

個人資料保護法與案例宣導



資深顧問師 彭至賢 (Sam Peng)

ISO27001/BS10012/ISO9001 主導稽核員

PMP&APMP 國際專案管理師

TTQS 國家訓練品質計畫評核委員

Mobile: 0952-695460

E-mail: sam@safelink.com.tw

Safelink 博創資訊科技股份有限公司



個人資料，無所不在





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



個人資料保護的重點

- 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？



你準備好了嗎？

- 你的業務需要處理個人資料嗎？
- 你的電腦裡有多少電子檔案嗎？
- 你有多少檔案裡面有個人資料？
- 你有多少極高風險的個資檔案？
- 如果以上的問題你都無法回答，
你認為如何可以保護個人資料？

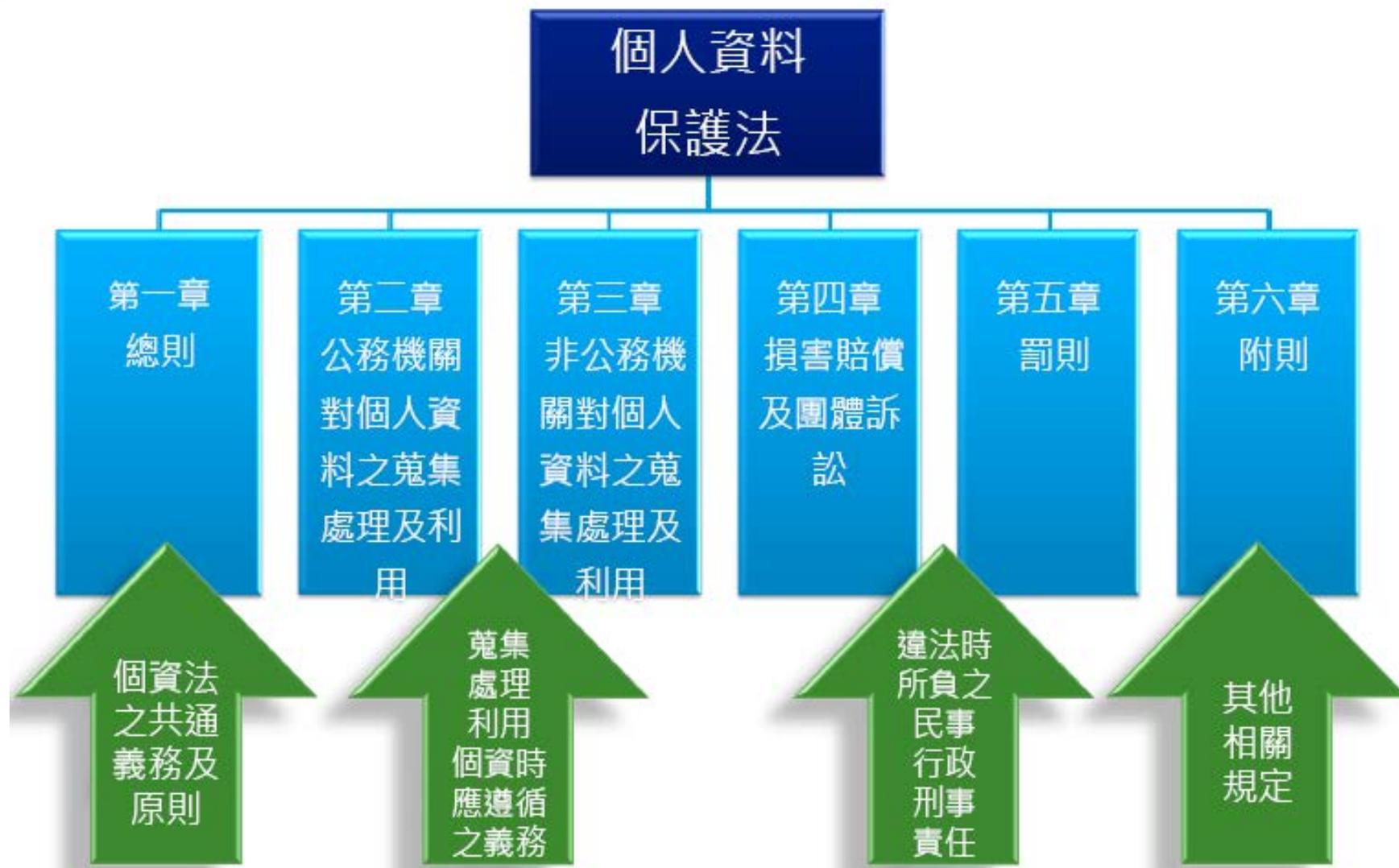


個人資料保護法

- 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
 - 我國個人資料保護法自101年10月1日施行迄今已3年有餘，為了讓個資法更能符合社會現況，立法院於104年12月15日完成三讀修正，定自105年3月15日施行。
 - 修正日期：104年12月30日
- 個人資料保護法施行細則
 - 修正日期：105年03月02日



個人資料保護法整體架構



個人資料保護法之立法目的

避免人格
權受侵害

促進個人
資料之合
理利用

蒐集

個人資料

利用

處理





個人資料保護法架構

- 新版個資法：共56條條文
 - 修正日期：民國104年12月30日
 - 生效狀態：自中華民國105年03月15日施行。





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

- 病歷
- 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



個人資料之定義

- 個資法第二條 用詞定義如下：
- 個人資料：
 - 指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、**病歷、醫療、基因、性生活、健康檢查、犯罪前科**、聯絡方式、財務情況、社會活動及其他-
 - 得以直接或間接方式識別該個人之資料。
 - 當事人：指個人資料之本人(指現生存之自然人)



個人資料之內容

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(個資法第 6 條:立法院於104年12月15日完成三讀修正): 包括病歷、醫療、基因、性生活、健康檢查、犯罪前科。
 - 特種個人資料不得蒐集、處理或利用, 除個資法第6條所定例外情形外才能夠蒐集(如下說明)。
 - 一、法律明文規定。(§§9)
 - 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內, 且事前或事後有適當安全維護措施。(§§10、§§11、§§12)
 - 三、當事人自行公開或其他已合法公開之個人資料。(§§13)
