個人資料保護法與案例演練宣導

101年8月13、14日
劉志銘 資深經理
NII 產業發展協進會

個人資料，無所不在


帳單地址
電子郵件信箱
帳戶資料
電信/網路
服務提供業者
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
BANK
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
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
學籍資料
人事資料
註冊/報名資料
家長會聯絡
BUS
SCHOOL
學校 / 補習班
社區活動中心

隱私權問題...

- 兆豐銀行電腦銷毀委外處理，因過程無監控，導致部分電腦的硬碟資料外流到二手市場，金管會開罰兆豐銀行200萬元罰鍰-2012/06/01
- 減肥名醫，洩漏緋聞女主角孫仲瑜病例，遭台北市衛生局約談－2009/11/20
- 東森休閒育樂公司離職經理，涉嫌從公司帶出7萬多筆客戶資料，並分別賣出 － 2008/1/24
- 桃園一家私人診所停業後，將過去病人的病歷，稱斤論兩賣給資源回收廠商 － 2006/3/27

3

新科技與新應用會產生風險嗎?

資料
http://daman.cc
my/term/20(

資料來源: http://www.switched.com/2010/06/21/in-a-nutshell-what-are-qr-codes/

新科技與新應用會產生風險嗎?(續)

資料來源:http://betakit.com/2012/03
to-make-scanning-qr-codes-a-profi

資料來源:
http://techorange.com/2011/03/22/great-qr-code-strategies/

1.切勿亂掃描來路不明
QR Code
2.掃描QR Code時應啟動
防護機制
3.避免於公共網路處理含
個人資訊的網站或事務

日本地下鐵的 QR Code乘車一日券。
(Source http://www.nic-nagoya.or.jp/en/e/archives/2533

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及安全處理與使用方式，作好適當的刪除與銷毀」。

簡報大綱

- 個人資料保護法基本認知與重要條文說明
- 情境案例
- 給學校的建議

個資法基本認知

- 立法目的
- 個資法架構
- 個人資料的定義
- 誰適用於個資法?
- 哪些個資不受個資法保護?

個人資料保護法

- 電腦處理個人資料保護法
  - 84年8月11日制定公布。
- 個人資料保護法
  - 99年5月26日由總統府正式公布修正之全文，施行日期由行政院定之。
- 個人資料保護法施行細則草案預告
  - 100 年 10 月 26 日法務部預告「電腦處理個人資料保護法施行細則」修正草案

個人資料保護法

施行細則修正方向

- 修正「刪除」的定義。

  刪除不等於銷毀，如果是紙本資料的刪除，只要將資料塗抹掉即可，如果是電子資料的刪除，則是按下Delete鍵就可以。

- 明定委託人應對受託人為適當的監督。

  委託人在尋找委外廠商時，可將資安措施、內部管控制度、隱私權的教育訓練等三點列為評估因素，在委外廠商履約過程中，也要適時地監督受託人，因為受託人（委外廠商）若發生資料外洩，委託人同樣得擔負起責任。

- 書面的定義。

  書面不一定只能是紙本文件，只要內容可以完整呈現、沒有被竄改，並可於日後取出供查驗者，在蒐集者及個資當事人同意下，就可使用電子文件，如：E-mail。

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

尋求個人資訊隱私權與資料合理流通之利益平衡。

個資法架構

個人資料保護法
(共56條)

第一章　總則

第二章
公務機關對個人資料
之蒐集、處理及利用

第三章
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

第五章　罰則

第六章　附則

何謂個人資料？

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

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。
	網路聯絡方式：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。

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
  - 特種個人資料除個資法第 6 條所定情形外，不得蒐集、處理或利用。

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。(此部份尚未確定)
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。

何種情況下才能夠蒐集特種個資?

個資法第 6 條

- 只有在下列情形時，才能夠蒐集特種資料：

法律明文規定。

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。

當事人自行公開或其他已合法公開之個人資料。

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。

案例：教育部提供各校使用「全國不適任教師查詢系統」作為新進人員資料查詢，是否合法?

