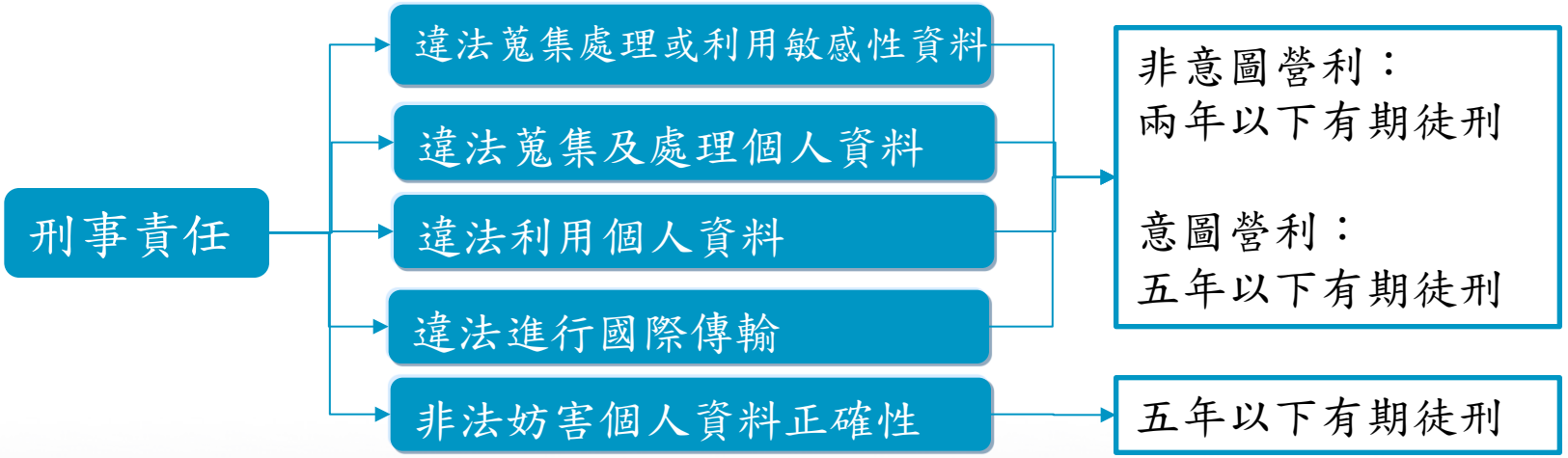


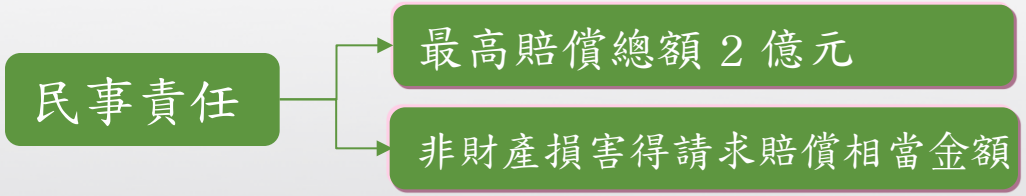
公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)



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份。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。。。(§28)

