新興醫療社團法人新興醫院

個資法與資訊安全認知訓練

林彥丞

108年7月24日

簡報大綱

1. 個資遭受侵害案例分享
2. 個資保護的法制現況
3. 個人資料保護法重要內容
4. 發生個資侵害事件緊急處理
5. 個資法常見疑義
6. 安全防護從現在做起

個資遭受侵害案例分享

學校漏洞 洩260新生個資

發生事故：

逾260名彰化縣○○國中學生的新生個資在網路上外洩，包括學生姓名、身分證字號、出生年月日、住家地址等都被看光光，意外發覺的民眾直呼「有夠誇張」。

發生原因：

學務電腦系統疑有漏洞。

可採取強化措施：

1. 緊急刪除檔案並通報須修正此程式。
2. 緊急刪除檔案。

員工盜勞動部3萬筆個資 約談老闆

發生事故：

勞動部勞動力發展署求職就業網站「台灣就業通」，疑被債務催收公司「元誠國際資產管理公司」竊取3萬4000多筆求職民眾個資，檢調懷疑個資被用於討債。

發生原因：

疑為帳號密碼被得知。

可採取強化措施：

1. 封鎖該連線電腦IP位址。
2. 變更密碼。

買二手硬碟 赫見機關往來個資

發生事故：

立委舉行「資安漏洞，隱私不保」記者會指出，一名林姓民眾向他反映，在光華商場購買2顆中古硬碟，接上電腦後發現有某業者的工作資料、民眾與銀行往來借貸相關資料，並清楚記載與銀行業務往來的民眾姓名、身分證資料、地址、借款金額等相關資料。

發生原因：

1. 對受託廠商之監控未完整。
2. 對資訊設備報廢之管控未完整。

可採取強化措施：

1. 制訂保存期限
2. 保全放置地點
3. 建立銷毀機制
   A. 銷毀前準備
   B. 銷毀時確認
   C. 銷毀後留存銷毀紀錄

通知單寄錯 學校洩50學生個資

發生事故：

一名不願具名的○○高中新生家長表示，七月一日他收到錄取通知單，通知單上竟不是小孩的姓名，因資料上還有學生的身分證字號，且小孩的其他同學也收到他人的通知單，並非個案，不免讓他擔心小孩的個資遭洩，「校方真該改善。」

發生原因：

電腦抓取資料過程有疏失，
錯置部分錄取學生的收件地址。

可採取強化措施：

1. 已致電給受影響的學生和家長，回收錯誤資料。
2. 加強人員資安教育。

提供拒絕行銷資料予其他公司進行行銷

發生事故：

○○金控公司將子銀行○○銀行所提供不同意其基本資料以外資料為行銷之目的而交互運用之客戶資料，經篩選後將該等客戶之資料提供予○○保險經紀人公司辦理共同行銷，違反金融控股公司法第42條第1項規定，依同法第60條第12款規定，核處新臺幣200萬元罰鍰。

發生原因：交付之資料實質上已涵蓋客戶信用等級及帳戶往來水準等基本資料以外之財務狀況資料。

可採取強化措施：

1. 進行人員宣導，使同仁瞭解拒絕行銷之需求。
2. 建立拒絕行銷流程，避免違法使用客戶資料行銷之機制。

離職員工以私人外接儲存裝置挾帶個資

發生事故：○○銀行信託部○姓員工於離職前，將客戶資料下載至私人外接儲存裝置(USB)並攜走。資訊系統之公用資料夾管理，未能依行員行使職權範圍建立妥適之存取權限及授權控管，致行員得存取非與其職務相關且含客戶個人資料之檔案。違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處新臺幣300萬元罰鍰。

發生原因：

1. 未建立公用資料夾之檔案存取權限及授權控管。
2. 未針對員工使用USB存取資料建立每日監視控管機制。

可採取強化措施：

1. 建立人員離、調職流程，控管公司資源存取權限。
2. 建立公用資料夾之檔案存取權限及授權控管，以及員工使用USB管理機制。

公所蒐集個資印在通訊錄上發放

發生事故：

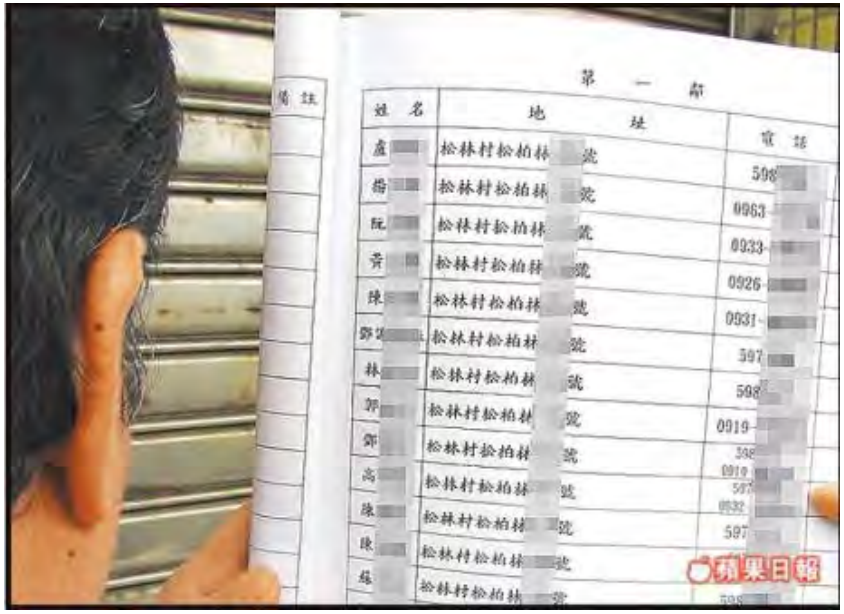
「全村都知道我的電話！」一名新豐鄉松林村民不滿指出，兩年前村裡的地方耆老曾來索取聯絡方式，當初告知要做為公務傳達、緊急聯絡使用，突然收到一本新豐鄉公所製作發放的戶長通訊錄，居然登錄村裡每一戶戶長的手機、市話，才得知個人資料全被公開，擔心遭有心人士利用。