判斷「全國不適任教師查詢系統」內的個人資料類別。

該查詢系統內含的個人資料為犯罪前科，屬於個資法所定義的特種資料。

確認是否符合個資法第 6 條可以蒐集特種個資的情況。

該系統為教育部、縣市主管機關、各級學校為執行教育人員任用條例第26條、第30條所定教師任用相關程序之職務，並履行同法第31條第1項所定任用限制、應予解聘或免職之義務所必要，應可認屬符合個資法第6條第1項第2款所定之「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」。

此案例中，除符合【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】外，還要符合【且有適當安全維護措施。】之規定，方能夠進行特種資料的蒐集、處理與利用。

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。

個人資料保護法的適用於個人嗎? 保護對象為?

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

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

個資法重要條文

1) 特定目的
2) 告知義務
3) 安全維護事項
4) 罰則

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加值網路業務
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
退憮基金或退休金管理	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

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。

蒐集個資時，應告知當事人哪些事項?

直接蒐集向當事人蒐集個資、以及間接向當事人蒐集個資的情境，個資法有不同的告知義務規定。(§8, §9)

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。

案例討論:

興興科技書面同意書

1	興興科技股份有限公司取得您的個人資料，目的在於個人資料保護法及相關法令之規定下，依本公司隱私權保護政策，蒐集、處理及利用您的個人資料。
2	您可依您的需要提供以下個人資料：姓名、出生年月日、國民身分證統一編號、連絡方式(包括但不限於電話號碼、E-MAIL或居住地址)或其他得以直接或間接識別您個人之資料。
3	您同意本公司以您所提供的個人資料確認您的身份、與您進行連絡、提供您本公司及關係企業或合作夥伴之相關服務及資訊，以及其他隱私權保護政策規範之使用方式。
4	您同意本公司利用您的個人資料之期間為，自即日起至您與本公司間所有契約均終止後五年止，利用地區為全球。
5	您可依個人資料保護法，就您的個人資料向本公司 (1)請求查詢或閱覽、(2)製給複製本、(3)請求補充或更正、(4)請求停止蒐集、處理及利用或(5)請求刪除。但因本公司執行職務或業務所必需者，本公司得拒絕之。
6	您可自由選擇是否提供本公司您的個人資料，但若您所提供之個人資料，經檢舉或本公司發現不足以確認您的身分真實性或其他個人資料冒用、盜用、資料不實等情形，本公司有權暫時停止提供對您的服務，若有不便之處敬請見諒。
7	您瞭解此一同意符合個人資料保護法及相關法規之要求，具有書面同意本公司蒐集、處理及利用您的個人資料之效果。

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)

個資法規定的安全保護相關規定有哪些?