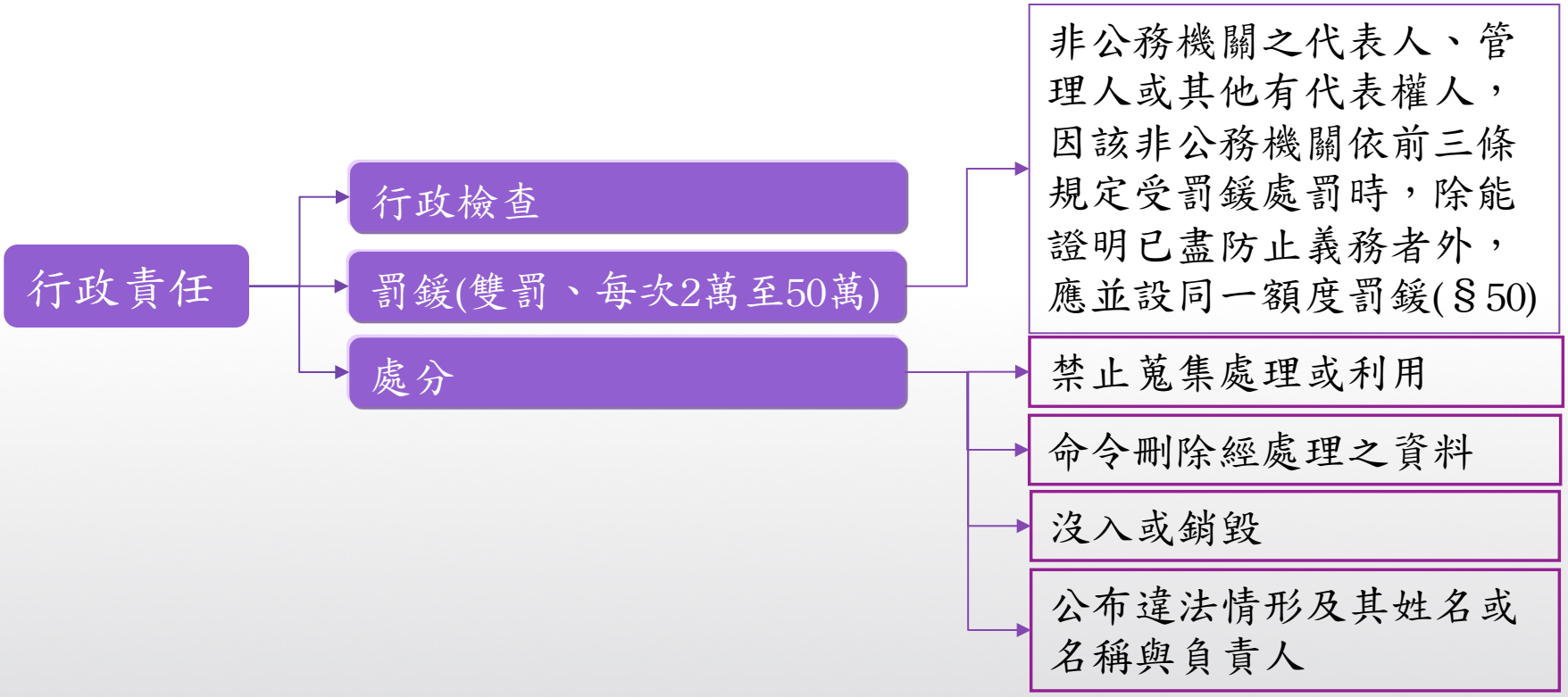
非公務機關之法律責任





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)

非公務機關之法律責任 (續)



簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

個資法施行細則

- 法務部2011年10月27日在官方網站公布個資法施行細則草案。法務部法律事務司副司長鍾瑞蘭表示，草案將進行14天的法案預告，來蒐集各界對草案的建議。
- 法務部2012年9月27日在官方網站公布個資法施行細則。法條共三十三條。

個人資料檔案(細則§3)

- 間接識別
  - 指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

52

間接識別案例說明

- Q：何謂以間接方式識別該個人之資料？何謂不能識別？例如學校職員A從校務行政資料庫，將學生資料中之一個欄位「聯絡方式」賣給補教業者B，則是否屬個人資料保護法所規範之可識別個人資料。

- A：(1)就A 而言，雖然A 只挑選學生資料中一個欄位「聯絡方式」，單純就連絡方式之資料內容來看，無法得知該資料之特定個人為何人，但是A 或A 所代表的機關本身，仍有該校務行政資料庫之其他資料欄位可供對照、組合、連結等間接方式，而能識別該特定個人，故就A 或A 所代表的機關該單筆資料欄位仍屬可間接識別之個人資料。A 以意圖營利之方式販賣可識別之個人資料，該當個人資料保護法第41條第2項之刑事構成要件而應負刑事責任。

(2)就B而言，該「聯絡方式」之個人資料如無法透過資料庫之對照、組合、連結等間接方式而加以識別該特定之學生，則屬查詢有困難之情形（究屬查詢困難、耗費過鉅或耗時過久始能特定之情形需個案認定），故為無法識別之個人資料，無個人資料保護法之適用，惟如屬其他法令規範之範圍，則仍有其他法令之適用，例如民法第18條及第195條之侵害隱私權等規定。

個人資料檔案(細則§4)

類別	內容（施行細則）
醫療	指包含病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。
基因	由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。
性生活	指性取向或性慣行之個人資料 。
健康檢查	指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料 。
犯罪前科	指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄 。

54

個人資料檔案(細則§5)

- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
- 備份資料

55

個人資料檔案(細則§6)

