台南市教育局

個人資料保護法與案例宣導

2014.7

課程大綱

一、個資法基本認知

二、適用範圍與條文罰則

三、個資盤點概要

四、個人資料保護管理作業流程

五、個資安全防護暨委外管理作業建議

六、實務案例說明

七、問題與討論

2

課程大綱

一、個資法基本認知

3

個人資料，無所不在

4


盜用
LINE
拐代墊詐財
主管帳號遭駭 發訊30同事2受害
林金聖、林志青・報導 LINE淪為詐騙工具！北市1名男子接獲主管LINE的請託訊息，幫忙代墊3500元收下網購的衣服，他代墊收貨之後，詢問主管才知被騙，他昨查詢發現同單位近30名同事都收過此訊息，包括他共2人受害，近日將報案。
刑事局指出，LINE在台用戶數逾1600萬，詐騙集團疑利用木馬程式等病毒，入侵電腦竊取LINE網路版的帳號密碼，再假冒親友身分行騙，據165反詐騙專線統計，近半月來共3件LINE詐騙諮詢案，其中1人被騙，尚不包含蔡男及其同事的詐騙案，提醒民眾收到代付貸款簡訊，應打電話求證。
◀被害民眾收到主管遭盜用的帳號傳訊，謊稱「先幫我墊付」。
在嗎
在忙？
我昨天買了一件adidas的衣服 週末天會到 但我有急事要出去幾天 你先幫我簽收 可以嗎
當然可以阿
不過是貨到付款的 可能要你先幫我墊付


+886931809616
女士,您正在申請網上支付103年4月電費共計1980元，若非本人操作，請查看電子憑證進行取消http://goo.gl/ZT5FSL
新增文字

5


LINE騙案猖獗
詐177萬
LINE帳號被盜申復流程
可惡，帳號又被盜了啦！
1
2
3
4
5
LINE被盜
通報救帳號
24小時內處理 審核後返還
俱增，刑事局日前與LINE台灣分公司開會討論，警方研判恐是用戶安裝電腦版LINE，才遭駭客盜帳號。
LINE隨後改善軟體安全機制，上月先推出「認證碼」，本月再增加「問題反應表」。LINE台灣公關公司表示，民眾可透過電腦或手機，在反應表填入相關資料後傳送，就會得到一組案件編號，同時提醒親友勿被騙，客服人員將在24小時內回傳電郵確認，審核通過就會返還帳號。
對LINE的防護機制，刑事局說，除「認證碼」和「問題反應表」外，將會限定單一手機門號只能有1個帳號，防帳號遭竊從事不法。
在忙嗎 能請你幫個忙嗎
好
很急嗎？
你現在方便幫我買下MYCARD點數卡嗎

資料來源：爽報

6

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

7

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。

8

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。

9

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

10

個人隱私資料
隨時隨地都在被洩露

- 批2科大洩數百生個資
- 補教業者，假冒學生會..... 非法收集個資
- 教育單位入口網站遭駭 學生資料恐不保
- 二手硬碟轉售，個資全都露
- 國中生資料隨意丟棄校外 主管連坐罰

11

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

12

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.