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) 。

- 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

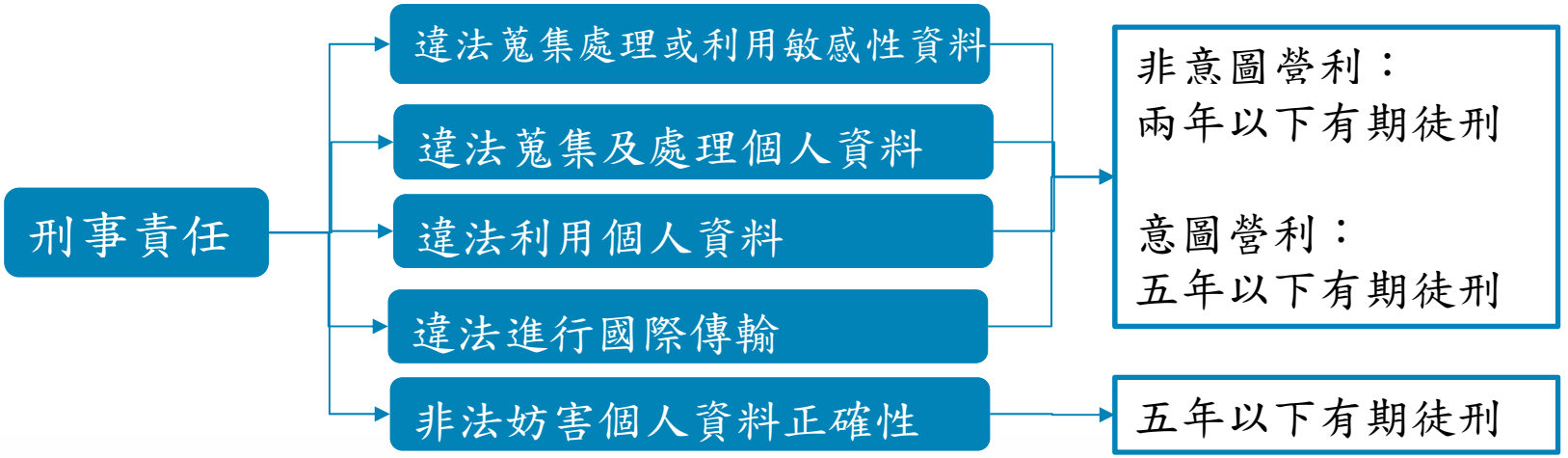
1	成立管理組織，配置相當資源。
2	界定個人資料之範圍。
3	個人資料之風險評估及管理機制。
4	事故之預防、通報及應變機制。
5	個人資料蒐集、處理及利用之內部管理程序。
6	資料安全管理及人員管理。
7	認知宣導及教育訓練。
8	設備安全管理。
9	資料安全稽核機制。
10	必要之使用紀錄、軌跡資料及證據之保存。
11	個人資料安全維護之整體持續改善。

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。

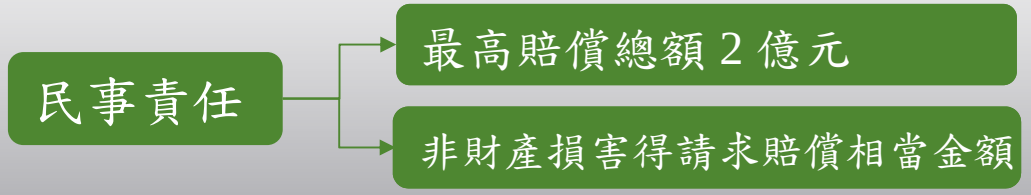
此11項安全措施內容為參照英國BS10012:2009 及日本JISQ15001:2006 等個人資料管理系統之規範，以P-D-C-A 循環之概念予以建立。

若違反個資法，只要罰錢就可以了嗎?