 - 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, 且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。



個人資料保護法之特種個人資料

- 特種個人資料(個資法第 6 條:立法院於104年12月15日完成三讀修正): 包括病歷、醫療、基因、性生活、健康檢查、犯罪前科。
 - 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
 - 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其不同意違反其意願者，不在此限。
 - 依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。



特種個資蒐集之案例探討

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。



確認是否符合個資法第6條可以蒐集特種個資的情況。

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。

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

個人資料保護法規範的行為

• 蒐集

- 為建立個人資料檔案而取得個人資料
- 取得方式不限，任何方式取得皆為蒐集
- 包括「直接蒐集」與「間接蒐集」。

• 處理

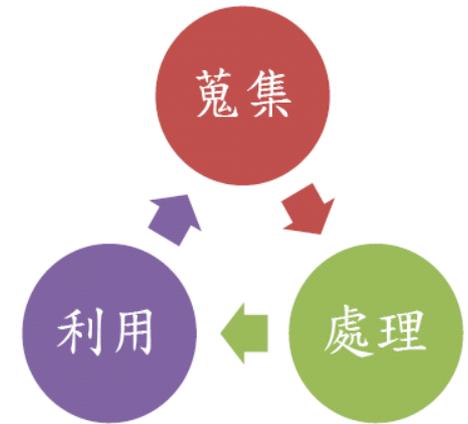
- 為建立或利用個人資料檔案所為之紀錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結、或內部傳送

• 利用 □

- 將蒐集之個人資料為「處理」外之使用。

• 國際傳輸

- 將個資作跨國(境)之處理或利用。



◎組織內部資料傳送 – 處理

◎將個資提供第三人 – 利用



個人資料法重要條文

- 特定目的
- 告知義務
- 安全維護事項
- 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)



公務機關個人資料之蒐集、處理及利用

- 第 15 條 (立法院於104年12月15日完成三讀修正)
 - 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：
 - 一、執行法定職務必要範圍內。(§§10)
 - 二、經當事人同意。
 - 三、對當事人權益無侵害。

公務機關個人資料之蒐集、處理及利用

- 第 16 條 (立法院於104年12月15日完成三讀修正)
 - 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： (§§10)
 - 一、法律明文規定。 (§§9)
 - 二、為維護國家安全或增進公共利益所必要。
 - 三、為免除當事人之生命、身體、自由或財產上之危險。
 - 四、為防止他人權益之重大危害。
 - 五、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經蒐集者依其揭露方式無從識別特定之當事人。 (§§17)
 - 六、有利於當事人權益。
 - 七、經當事人同意。