- 刪除
  - 指使已儲存之個人資料自個人資料檔案中消失
  - 刪除行為之認定，應視刪除當時科技水準及技術，參酌適用主體之組織型態，使用一般社會通念之標準，所為使個人資料消失之行為，以作為參考標準，尚無需達「不復存在」之標準，始謂符合本法所稱之「刪除」

- 內部傳送
  - 指公務機關或非公務機關本身內部之資料傳送

56

個人資料檔案(細則§7)

- 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

57

個人資料檔案(細則§8)

- 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。
  - 監督至少應包含下列事項：
    一. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間
    二. 受託者就第十二條第二項採取之措施。
    三. 有複委託者，其約定之受託者。
    四. 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
    五. 委託機關如對受託者有保留指示者，其保留指示之事項。
    六. 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

58

個人資料檔案(細則§8)

- 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。
  - 第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。
  - 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關

59

個人資料檔案(細則§9,10)

- 本法第六條第一項第一款、第八條第二項第一款、第十六條第一項第一款、第十九條第一項第一款、第二十條第一項第一款所稱法律，指法律或法律具體明確授權之法規命令。
- 本法第六條第一項第二款、第八條第二項第二款及第三款、第十條第二款、第十五條第一款、第十六條所稱法定職務，指於下列法規中所定公務機關之職務：
  - 一、法律、法律授權之命令。
  - 二、自治條例。
  - 三、法律或自治條例授權之自治規則。
  - 四、法律或中央法規授權之委辦規則

60

必要措施包括(細則§12)

成立管理組織，配置相當資源

界定個人資料之範圍

個人資料之風險評估及管理機制

事故之預防、通報及應變機制

個人資料蒐集、處理及利用之內部管理程序

資料安全管理及人員管理

認知宣導及教育訓練

設備安全管理

資料安全稽核機制

必要之使用紀錄、軌跡資料及證據之保存

個人資料安全維護之整體持續改善

61

必要措施包括(細則§12)

- 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。

62

書面同意(細則§14,15)

- 本法第七條所定書面意思表示之方式，依電子簽章法之規定，得以電子文件為之。
- 本法第七條第二項所定單獨所為之書面意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。

63

告知(細則§16)

- 依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。

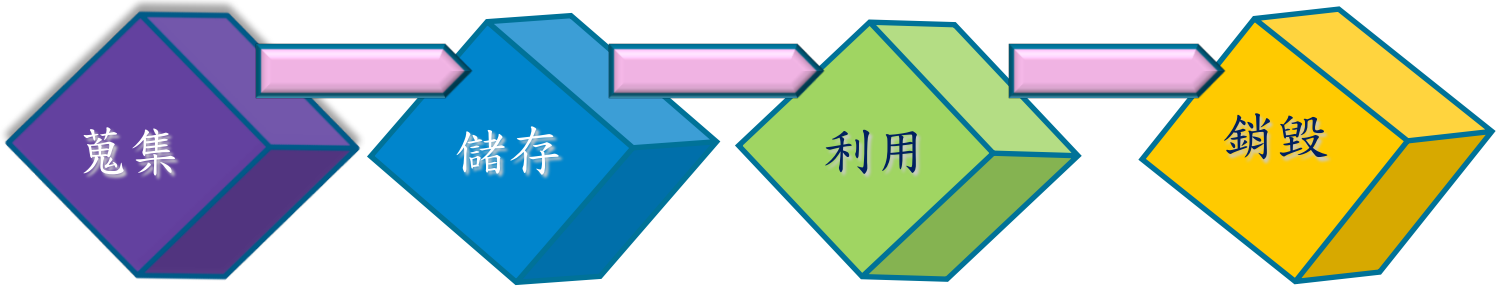
64

專人(細則§25)

- 公務機關指定『專人』辦理安全維護措施
  - 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，應辦理或使專人接受相關專業之教育訓練

65

施行細則內容



依法進行告知義務

取得書面同意

採取適當保護措施，避免個人資料被竊取、竄改或毀損

應於蒐集之特定目的內 使用

特定目的外之使用應另 外取得書面 同意

特定目的消失

期限屆滿

當事人要求

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

哪些個人資料不受個資法保護（個資法第51條）？

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

- 例如社交活動、寄送喜帖、親友通訊錄等
- 上述資料的蒐集必須與職業或業務職掌無關

於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料

- 例如運動會照片、遊樂場拍攝小孩與其他小孩一起遊玩的影片等
- 為解決合照或其他在合理範圍內之影音資料須經其他當事人書面同意始得蒐集、處理或利用之不便，因此排除個資法對上述影音資料的適用，回歸民法規定。