公務機關(公立學校)之法律責任

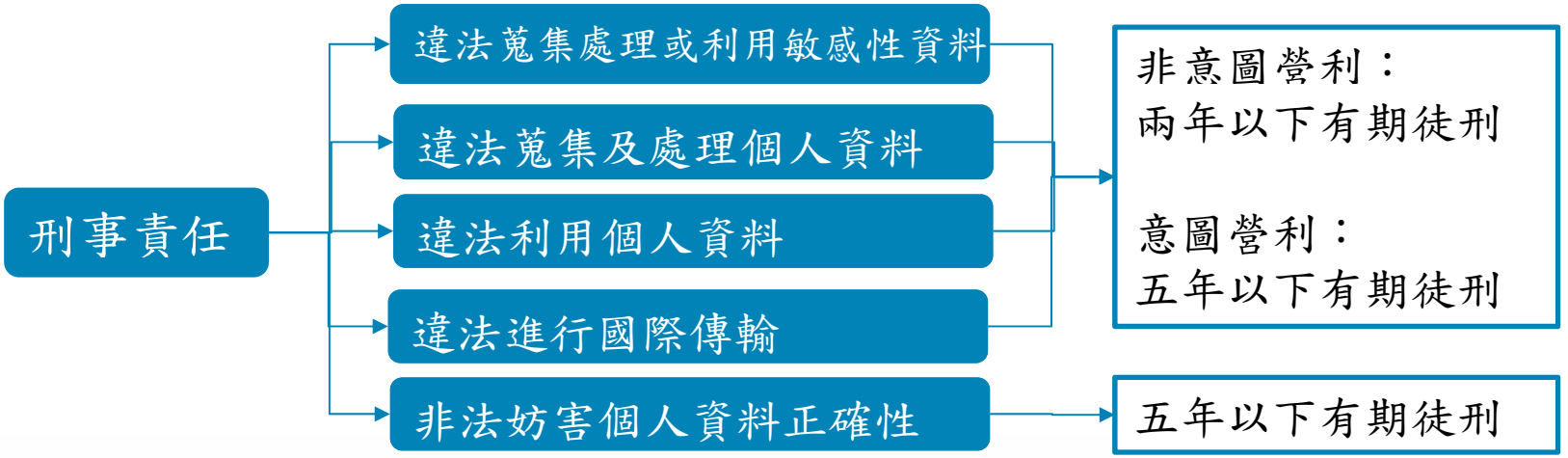


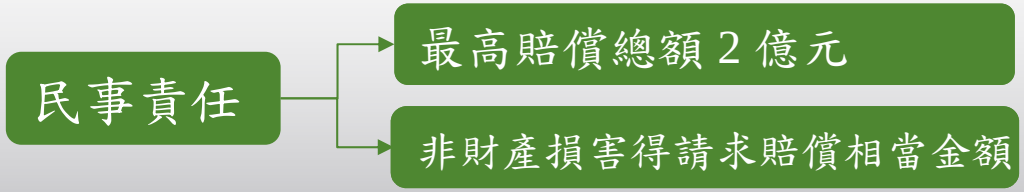
公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)



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)