非公務機關個人資料之蒐集、處理及利用

- 第 19 條 (立法院於104年12月15日完成三讀修正)
 - 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：
 - 一、法律明文規定。(§§9)
 - 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。(§§26、§§27)
 - 三、當事人自行公開或其他已合法公開之個人資料。(§§13)
 - 四、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經蒐集者依其揭露方式無從識別特定之當事人。(§§17)
 - 五、經當事人同意。
 - 六、為增進公共利益所必要。
 - 七、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。(§§28)
 - 八、對當事人權益無侵害。
 - 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

- 第 20 條 (立法院於104年12月15日完成三讀修正)
 - 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：
 - 一、法律明文規定。(§§9)
 - 二、為增進公共利益所必要。
 - 三、為免除當事人之生命、身體、自由或財產上之危險。
 - 四、為防止他人權益之重大危害。
 - 五、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經蒐集者依其揭露方式無從識別特定之當事人。(§§17)
 - 六、經當事人同意。
 - 七、有利於當事人權益。
 - 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)



直接蒐集個資-告知之義務

5. 告知事項

§8 直接取得告知事項

§8-1 原則

- 一、機關名稱
- 二、蒐集之目的
- 三、個人資料之類別 依法務部施行細則之附件定之
- 四、個人資料利用之期間、地區、對象及方式
- 五、當事人依第三條規定得行使之權利及方式
- 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響

§8-2 例外免告知

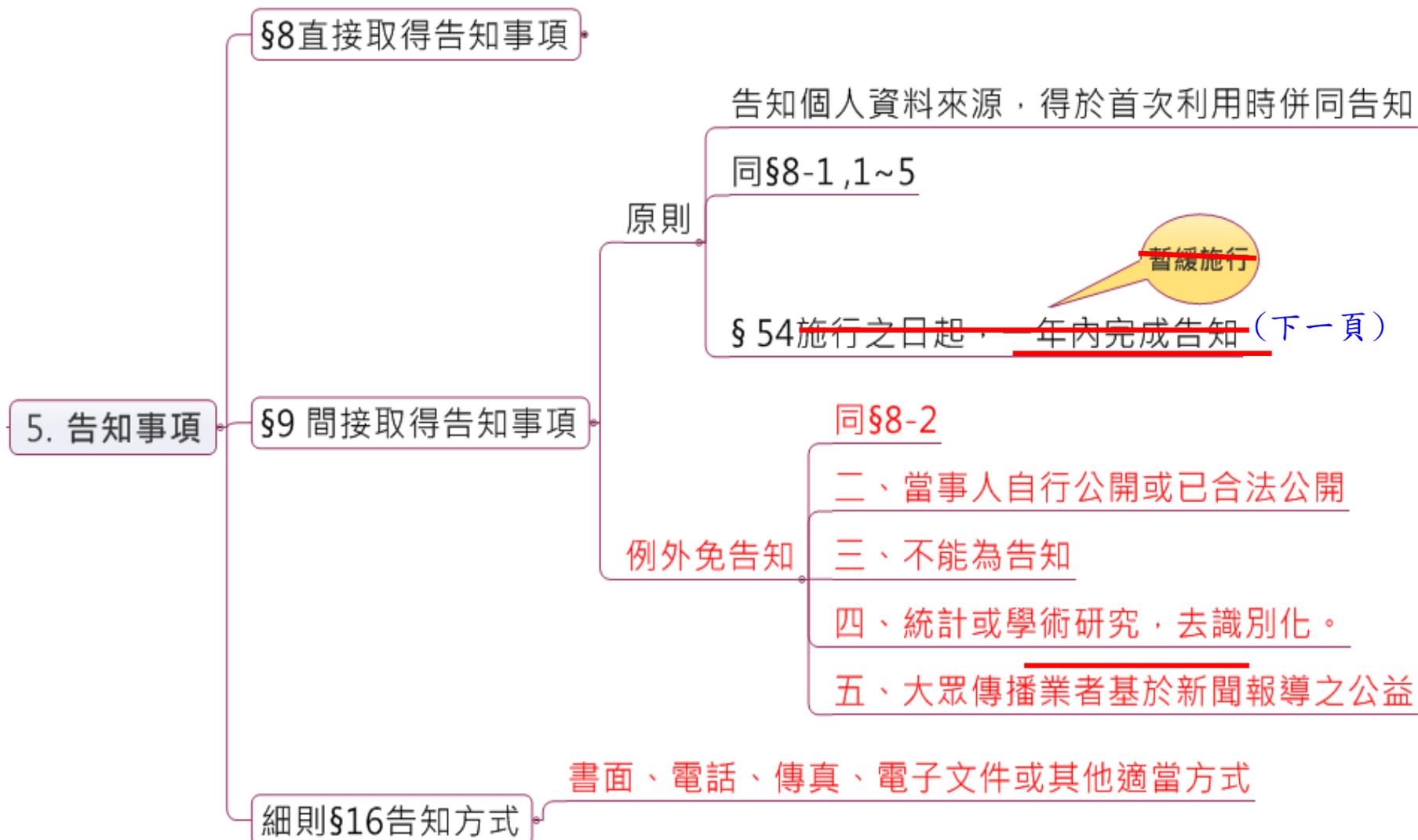
- 一、依法律規定
- 二、公務機關執行法定職務或非公務機關履行法定義務所必要
- 三、告知將妨害公務機關執行法定職務
- 四、告知將妨害第三人之重大利益公共利益
- 五、當事人明知應告知之內容
- 六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

