國立中興大學

個人資料保護法與案例宣導

2013.3

個人資料，無所不在

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

其他資料
- 得以直接或間接方式識別該個人之資料

3

個人資料內容

類別	內容
特徵	年齡、性別、出生地、國籍、身高、體重、血型、抽煙、喝酒等。
婚姻	婚姻之歷史：前次婚姻或同居、離婚或分居等細節及相關人之姓名等。
	家庭其他成員之細節：子女、受扶養人、家庭其他成員或親屬、父母等。
家庭	是否結婚、配偶或同居人之姓名、前配偶或同居人之姓名、結婚日期、子女數等。
教育	學校紀錄：學歷、科系、畢業或肄業等。
	學生紀錄：學習過程、相關資格、考試成績或其他學習紀錄等。
職業	現行之受僱情形、離職經過、工作經驗、工作紀錄。
病歷	依醫療法(第六十七條)所定之病歷應包括下列各款之資料： 一、醫師依醫師法執行業務所製作之病歷。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。(此部份尚未確定)
聯絡方式	傳統聯絡方式：電話、地址、電子郵件等。
	時尚聯絡方式：MSN、SKYPE、Facebook、噗浪、微博、部落格、PTT 帳號等。
財務情況	帳戶之號碼與姓名、信用卡或簽帳卡之號碼、收入、所得、資產、投資、銀行、負債、支出、信用評等、貸款、結匯紀錄、票據信用、津貼、福利、贈款等。
社會活動	移民情形、旅行及其他遷徙細節、休閒活動及興趣等。

4

個人資料內容(續)

- 特種個人資料，包括醫療、基因、性生活、健康檢查、犯罪前科

類別	內容
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；或基於診察、診斷結果，以治療為目的，所為的處方、用藥、施術或處置等行為全部或一部之總稱。
基因	指人體之染色體所儲存超過十萬對以上最基本而具有全部遺傳特質或特定生物功能DNA(去氧核醣核酸)之遺傳單位。
性生活	指所有與性行為有關之活動之總稱，如性傾向、性慣行等。
健康檢查	指以檢驗為目的所為一般性或遺傳性、傳染性、精神性等疾病檢查之健康資料之總稱，如健康檢查報告等。
犯罪前科	指構成犯罪之具有犯罪紀錄者而言。

5

個資外洩管道

- 問卷
- 電話客服中心
- 網購
- **掛馬網站、設計不良的網站**
- **駭客入侵**
- **社群網站**
- **P2P軟體使用**
- 銀行申請單
- 會員手冊
- 信用卡
- 內部人員
- 補習班
- 電子謄本系統
- 直銷公司
- 盜版光碟
- **即時通訊軟體(IM)**
- 無個資保護認知
- **釣魚網站**
- 委外廠商

6

個人隱私資料
隨時隨地都在被洩露

- 扯2科大洩數百生個資
- 當紅炸子雞 臉書賣個資賺錢
- 蘋果用戶上谷歌 隱私恐不保
- 銀行二手硬碟 民眾借貸資訊全都露
- 警濫權查名人個資 主管連坐罰

7

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

9

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.

10

“過去從來沒有一個時期像今天，隱私資料會如此重要而且容易被取得。隱私資料是銀行、金融、醫療，甚至社交網路上處理、交易的基礎。透過數位化與網路的普及，大量的隱私資料被政府部門與企業蒐集、儲存與分析。歐盟的立法機構、法規部門以及企業現正面臨「如何保護人民的個人資料被罪犯或恐怖分子利用的同時，可以確保資訊的自由流通以維持正常經濟、社會的運作」的挑戰。”

Milon Gupta, Eurescom

11

“雲端計算、社交網路、RFID晶片、LBS(位基服務)、手機數位通訊、搜尋引擎等” 都會沖擊到我們的隱私資料，歐盟的人民或世界上的每個人都會面臨網路犯罪的風險，而這些挑戰經常來自歐盟以外的地區。”

Milon Gupta, Eurescom

12

“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。
- 個人資料保護法：101年10月1日正式施行。
  - 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。
  - 100年10月26日施行細則草案公告。
  - 施行細則101年9月26日正式施行。

13

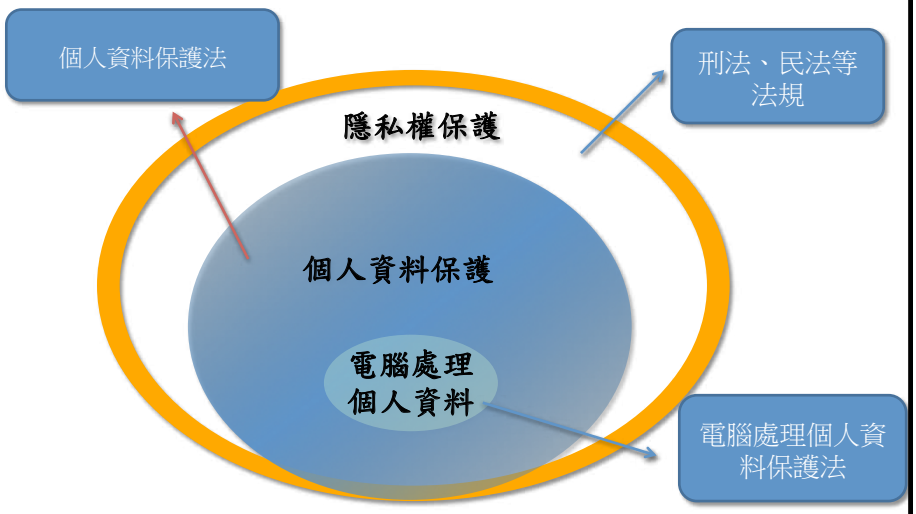
個人資料保護法之立法目的

避免人格權侵害

促進個人資料合理利用

14

隱私權與個人資料保護？



15

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

16

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）

17

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。

18

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

19

個人資料保護法規範的行為 (態樣)