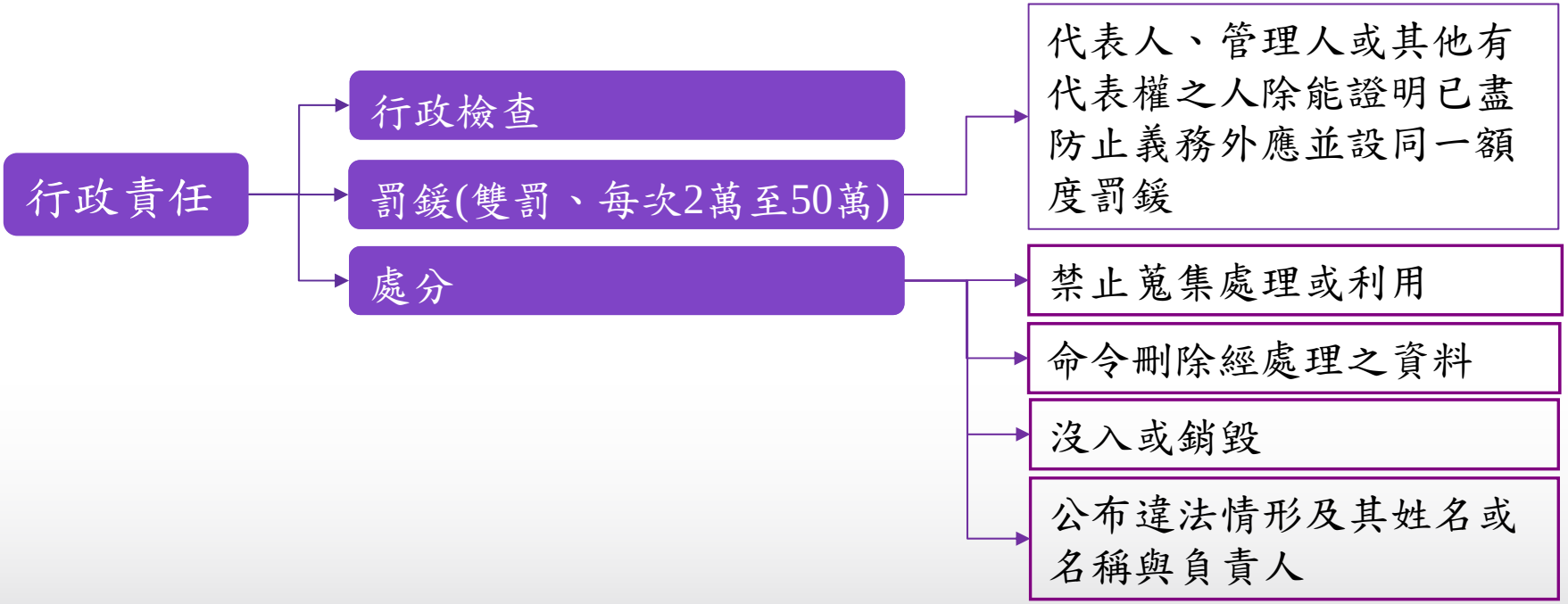
非公務機關(私立學校)之法律責任





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(私立學校)之法律責任 (續)



課程大綱

- 個人資料保護法基本認知與重要條文說明
- 情境案例
- 給學校的建議

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
- 會計帳務資料

案例：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：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：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：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：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：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：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：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。

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。

國中校務行政系統個資外洩新聞

遭駭客入侵○○教育局加強網路機密維護

【大紀元6月25日報導】（中央社記者陳朝福二十五日電）○○市國中校務系統被駭客入侵，學生基本資料被竊，○○市政府教育局已與負責廠商聯繫，移除入侵程式，也將加強維護網路資訊機密。

教育局今天表示，○○市國中校務行政系統委由廠商服務，這次國中學生資料被駭客竊取，是這程式遭駭客侵入，所竊資料供補習班招生、宣傳、寄送資料等用途，目前調查尚無其他用途。

教育局已與負責廠商聯繫，將入侵程式移除，並修補程式漏洞，並加強網路安全，以維護學生權益。

課程大綱

- 個人資料保護法基本認知與重要條文說明
- 情境案例
- 給學校的建議

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。
- 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。

如何進行個人資料保護?