＊日本個人資料保護法另外排除五千筆資料以下的單位

案例：學生入學後，學校可以如何使用其資料？例如：學校相關活動（含社團等）是否可以透過信件寄發給所有學生？誰有資格寄發或使用？

學校、社團辦活動可透過信件寄發通知給學生。

學校辦活動之單位及社團都可以寄並使用學生的個人資料，此符合學校教育以及成立社團之特定目的，但若學校所辦活動其實是廠商的行銷活動，則有爭議。

學校不可以把學生的資料給合辦活動的廠商使用，這部份請學校評估學校使用學生個人資料之用途與目的，是否符合學校教育興學之目的。

69

案例：學生入學新生訓練時，是否是恰當時機，讓學生知道學校可能利用其資料的狀況，並在新生訓練或註冊時，取得同意的「授權」？

除非學校使用個人資料有可能超過教育行政之特定目的,不然是不需要學生額外授權。不過因為新法增加了"告知"義務，在學生入學時就要立刻履行告知義務

詳述學校使用個人資料之範圍用途等等。如果學校或做超過特定目的之利用,就應該及早告知學生並取得"書面同意"。

70

案例：畢業生紀念冊上的學生相關資料應該屬於個人資料？但目前都視同慣例，是否未來有風險？如何補救？至於圖書館陳列的歷屆畢業紀念冊是否應該管理?

紀念冊上的學生資料是個人資料。

過去紀念冊的蒐集與公開並非違法行為，但是因為現在有販賣個人資料或是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並加以控管，例如限制可以閱覽紀念冊的人員。

71

案例：學校目前的畢業學生資料，如何是屬於合法使用？是否可以寄發活動通知？或者應該在學生畢業前，先取得畢業學生的同意授權？至於過去幾時年的畢業生資料如何使用與管理才能符合新的個人資料保護法的蒐集、利用之範圍？

學校使用校友的資料應該還是必須符合"教育行政"的特定目的，如果超過這個目的還是不能使用，可能需要在畢業前取得學生授權。

一般人並不會反對辦校友活動會超過特定目的，這個部分學校應該與教育部以及法務部溝通確保學校能繼續使用校友資料，學校還是應該要建立控管機制，避免校友資料外洩。

72

案例： 老師在幫學生寫介紹信前，會要求學校職員提供該學生多年的相關資料（個人資料與成績），該如何處理？職員提供該資料前，是否應取得學生之同意？

老師幫學生寫介紹信在美國教育體系下是老師的義務，若在臺灣，幫學生寫介紹信已經成為教授或老師天經地義的工作，則學校應該要提供給教授相關資料而無須取得學生同意。

重點在於，證明教授或老師是為了寫介紹信而不是為了其他目要求學校提供學生資料。

學校可考量要求教授或老師出示學生的申請書，或者是教授或老師要求學生自己向學校申請資料並由學校直接交給教授等，不同的做法。

73

案例：學生借書紀錄，是否涵蓋在個資範圍內？老師擔心學生最近是否因閱讀某一些讀物而行為有一些偏差，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？

學生借書紀錄包括學生姓名、社會活動或其他得以識別學生之資料，構成學生個資。

圖書館保存借書紀錄的目的是為了「圖書館管管理」之特定目的，而非為了讓老師檢查學生行為偏差是否與閱讀某些讀物有關之目的。

如有證據可合理懷疑某學生偏差行為與閱讀有相當關聯，老師為了進一步確認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，且應尊重當事人之權益。若老師在無任何證據情況下調取學生借書紀錄，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。

因此，「圖書館」是否可以將學生借書紀錄提供給老師，應視具體個案中老師可否提供合理之說明及證據來作決定。

74

案例：學務處提供家長查詢學生考試成績或學習紀錄，使用方式是以「學生的身分證字號」登入為查詢依據，請問學務處可以提供家長查詢嗎？若可以，可以提供到什麼程度？另外針對已成年的學生或未成年的學生是否有不一樣的處理方式。

應區分成年和未成年，成年學生的家長應無法查詢，除非有學生授權。未成年的家長是學生的法定代理人，應該都能看才對。

案例：學校可以為了保護學生，蒐集學生病史、健康、身分（低收入戶）資料等涉及特種個資嗎？

有關病史、健康檢查的部分，要看教育部的法規有沒有允許。低收入戶並非特種個資。

75

案例：導師是否可以知道班上同學的學習狀況，導師可以知道同學修課成績嗎?