個人資料檔案

- 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
  → 非經電腦處理的個人資料（如紙本）亦納入規範

蒐集

- 以任何方式取得個人資料
  → 不限於為建立「個人資料檔案」取得
  → 包括直接向當事人蒐集、間接從第三人取得

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。
  → 不限於電腦處理，可能是快遞寄送、影印機複製等行為

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亦屬於利用之行為

20

資料違法外洩時，一定要和當事人說嗎?

21

- 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)

22

個資法規定的安全保護相關規定有哪些?

23

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) 。

24

個資法施行細則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。

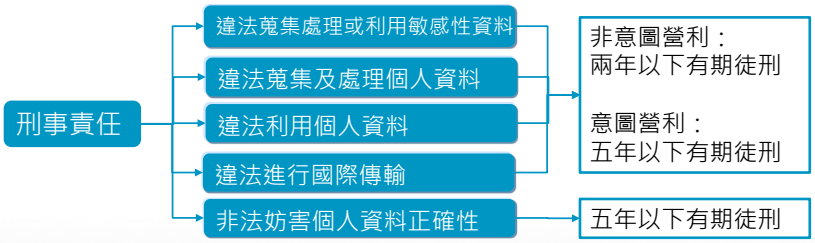
此11項安全措施內容為參照英國BS10012:2009 及日本JISQ15001:2006 等個人資料管理系統之規範，以P-D-C-A 循環之概念予以建立。

25

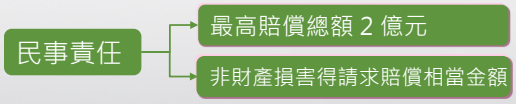
若違反個資法，只要罰錢就可以了嗎?

26

公務機關之法律責任



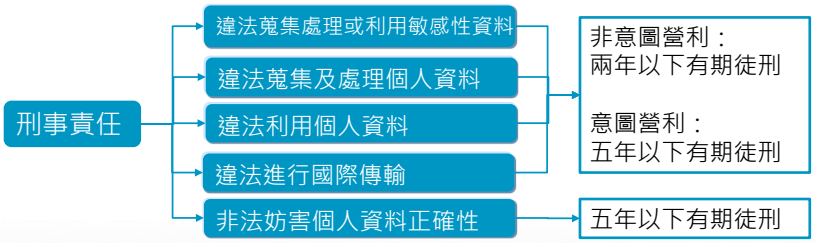
公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)

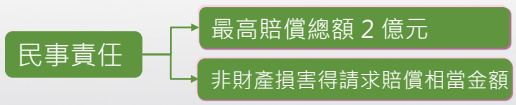


公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。(§28)

27

非公務機關之法律責任

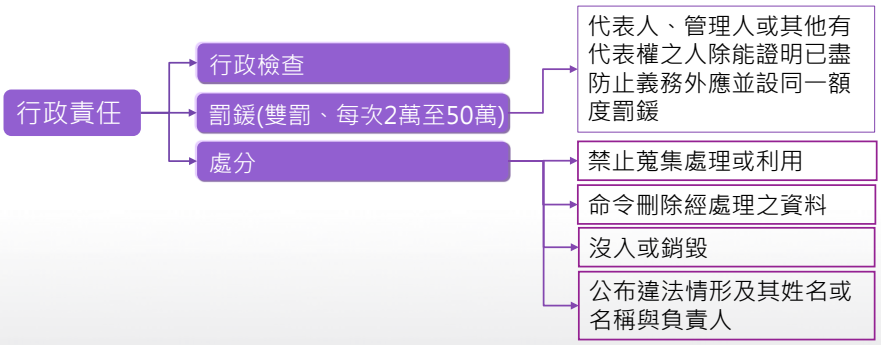




非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵 害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。(§29)

28

非公務機關之法律責任 (續)



29

案例：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。

30

個資保護，你可以作什麼？

- 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。

- 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**。

- 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。

- 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**。

個資保護，你可以作什麼？(續)

- 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。

- 對於調閱個人資料的人，加以**記錄其調閱身分及行為**。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。

- 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)

- **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。
- 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。
- 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。
- 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**。

33

個資保護，你可以作什麼？(人員管理)

- 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。
- 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。
- 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。

34

個資案例分享與討論
(社團活動篇)

35

個資保護管理要訣

個資保護管理要訣：

- ✓ 人員意識(教育訓練宣導)
- ✓ 內部權責區隔
- ✓ 資料分權原則
- ✓ 最小儲存原則(僅取所需個資)
- ✓ 資料加密原則
- ✓ 最小揭露原則
- ✓ 資料遮隱原則
- ✓ 實體安全
- ✓ 設備與媒體管理
- ✓ 委外廠商管理(Nokia 事件)
- ✓ 不公務家辦(家用電腦安全)

36

Q&A 問題與討論

37