推動個人資料保護
及管理制度
實施個人資料管理及
保護教育訓練
評估可行之個人資料管理
及保護之技術方案
滿足基本
個人資料保護

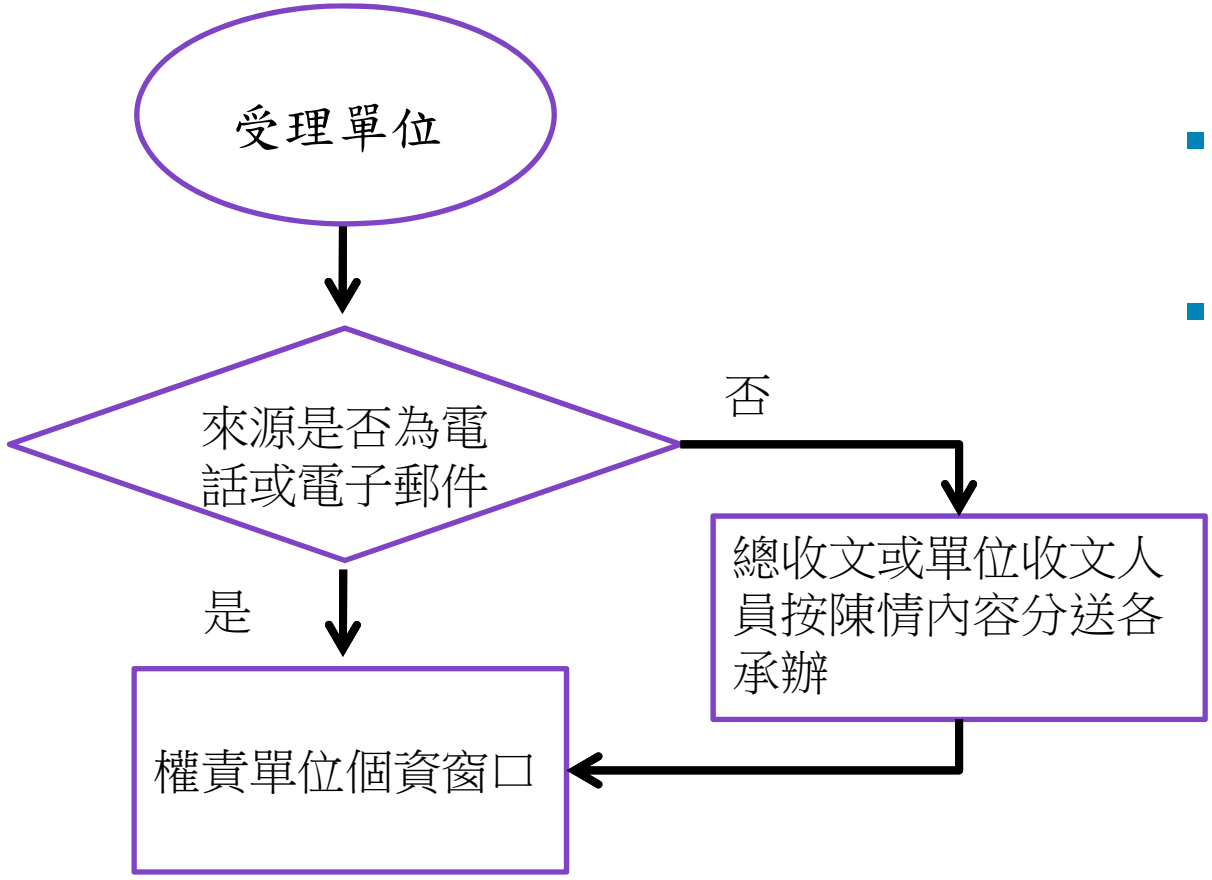
個人資料保護
案例情境演練

情境案例討論:

2012年XX月XX日一位同學寫信給某大學校長表示有朋友在網路上搜尋資料，意外發現該同學手機號碼及連絡資料在GOOGLE搜尋引擎上被找到，其中資訊包含系別年級、學號、姓名、電話及email，同學希望學校能解決此事。