發生原因：

個人資料保護法認知、意識不足。

可採取強化措施：

1. 進行個資保護宣導，強化同仁對於個資法的認知。
2. 個人資料的蒐集、處理、利用應有核准機制。



天上掉下工作機會？ 詐騙集團騙個資

發生事故：

前陣子出現新型詐騙手法，民眾突然收到一個Line訊息，對方表示，六合彩、運動彩券等需要招募會員，拉一個人可賺得4200元、二個人8400元，宛如在家滑手機、輕鬆賺小錢。詐騙集團佯稱，「公司已經先代繳會費，發薪資需等開盤後」，為了確認會員身份需要名字、電子信箱、手機號碼、Line ID等個人資料，發薪資則需要銀行帳戶、帳本、提款卡等

發生原因：

人員安全認知不足。

可採取強化措施：

1. 加人員強安全認知訓練。
2. 撥打165反詐騙專線。

個資法首宗刑事判例

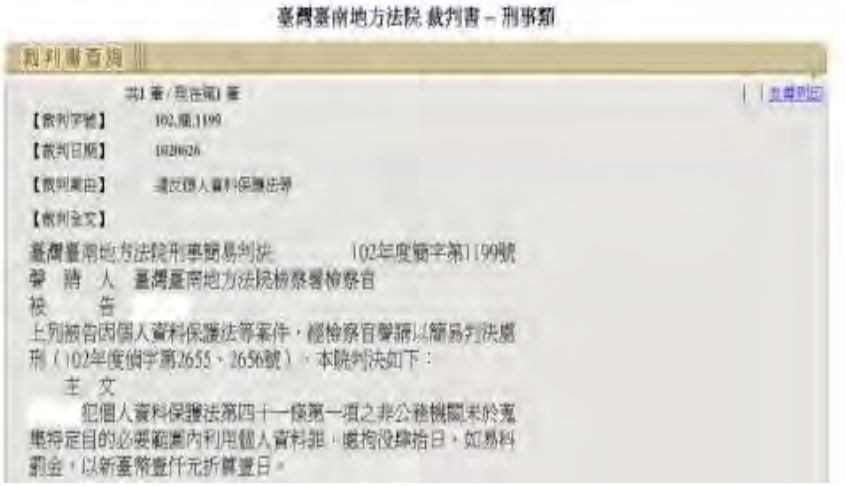
發生事故：根據判決書的內容，發生在臺南的個案，起因是被告不滿社區地下停車場使用的爭議，遂在自己的Facebook專頁上，公開告訴人的姓名、照片等資料，除了公布他人個資之外，文字中並帶有誹謗字眼。

發生原因：

對被告使用停車場行為不滿。

判決：

1. 依違反個資法第20條第1項、第41條第1項，處拘役40天，可繳交易科罰金4萬元。
2. 誹謗罪的刑事處分。


臺灣臺南地方法院 裁判書－刑事類

裁判書查詢

【裁判字號】 102,簡,1199

【裁判日期】 1020626

【裁判案由】 違反個人資料保護法等

【裁判全文】

臺灣臺南地方法院刑事簡易判決　　102年度簡字第1199號

聲 請 人　臺灣臺南地方法院檢察署檢察官

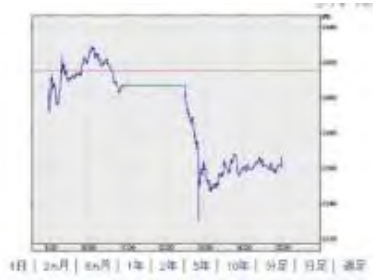
被　　告

上列被告因個人資料保護法等案件，經檢察官聲請以簡易判決處刑（102年度偵字第2655、2656號），本院判決如下：

主　文

犯個人資料保護法第四十一條第一項之非公務機關未於蒐集特定目的必要範圍內利用個人資料罪，處拘役肆拾日，如易科罰金，以新臺幣壹仟元折算壹日。

個資外洩的後果



如何喚回使用者的信任

主管機關密切監督

鉅額罰款損組織元氣

外界與論壓力

危害組織良好形象

個資保護的法制現況

《個人資料保護法》已於2012.10.01正式上路！

2012年9月30日
公布《施行細則》


電腦處理個人資料保護法施行細則修正條文對照表

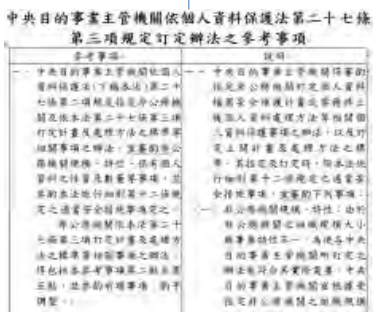
2012年10月1日
《個資法》正式上路！

2013年1月8日　公布《非公務機關之中央目的事業主管機關》


個人資料保護法非公務機關之中央目的事業主管機關

代碼（行政院主計總處行業分類代碼小類）	行業標準分類（參考行政院主計總處之分類）	中央目的事業主管機關
011	農作物栽培業	行政院農業委員會
012	畜牧業	行政院農業委員會
013	農事及畜牧服務業	【畜牧服務業】：行政院農業委員會
021	造林業	行政院農業委員會
022	林產採伐業	行政院農業委員會
031	漁撈業	行政院農業委員會
032	水產養殖業	行政院農業委員會
050	石油及天然氣礦業	經濟部
060	砂、石及黏土採取業	經濟部
070	其他礦業及土石採取業	經濟部
081	肉類處理保藏及其製品製造業	【未辦平內銷】：行政院農業委員會 【已辦有內銷】：行政院衛生署(基於食品衛生管理)
（新增）	屠宰業	行政院農業委員會