13

"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。

14

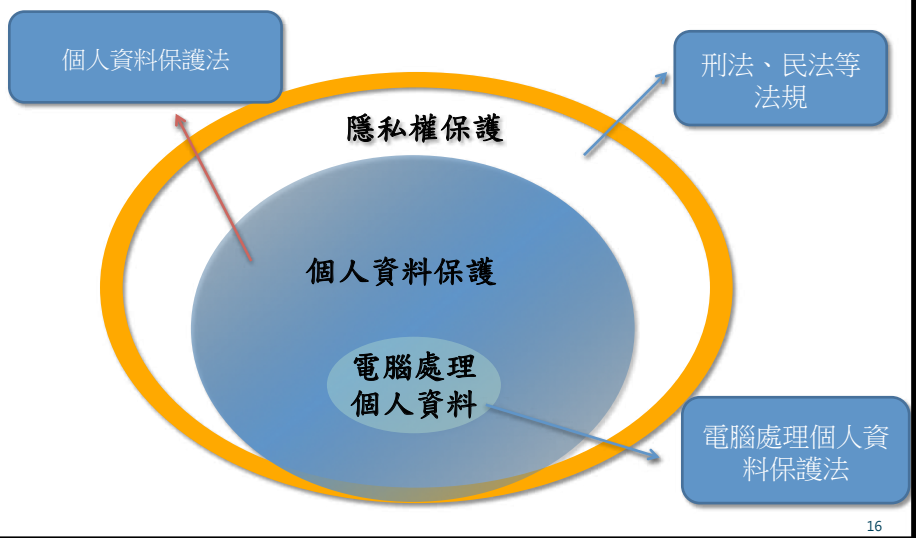
個人資料保護法之立法目的

避免人格權侵害

促進個人資料合理利用

15

隱私權與個人資料保護？



16

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

17

課程大綱

二、適用範圍與條文罰則

18

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）

19

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。

20

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

21

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

22

資料違法外洩時，一定要和當事人說嗎?

23

- 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)
- 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)。

24

個資法規定的安全保護相關規定有哪些?

25

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	配置管理之人員及相當資源。
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。

26

若違反個資法，只要罰錢就可以了嗎?

27

公務機關之法律責任

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)

28

課程大綱

三、個資盤點概要

29

個資的價值?
一個存有個資的小小隨身碟的價值，就等同一棟豪宅

- 假設每筆求償金額為10,000元台幣。若有20,000筆資料遭竊或不慎外洩，求償金額將可達10,000x20,000= 200,000,000(台幣2億元)
- 也就是2萬筆個人資料的價值，約等於豪宅一棟

人手一支的USB隨身碟，至少可儲存個資檔案數萬至數百萬筆

姑且不論資料本身的附加價值，僅幾萬筆個資盜失所造成的損害賠償金額，就已等同於1棟以上豪宅價值

豪宅，每戶至少價值1.5-2億以上

個資法第二十八條—

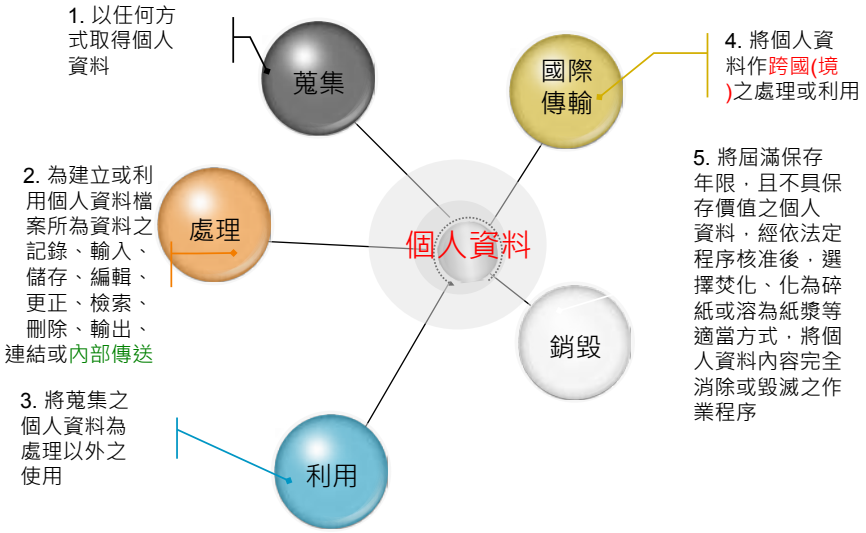
公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

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分。

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。

30

個人資料檔案盤點作業(續)



個人資料檔案盤點重點在於個資之生命週期

31

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

32

課程大綱

四、個人資料保護管理作業流程

33

學校暨幼兒園個人資料保護管理作業流程

34

課程大綱

五、個資安全防護暨委外管理作業建議

35

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、毀損與滅失。

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。

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**。

36

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**。

個資保護，你可以作什麼？(人員管理)

持續訓練

- 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。

39

課程大綱

六、實務案例說明

40

個資案例分享與討論

41

課程大綱

七、問題與討論

42

Q&A 問題與討論

43

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
- ✓ 不公務家辦(家用電腦安全)

44

聯絡資訊

王吉祥(Davies) 講師暨資深經理
+886 970 350 128
dvings@gmail.com

45