如果導師取得學生的修課成績，是為了瞭解學生的學習狀況，此為執行法定職務必要範圍（公立學校）或因學校與學生間之契約關係（私立學校），為了特定目的（教育或訓練行政）所為，符合個資法的規定。

案例：學校是否可寄發認同卡相關資料給校友?

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。

76

案例：個資法中之特種個人資料規範中，若個資擁有者自行公開之個人資料，是可以收集的，但是請問這樣的資訊可以拿來傳播嗎？

雖然已公開的特種個資是可以蒐集的，但蒐集及利用仍須符合特定目的，並不是任意可以拿來傳播的。

案例：身心障礙是否為特種資料？（例如：殘障手冊，或公務人員履歷表上註明身心障礙）

身心障礙須依據醫療機構之鑑定結果核發身心障礙證明而為認定。如以法務部指定之個資法施行細則草案之定義，「醫療」指「以治療、矯正或預防人體疾病、傷害、殘缺為目的，所為的診察、診斷及治療…」，身心障礙似符合上述「醫療」之定義，從而屬於特種個人資料之一種。

77

案例：網頁上的學生家長區，家長可以查詢學生的個人缺曠、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，似為學校執行法定職務必要範圍，且與蒐集之特定目的（教育或訓練行政）相符。

惟大學生瞭解自己的缺曠課資料及操行成績，依其年齡及身分，應為其日常生活所必需，且滿20歲之大學生已為成年人，不論其為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的缺曠課資料及操行成績提供家長查詢，始能達到教育或訓練行政之目的，恐有疑義。

建議教育部對此作成統一解釋，以便學校知所遵循，避免學生質疑。

78

案例： 在公告欄上公告曠課學生名單（學生姓名、學號）有違反個資嗎?

有關獎懲之作法，應符合學校辦理教育行政之目的，公布應不違反個資。

學生成績預警制度，若有扣8分或扣16分的情形，是否可以寄給家長知道?

學校將學生預警制度扣分情形告知家長，似為學校執行法定職務必要範圍，且與蒐集之特定目的（教育或訓練行政）相符。

大學生收受成績預警制度之資料，依其年齡及身分，應為其日常生活所必需，且滿20歲之大學生已為成年人，不論其為意思表示或受意思表示，均無須法定代理人（家長）之允許，因此大專院校是否必要告知學生本人之成績預警資料，另行提供學生家長，始能達到教育或訓練行政之目的，恐有疑義。

79

案例：某大學為獎勵學生畢業，將學生部分資料公開於網頁上，經學生提告後，將網頁資料撤銷，但在Google仍搜尋得到，請問是否可以要求學校向Goolge交涉，或需由學生自行要求Google撤銷其資料？

網頁由學校建立，學校應盡早找 Google 交涉，否則有可能仍然有責。

案例：系所或系科主任希望知道各老師教學狀況，以作為老師的教學評量、教學評鑑使或其它考核用途，請問課務組該如何因應處理？

課務組提供老師教學狀況給系所或系科主任，作為教學評量、評鑑或其他考核用途，屬於學校處理及利用老師個人資料的行為，應屬特定目的（教育或訓練行政）之必要範圍，符合個資法規定，因此是可以提供的。

80

案例：「就業輔導處」針對學生畢業後，使用學生相關個人資料，是否邀簽署同意書？是否有時效問題（例如：5年或7年）？若資料須放更久，如何處理？

如學校已經在簽署同意書上說明特定目的與理由，則學校於符合特定目的之情況下，得於學生畢業後繼續使用學生之個人資料，不會受到期間的限制。

案例：學校的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招生資料?

學校蒐集考生個人資料之特定目的為學生資料管理，而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。

81

小結

- 學生獎懲資料符合學校辦理教育行政之目的，公布不違反個資法。
- 每位教職員均應檢視自己放在網路上與學校有關業務的資料是否違反個人資料保護法蒐集、處理與利用之規範，若有請立即自行刪除，若無法自行刪除者，應通知學校資訊單位協助處理。
  - 例如，班級網頁中是否有學生的姓名、生日、照片(特別是照片旁有標註可供辨識學生身份的資料) 等之資訊揭露。
- 學校辦理研習課程等活動之簽到單，須妥善保管並定期或不需要時予以銷毀。
- 學校網站上若出現學生班級、座號、全名、健康狀況、家庭狀況、聯絡方式、輔導紀錄、申請補助進度等資訊，須進一步檢視公開之必要性，或進行必要處理後再公開。