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對照表


中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項

除了個資法外，法務部亦公布其他應遵循之法令規範。（如：施行細則、安全維護計畫等）

2012年9月30日　公布《特定目的》與《個資類別》

2013年1月7日　法務部公布《中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項》

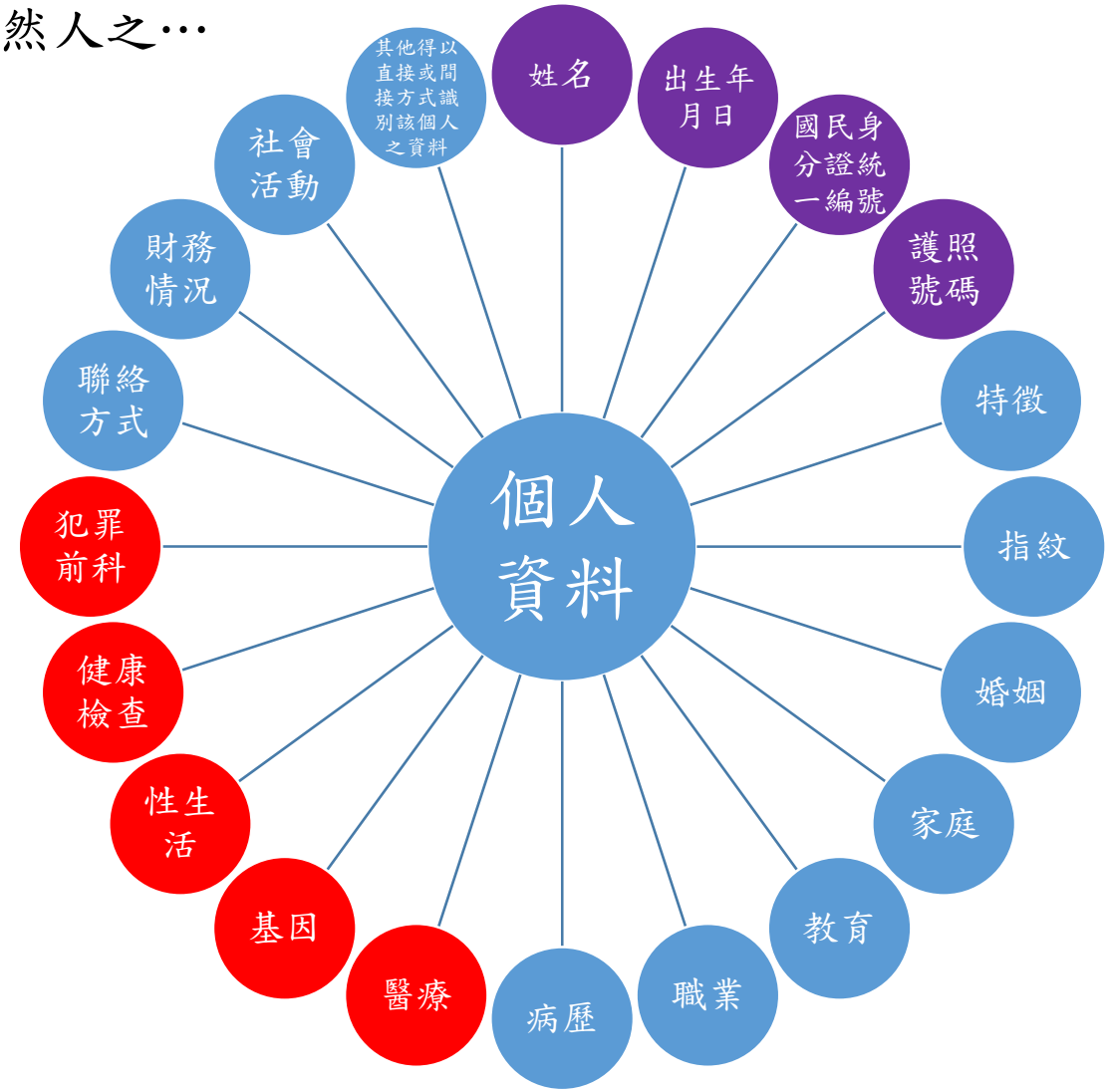
最新修訂

- 104年12月30日修正公布之「個人資料保護法」部分條文，行政院定自105年3月15日施行。
- 本次修正本法第六條至第八條、第十一條、第十五條、第十六條、第十九條、第二十條、第四十一條、第四十五條、第五十三條及第五十四條規定（共12條）。