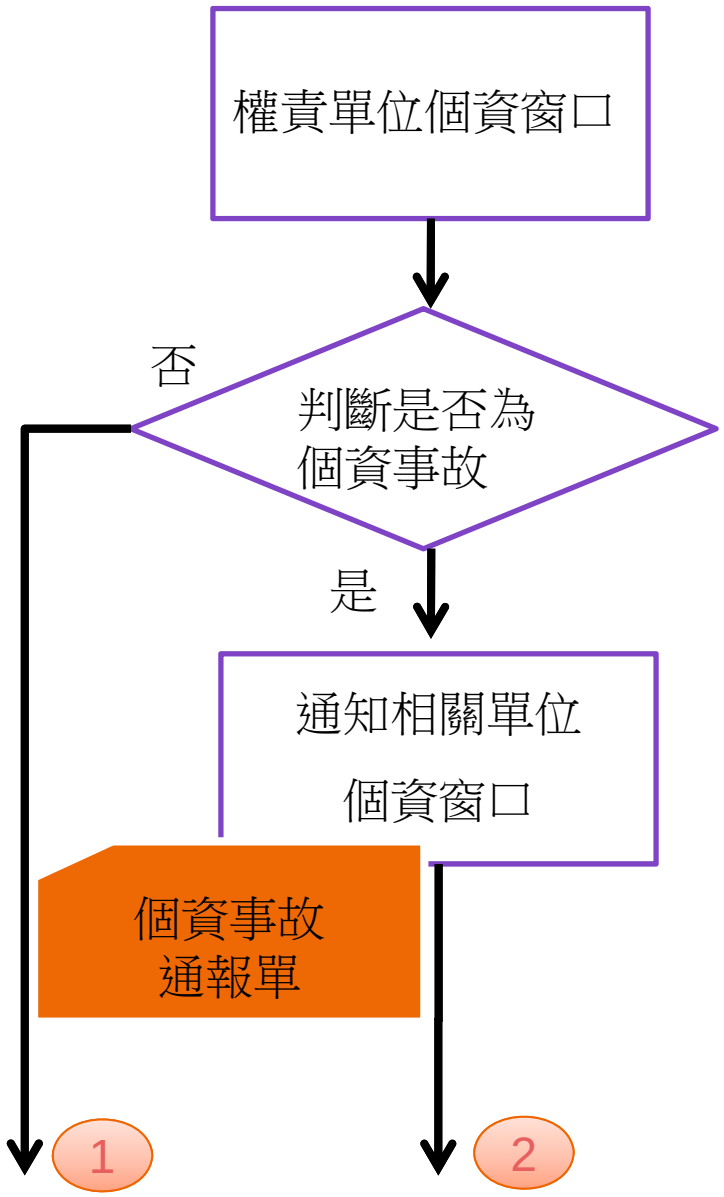
個資事件應變處理流程

信函、陳情書、電子郵件、傳真、電話等各種個資事故訊息來源



- 1.校長轉寄個案信件請秘書室協助處理
- 2.秘書室依據個案內容通知業務權責單位
- 3.業務權責單位個資聯絡窗口，協請計中實施緊急應變處理及原因分析，並請學校法務專家判斷是否違反個資法，同時循管道先行安撫當事人，相關處理記錄於「個資事故通報單」。

個資事件應變處理流程(續)