82

小結 (續)

- 教師索取學生個資需由業務承辦人判別是否合乎該師之職權，方可給予個資；可透過建立調閱紀錄表並由權責主管簽核等方式進行管控與追縱。
- 歷屆的畢業紀念冊不開放讀取，必要時可上鎖保存，並建立限制可接觸畢業紀念冊人員之規定。
- 保留重要或敏感個資之處所需有門禁等實體安全控管機制；存放個人資料的電腦也需安全控管機制，例如密碼。
- 包含個人資料的電腦在報廢前，需將硬碟資料進行完全知移除（不只是清空電腦資源回收筒）。
- 因教學、行政而辦的活動，可透過電子信件寄發給所有學生，不違反個資法。
- 向尚未成年之學生取用個資，需取得當事人或監護人同意方可行之。

83

簡報大綱

一、什麼是個人資料

二、個資法基本認知

三、個資法架構與第一章部分條文

四、個資法蒐集、處理及利用

五、個資法部分條文罰則

六、個資法施行細則重點

七、相關案例

八、 建議

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**是否充分且符合業務推動之需求，適時向主管機關（教育部獲教育處）提出修正或增修之建議。

- **立即進行組織內個人資料盤點工作，瞭解組織擁有的個人資料種類、數量、保存與利用情形，並確認蒐集當時的特定目的，以為後續風險評估與建議安全管控措施之基礎。**

- 設置組織負責規劃個人資料保護相關事宜。

- **進行必要的資訊安全與個資教育訓練。**

資料蒐集、處理、利用之自我檢查五步驟

步驟一：清點所有之個人資料

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

施行細則第十二條說明

措施1：配置管理之人員及相當資源

企業必須指派一位人員出任個資管理代表，也就是專門處理個資相關事項的專員。另外，依據執行時的需要，企業必須提供相關的經費、人力等資源，來協助管理人員實施各項管理程序。

措施2：界定個人資料之範圍

也就是所謂的個資盤點，目的是要找出企業內部所有的個人資料。企業可依據個資的資料流來設計盤點表，讓各部門逐一清查，找出各部門中存放個資的載體，例如可能儲存個資的文件、手冊或系統等。

措施3：個人資料之風險評估及管理機制

企業可進行風險評鑑或是隱私權衝擊分析，從這兩項作業中了解資產的價值、可能遭遇的風險以及有哪些較為敏感的個資。

措施4：事故之預防、通報及應變機制

企業應建立起事故應變的通報程序，也就是發生了事故後，該通知誰，該如何處理，都要有相對應的方法。此外，要從發生的事故中找出對應的預防措施。

措施5：個人資料蒐集、處理及利用之內部管理程序

企業要制定出一套合法的業務流程，對於蒐集、處理及利用這三項有明確的流程規範，並將其制定成程序書，以便員工查閱。

措施6：資料安全管理以及人員管理

企業要將資料分級，並依據不同職位的員工設定存取權限，而存放資料的位置，要採取防護措施，像是資料加密、防火牆、入侵偵測系統等等。

措施7：認知宣導及教育訓練

企業應定期對全體員工舉辦教育訓練，內容包括法令宣導、內部規範宣導等等。而且企業必須要保存這些教育訓練或認知宣導的實施記錄，作為未來證明自己的確有善盡良善管理之責的證明。

措施8：設備安全管理

針對各式各樣的設備，如：USB、隨身硬碟、行動裝置等，要有明確的使用規範，才不會因為使用這些載具而造成個資外洩。

措施9：資料安全稽核機制

企業可聘請專業顧問公司定期稽核個資保護的流程，或是舉辦內部稽核活動，可以從報告中找出缺失或潛在的問題。

措施10：使用紀錄、軌跡資料及證據保存

經由各項程序所產生的任何形式記錄，企業皆需妥善保存，以利日後舉證之用。依個資法的規範，發生個資損害事件後的5年內都可求償，這也意味著企業相關個資記錄至少要保存5年。

措施11：個人資料安全維護之整體持續改善

企業的管理高層應該定期開會，或是有重大事故時召開會議，評估個資保護制度落實的程度，並持續改善。同樣的，這些改善會議或企業個資保護措施的改善作為也都需要記錄。

簡報完畢，敬請指教