個人資料保護法重要內容

什麼是個人資料？

- 個人資料係指自然人之…



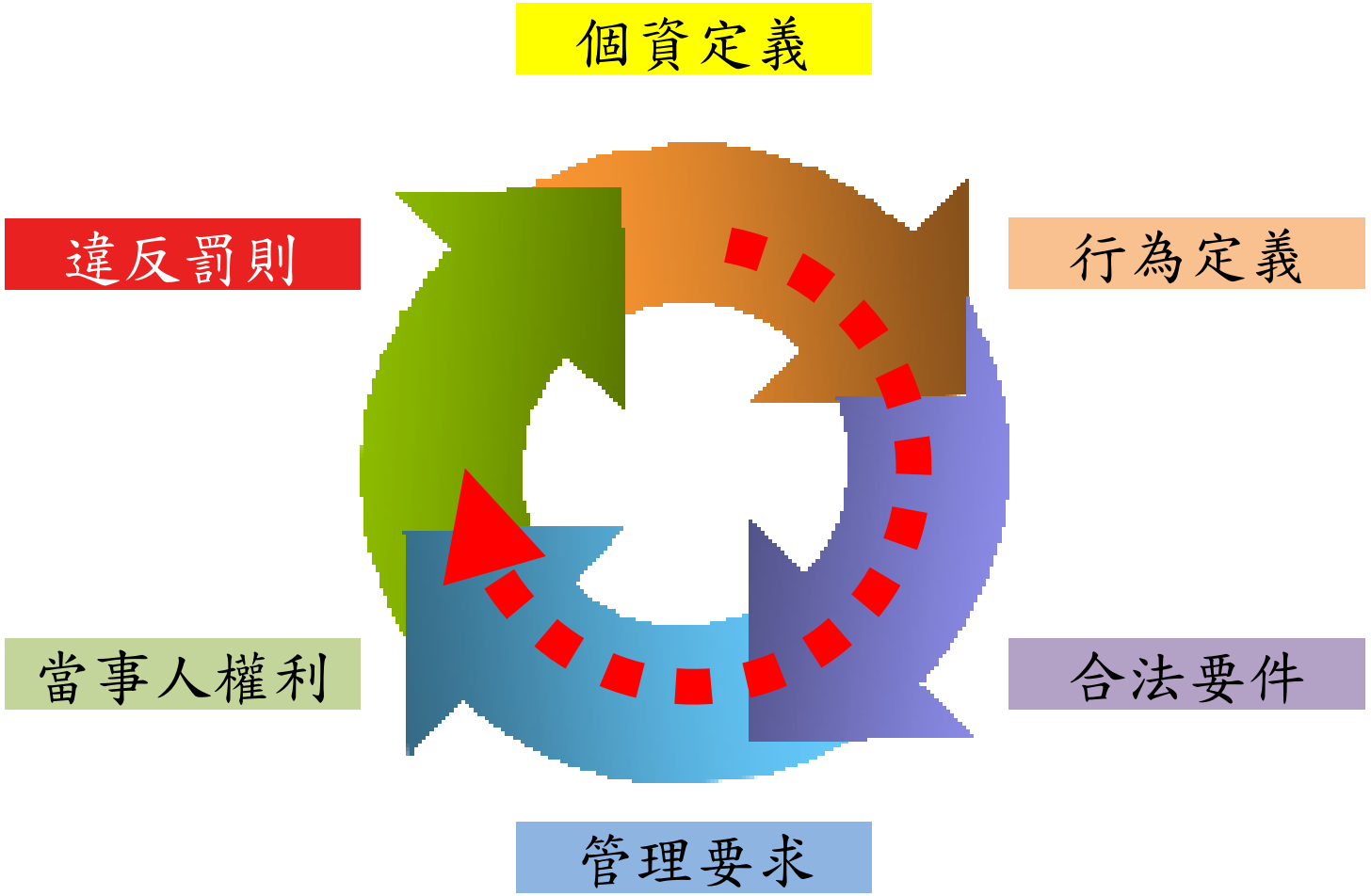
個資作業分類

當事人(蒐集)	單位內部	廠商/其他機關
患者個資	員工個資	廠商/委員/其他機關
告知及蒐集處理要件	正式、約聘雇內/外部個資利用	因業務而公開

委外管理/契約

適當安全維護

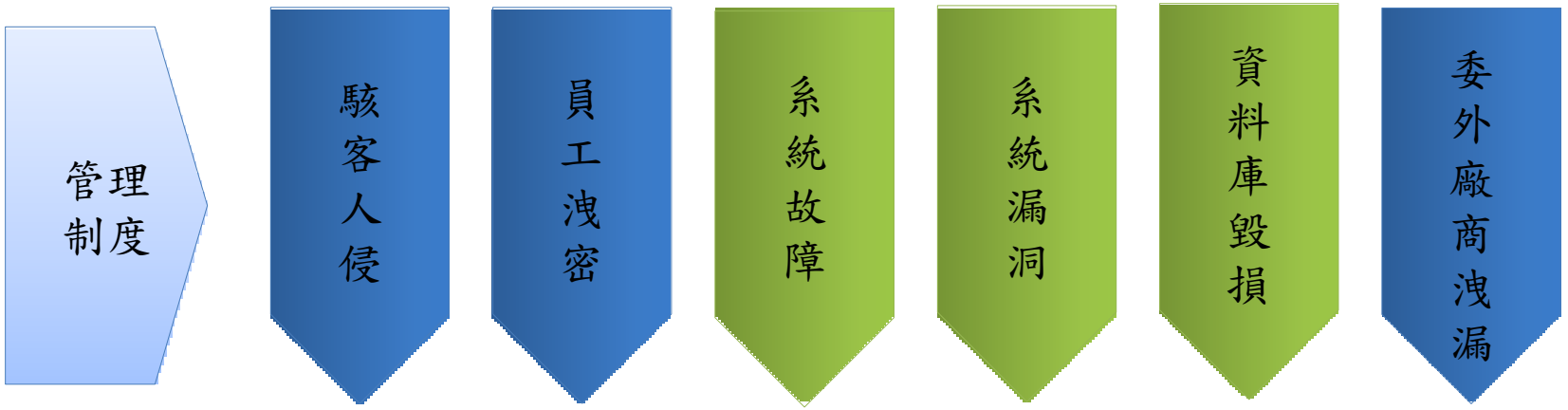
個資法設計主軸

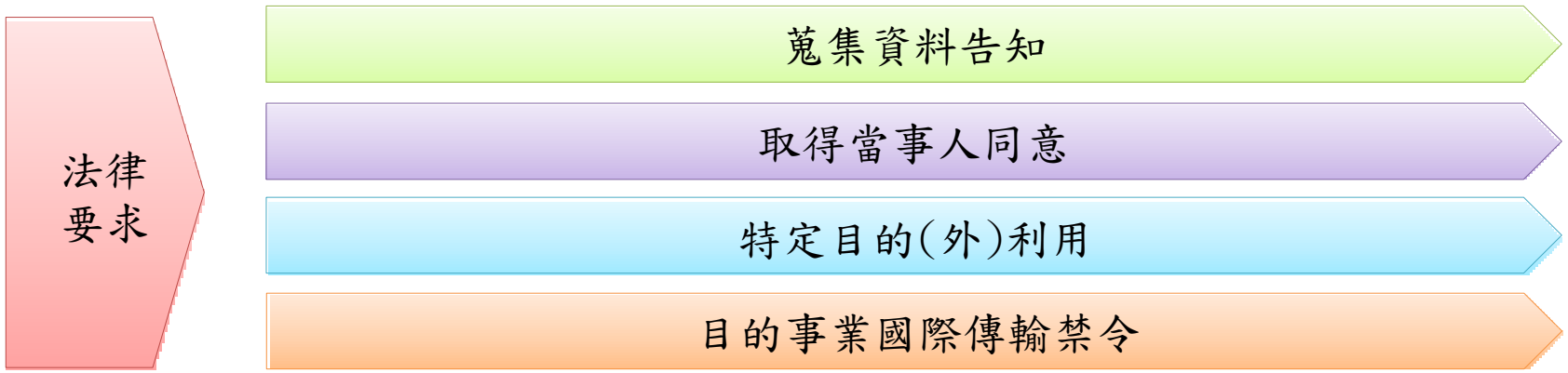


適當安全維護措施-施行細則12

- 適當安全維護措施要求—適當比例為原則
  - 一、配置管理之人員及相當資源。
  - 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、使用紀錄、軌跡資料及證據保存。
  - 十一、個人資料安全維護之整體持續改善。