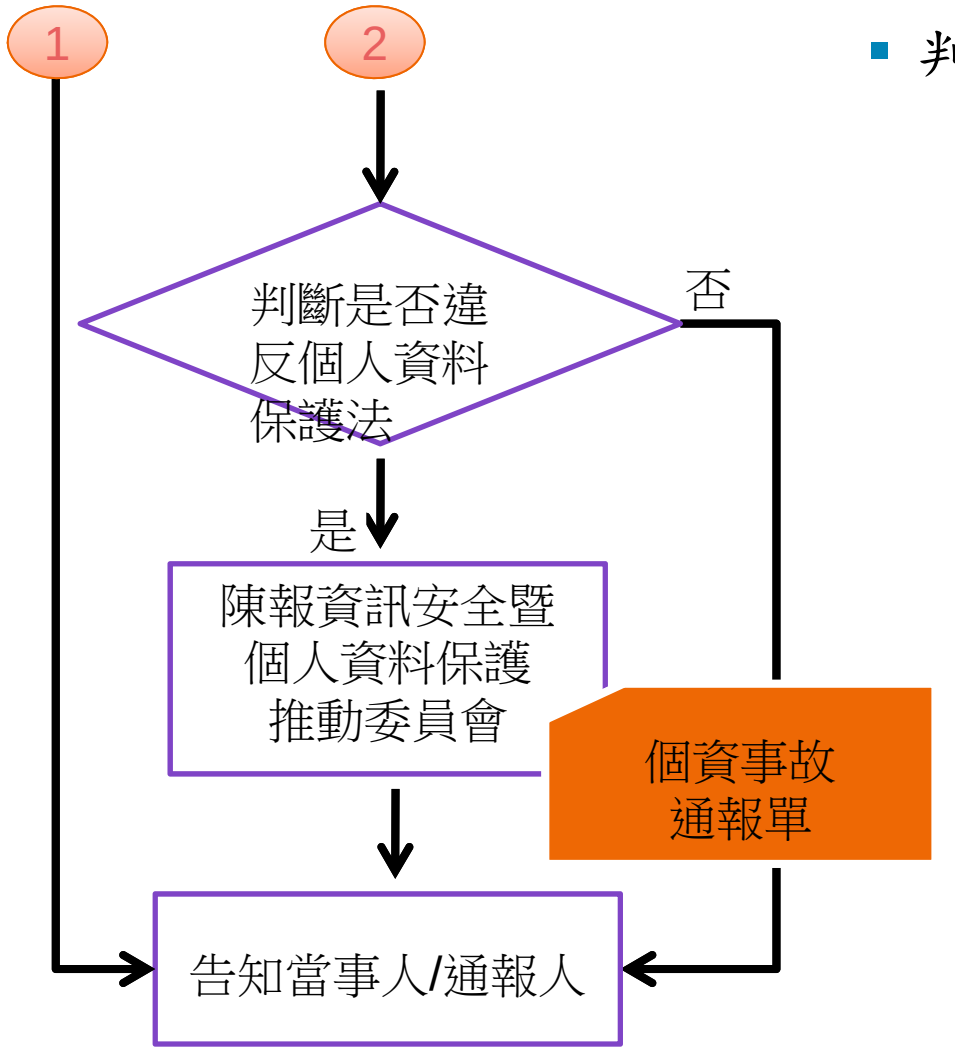


- 應變措施：
  - (1).將個資外洩之IP暫時停權，實施實體隔離。
  - (2).實施資料證據保留(如截取畫面等)
  - (3).通知系統管理者將其個資網頁移除。
  - (4).請系統管理者檢查系統，是否仍有其他資安漏洞。
  - (5).Mail及公文至Google公司,請Google將cache的網頁移除，避免事件再延續擴大。
  - (6).製成個資外洩案例，向全校教職員工生宣導。

個資事件應變處理流程(續)

- 個資事故根因分析：實施根因分析，避免類似事件繼續發生。
- 經權責單位個資窗口與個案發生事件單位及計中處理人員瞭解後發現，網站管理人員無法釐清資料為誰轉成文字檔(.txt)，而此網站由委外廠商開發及維護，廠商也表示不知情。

個資事件應變處理流程(續)



- 判斷是否違反個資法：
  - 發現人未循法律途徑，還是違反個資法，但可能無求償問題。
  - 發現人循法律途徑，則依據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。
  - 委外廠商部分:
    - 個資法第四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。

個資事件應變處理流程(續)

- 4.陳報資訊安全暨個人資料保護推動委員會
  - 向召集人報告個資事件處理情形與矯正預防處 理記錄於「個資事故矯正預防單」。
- 5.回覆當事人/通報人

個資事件應變處理流程(續)

- 矯正預防
  - (1).從個資處理生命週期(蒐集、處理、利用、傳輸、銷毀)考量，若單位要提供資料給其他單位(如委外廠商)應提出申請，並留存相關紀錄(如填寫個人資料使用資訊服務申請表)。
  - (2).單位實施資料傳遞時應使用適切之加密機制。
  - (3).單位若與委外廠商有合約關係，應於合約內訂定安全控管要求如簽署保密切結，若系統由廠商開發則應實施安全檢測(如滲透測試或弱點掃描)，並有測試報告。
  - (4).實施教育訓練，提高教職員工生個資法制觀念與個資保護意識。

個資事件應變處理流程(續)

- 後續建議:
  - (1).請各單位檢視含有個資資訊的應用系統應實施安全檢測(檢測是否有漏洞或弱點)。
  - (2).網頁式的應用系統應建立資料傳輸加密機制。
  - (3).建議可考量建置安全管控措施，如防火牆。
  - (4).若機敏資訊須由廠商輸入系統，則應與廠商簽訂保密切結與安全條款，資料匯入完後應立即刪除/銷毀，資料傳輸過程應使用適切之加密機制。
  - (5).廠商或人員實施資料變更應提出申請，保留相關紀錄。
  - (6).資料庫機敏資訊部分之欄位可考量加密。
  - (7).透過資訊系統所公開顯示之敏感性資料欄位，應採取適當之遮蔽方式(如身分證字號A123******)。

個人資料保護措施提醒

本校各單位辦公環境下班無人時，門、窗須上鎖或設定門禁。

處理完之個人資料檔案(紙本、電子)，若無需保留應立即絞碎或刪除(電子檔案應確實清除「資源回收筒」)，含有個人資料之報廢紙張不得回收及再利用。

針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖，以避免外洩。

伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護；自行啟動螢幕保護程式的時間設定應不超過10分鐘。

個人電腦(含筆記型電腦)應設密碼保護，密碼須英數字混合(密碼複雜度)且不得與帳號名稱相同，長度至少6碼，並不得與前次設定相同；原則上密碼至少3個月變更一次，最長不得超過6個月變更。

簡報完畢，敬請指教