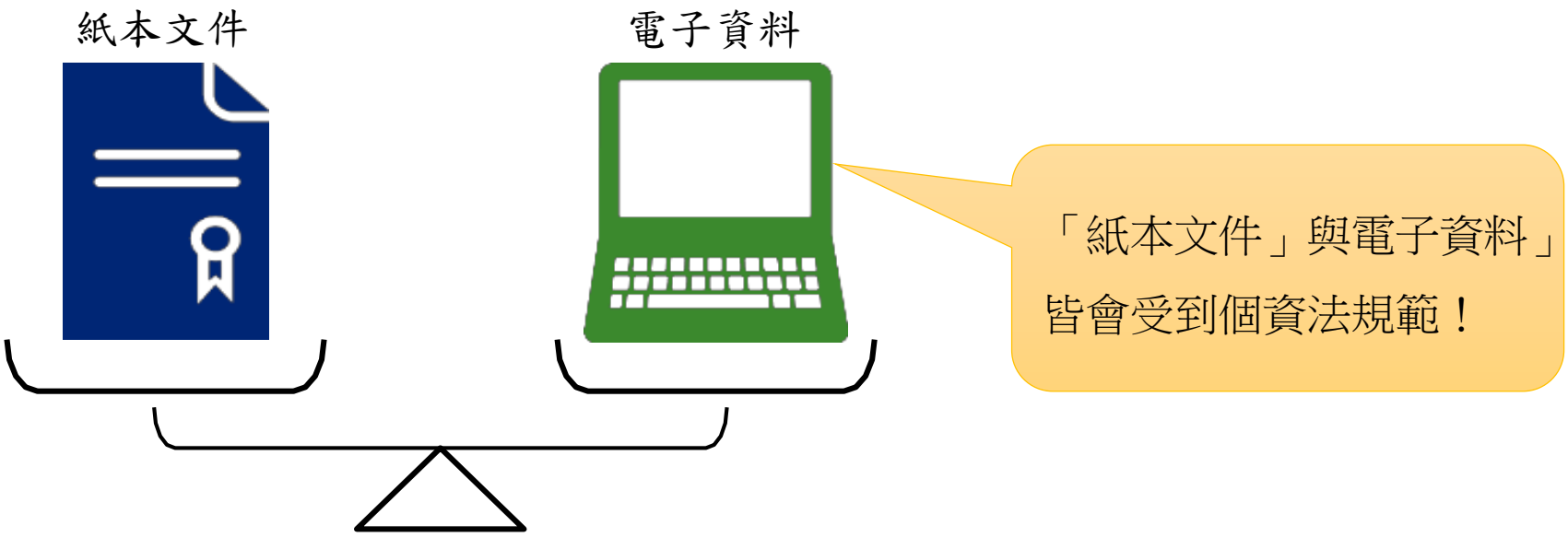
個資法的執行重點


管理制度
駭客入侵
員工洩密
系統故障
系統漏洞
資料庫毀損
委外廠商洩漏


法律要求
蒐集資料告知
取得當事人同意
特定目的(外)利用
目的事業國際傳輸禁令

個人資料保護法重要內容(1)

■ 擴大保護客體



個人資料保護法重要內容(2)

■ 擴大適用主體及領域

任何產業只要會蒐集、處理與利用個人資料者，皆會受到個資法規範！

個人資料保護法重要內容(3)

■ 不定義主管機關

非公務機關	中央目的事業主管機關
醫院	衛生福利部
學校	教育部
電信事業	國家通訊傳播委員會
金融業、證券業、保險業	金融監督管理委員會
廣播業	國家通訊傳播委員會
期貨業	金融監督管理委員會證期局
不動產經紀業	內政部
管理顧問業	經濟部
鐵路運輸業	交通部
宗教組織	內政部
博弈業	交通部

個人資料保護法重要內容(4)

■ 本法排除適用範圍

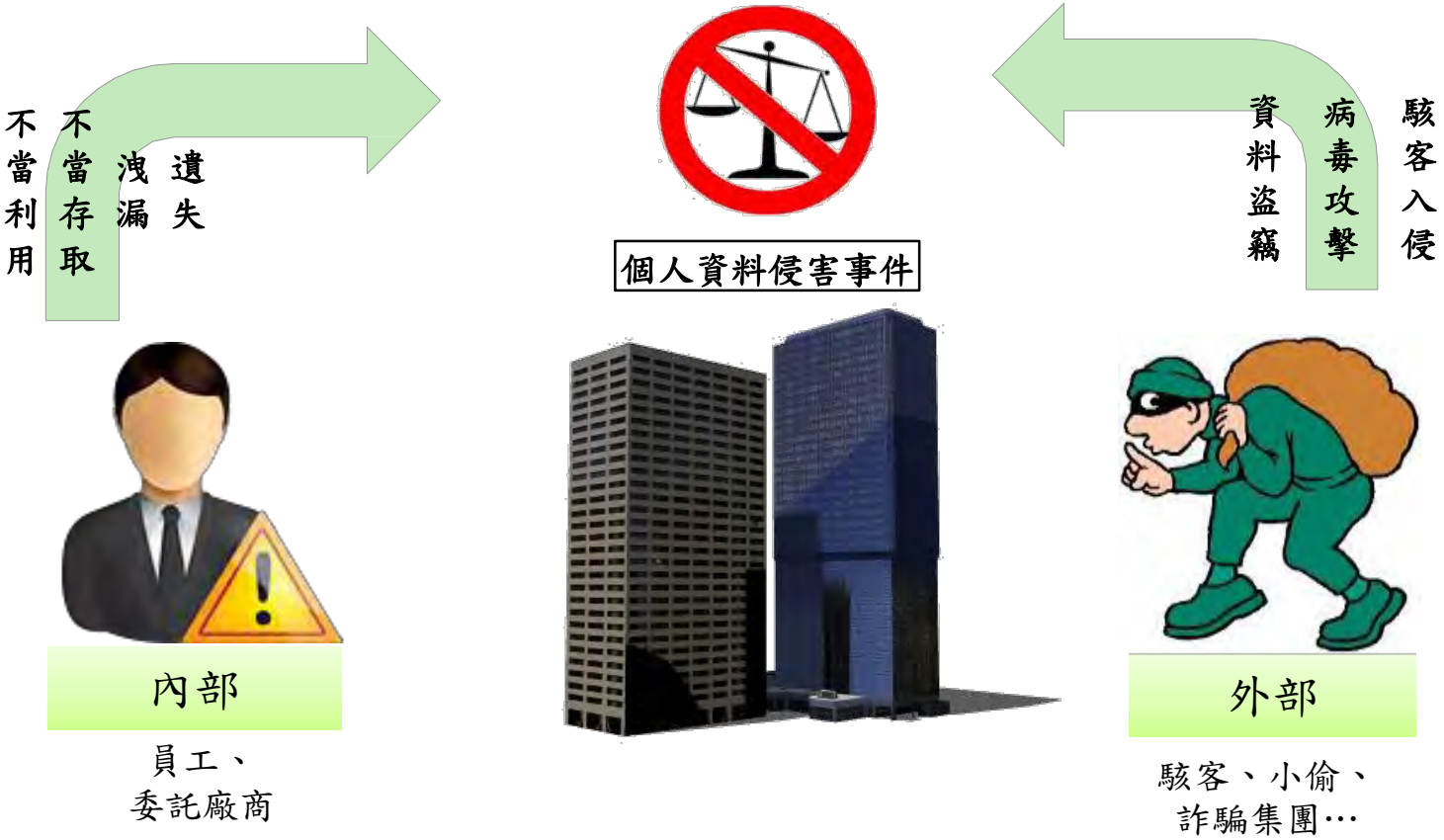
自然人為單純個人（如：社交活動）或家庭活動（如：建立親友通訊錄）

新聞媒體於公開場所或公開活動中採訪所取得之影音資料。

發生個資侵害事件緊急處理

什麼是個人資料侵害事件？

■未經個人資料當事人授權使用或不當蒐集、存取及揭露個人資料而超乎預期使用狀況。



案例：招募作業

電子表單
（空白）

E-mail

人事系統資料庫

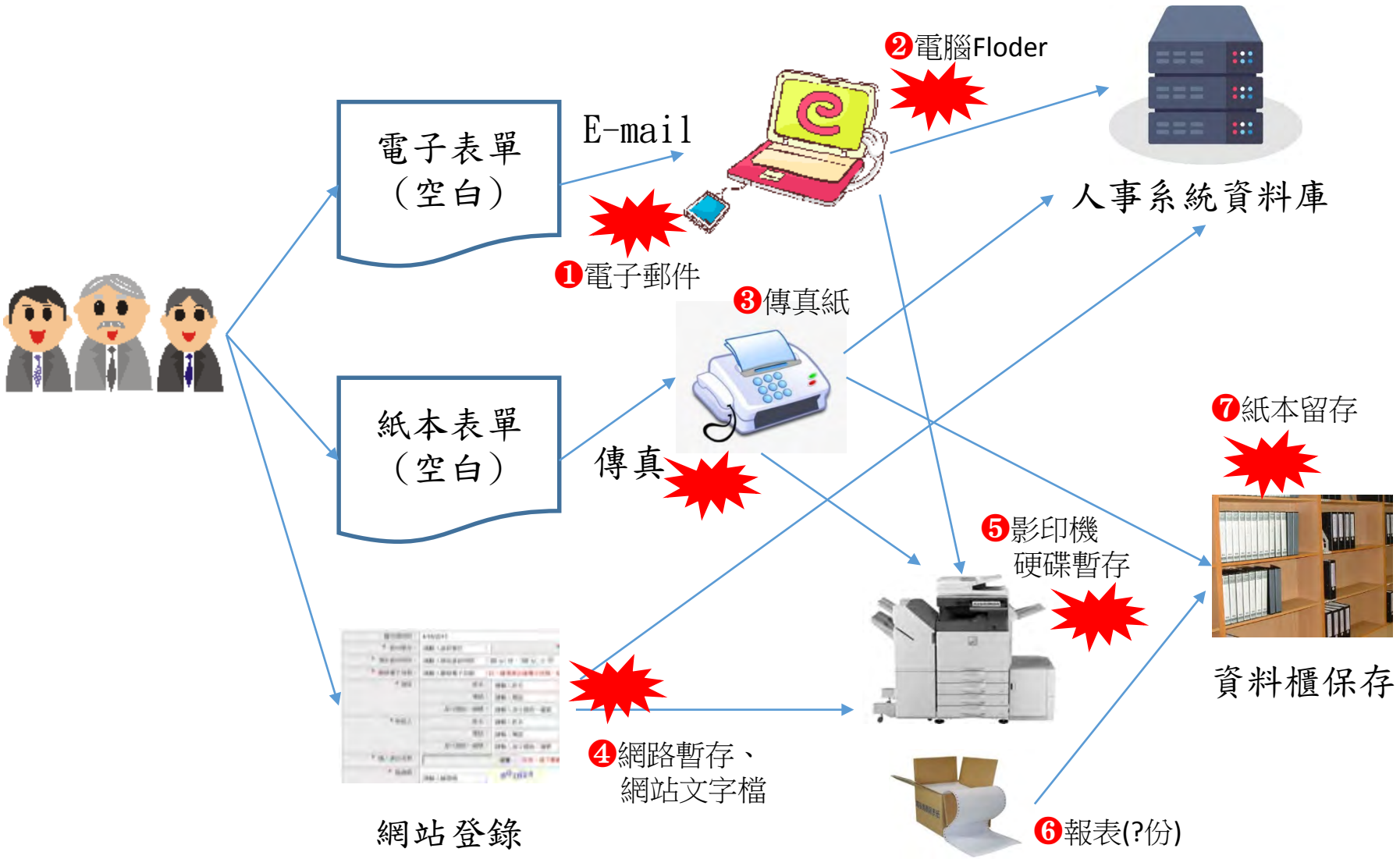
紙本表單
（空白）

傳真

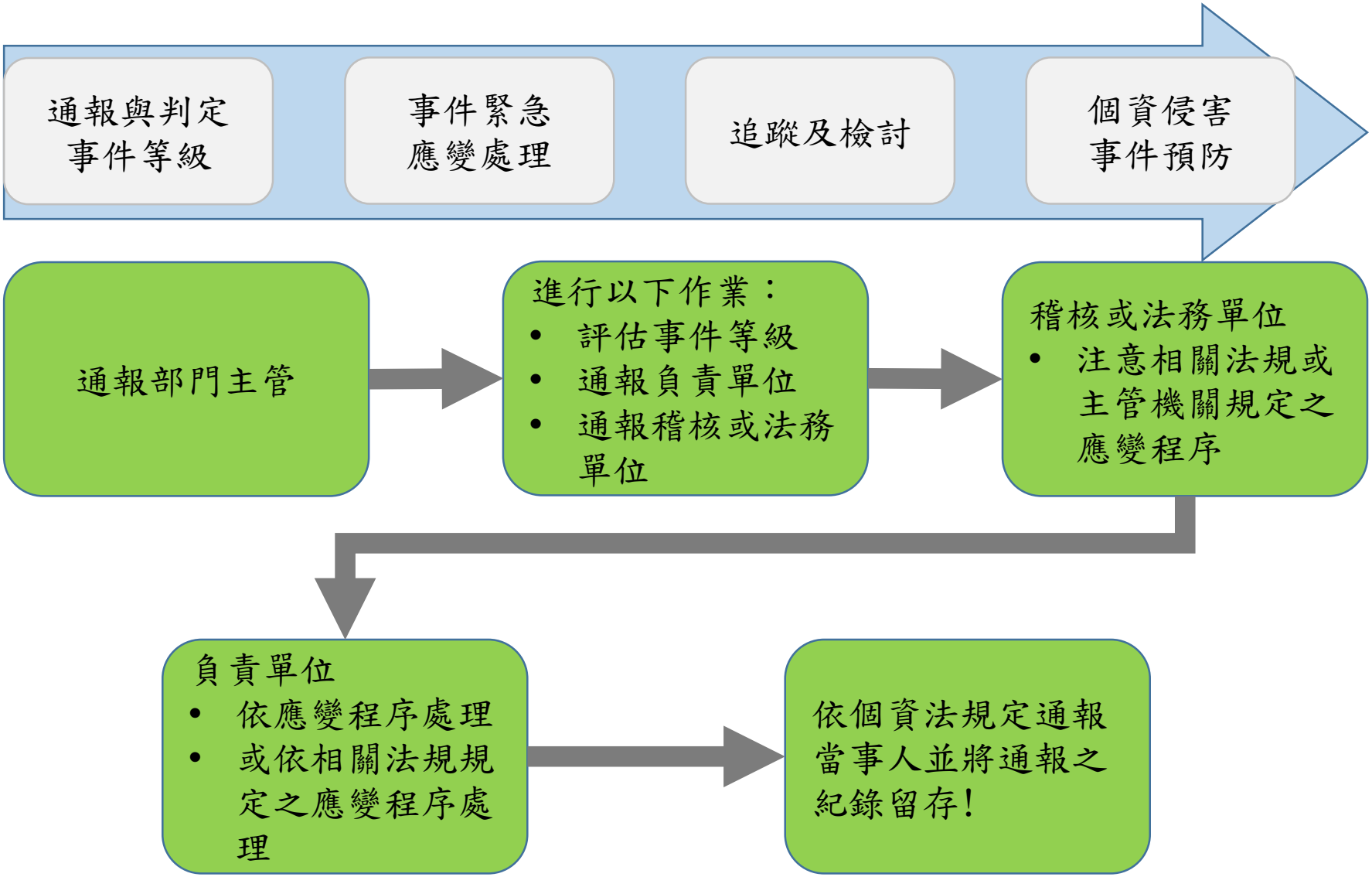
網站登錄

資料櫃保存

案例:招募作業檢查-發現問題



當個資侵害事件發生時


通報與判定事件等級
事件緊急應變處理
追蹤及檢討
個資侵害事件預防
通報部門主管
進行以下作業：
• 評估事件等級
• 通報負責單位
• 通報稽核或法務單位
稽核或法務單位
• 注意相關法規或主管機關規定之應變程序
負責單位
• 依應變程序處理
• 或依相關法規規定之應變程序處理
依個資法規定通報當事人並將通報之紀錄留存!

個資法常見疑義

個資法常見疑義(1)

基於社交禮儀交換名片，是否有個資法適用問題？

- 個資法所稱非公務機關雖包括自然人，惟有關自然人為單純個人社交活動而蒐集、處理或利用個人資料，係屬於**單純個人活動**之私生活目的行為，**依個資法第51條第1項第1款規定，並不適用個資法。**

個資法常見疑義(2)

可以因為各項問卷調查蒐集個人資料嗎？

- 可以因為各項問卷調查蒐集個人資料嗎？

跨行匯款提供受款人帳戶與姓名，是否須告知受款人？

- 不用，依個資法第8條第2項，因為受款人明知帳戶與姓名為應告知內容，故可免為告知義務。

個資法常見疑義(3)

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歲為成年**。
- 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。
- 但已經結婚之未成年人，有行為能力。
- 換言之，已經結婚只未成年人，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。

網路「肉搜」、提供纜人包，是否構成違背個人資料保護法？

- 在網路上發動人肉搜索而「蒐集」來的資訊，絕大部分也都是當事人主動在網路上公開的個資，這部份並無觸法之虞，只要不是透過非法駭客入侵所取得，就沒有問題。

個資法常見疑義(4)

當事人要求刪除就得照做嗎？可以拒絕嗎？

- 參考《個人資料保護法施行細則》第21條。
- 因執行職務或業務所必須或經當事人書面同意者，不在此限(可不刪除)：
  - 有法令規定或契約約定之保存期限。
  - 有理由足認刪除將侵害當事人值得保護之利益。
  - 其他不能刪除之正當事由。

當事人若要求刪除，應如何處理才算刪除？

- 刪除之定義：
- 指使已儲存之個人資料自個人資料檔案中消失。
- 只要有上述事由，即可不刪除。

安全防護從現在做起

從現在做起

識別業務範圍的法令依據

- 請針對所負責的業務，整理相關的法令依據及可能之個資檔案，包含：
- 法令規範可以蒐集的資料(如：員工健康檢查)；
- 法令規定可以給的資料(如：配合檢警調查)；
- 法令規定不可刪除的資料(如：離職員工資料的保存年限要求)。

留意個資的流向與管理方式

- 請時時留意身邊各種可能的個人資料，以及相關的管理方式是否適當，如：
- 傳真機的資料是否隨時取回；
- 包含個人資料的紙本是否有適當的銷燬而未被當成回收用紙使用。

實體紙本/電子檔案控管(1)

- **是否有訂定個人資料保存期限之規定？**

　　各單位蒐集之個人資料，應訂定各類資料保存期限或保留期間；若有法令規定者，保留期間不得低於法令要求；且非有特殊理由，原則上不得將個人資料檔案之保存期限定為永久保存。

實體紙本/電子檔案控管(2)

- **實體紙本**和**電子檔案**各有哪些保管要求？

實體紙本保管

1. 含有個人資料之實體紙本應由專責人員保管，於無人員看管時，應妥善收存於上鎖之箱櫃或安全處所中，並由專責人員保管鑰匙。
2. 使用影印機、印表機、傳真機或多功能事務機後，應立即將含有個人資料之實體紙本取走。

電子檔案保管

1. 公用資料夾、公用個人電腦不得存放含有非業務所需個人資料之電子檔案。
2. 業務所需之個人資料檔案存放於個人電腦、公用資料夾、公用個人電腦中時，個人資料檔案於使用完畢後應予以刪除。
3. 應評估個人電腦、公用資料夾、公用個人電腦之電子檔案備份及加密之必要性，儲存備份資料之媒體亦應以適當方式保管，並依各單位相關規定辦理，以確保備份之有效性。

實體紙本/電子檔案控管(3)

- **銷毀**紙本個人資料時，是否有程序可遵循？

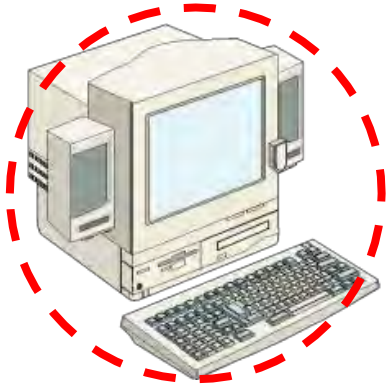
文件銷毀時，除授權自行利用碎紙機徹底粉碎之情況外，銷毀之封箱文件應由各單位保留相關紀錄。

除有其他銷毀規定可遵循之單位外，各單位應由指定人員收集單位內待銷毀之文件，裝箱後交予專責人員，並陪同合作廠商進行銷毀。

運送及銷毀過程須全程陪同監控且拍照留存備查，確認所有銷毀文件與資料均已確實銷毀並無外流之情況後，填寫相關表單，交付銷毀廠相關人員簽署蓋章。

銷毀程序完成後，須將銷毀拍照之檔案併相關表單，送相關單位覆核後留存備查。

日常作業應注意事項(1)

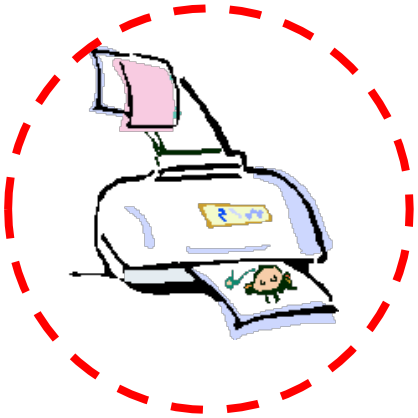


- 個人電腦安全防護
- 電腦閒置時，應設定螢幕保護程式或關機
- 不應將使用者之帳號密碼記錄於紙本
- 重要的電腦需有妥善的保護措施

- 儲存媒體應妥善保管
- 使用、移動及存取多媒體應遵循管制程序
- 報廢的儲存媒體需確實銷毀

日常作業應注意事項(2)

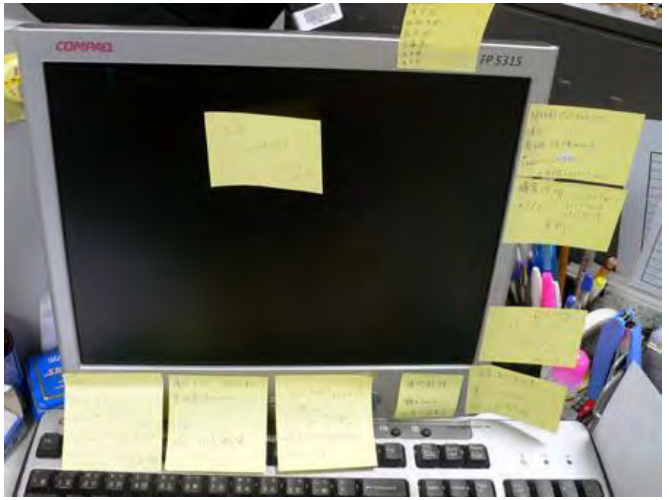
- 離開座位時，機密文件不應置於辦公桌
- 下班前需清理工作場所



- 傳真、列印個人資料時，應隨時取回 欲丟棄之紙本個人資料是否有適當的處裡，如：碎紙機、集中銷燬

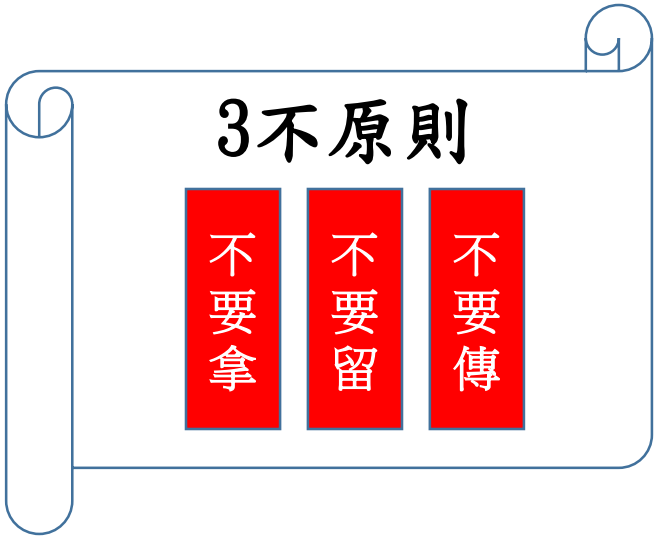
日常作業應注意事項(3)

- ✓ 需包含英文大小寫、數字及特殊符號。
- ✓ 密碼需要 8 個字以上。
- ✓ 不可以另外寫下或存在電腦檔案裏。
- ✓ 避免使用個人公開的資料，如生日、電話號碼與身分證字號等。



個人資料管理建議事項

- 經識別的個人資料，都必須評估其風險，並依其風險大小設置對應之安全控管機制，故個資留越多，組織所要花的控管成本將越高。
- 故我們建議：



資訊安全管理建議事件

- 設定安全的系統密碼。
- 安裝防毒軟體並定期更新。
- 定期更新視窗作業系統。
- 不任意開啟可疑郵件及檔案。
- 使用防火牆。
- 關掉不必要的服務。

結語

- 國內外個資外洩事件之影響與衝擊宜正視及有效因應。
- 個資法通過後對政府機關造成影響與衝擊，相關權責主管機關應妥善研擬相關配套措施。
- 資訊安全與個資保護是一體兩面，政府資安工作除健全的基礎設施外，最重要的是先做好個人的資訊安全，人人做好資訊安全第一線防護，機關資訊安全就能得到保障，進而提升我國整體資訊安全及個資防護。

THE END