§9 間接取得告知事項

細則§16告知方式



間接蒐集個資-告知之義務





間接蒐集個資-告知之義務(續)

- 第 54 條 (§§16、§§32) (立法院於104年12月15日完成三讀修正)
 - 本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。
 - 前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。
 - 未依前二項規定告知而利用者，以違反第九條規定論處。



告知函範例

- ○○**生物科技股份有限公司**，秉持臍帶血是救命事業的理念，經營○○臍帶血銀行，為了提供給您豐富的臍幹細胞及嬰幼兒照護資訊之**蒐集目的**，需要您的**個人資料類別**包括：姓名、職業、年齡、胎次、地址、聯絡電話、E-mail等(包含C001、C038等資料類別)。**利用期間**係本公司營運期間，**地區**限於台灣，**利用對象**為本公司，**利用方式**為郵寄、電話、派遣專人解說、辦理媽媽教室活動、或是其他可以提供給您臍帶血及嬰幼兒照護訊息之通知。
- 您可以依據**個資法第3條**針對共同蒐集您個人資料之公司，行使以下權利：包含查詢、閱覽、製給複給本、補充更正、請求停止蒐集、處理或利用或刪除。請撥打0800-000-000
- 您可以自由選擇是否提供個人資料，若不願意提供並不會影響您參與本次活動。
- 當事人簽名：_____ 日期：_____年____月____日



告知函範例

• 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，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？

- 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。(§27)
 - 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)



個人資料法施行細則所列之安全維護事項

- 保護標的：防止個人資料被竊取、竄改、毀損、滅失或洩漏。

- 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。

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。



舉證責任倒置

■ 公司舉證責任：（第29條）

- 公司必須負責「舉證責任」，證明自己符合法規要求且已善盡保管責任，無故意或過失責任才能免責



- 各種告知義務、取得當事人同意或回應個人請求等行為，都必須留下記錄以作為未來舉證之用





法律責任之範圍

行政責任

法定義務



法定職務

民事責任

刑事責任



行政責任

§§47~50行政責任
(僅限**非**公務機關)

§47 違反特定目的外之利用

§6 I 特種個人資料蒐集、處理、利用 ~~(暫緩施行)~~

§19 非公務機關蒐集、處理應有特定目的

§20 I 非公務機關特定目的外之利用

§21 國際傳輸之限制

處新臺幣五萬元以上五十萬元以下罰鍰，
並令限期改正，屆期未改正者，按次處罰之

違反者立即處分



§48

違反告知及基本權利履行
未訂定個資檔案安全維護計畫

§8 直接蒐集之告知

§9 間接蒐集之告知

§10 答覆查詢、閱覽或製給複製本

§11 請求更正或補充

§12 適當方式通知當事人

§13 受理准駁之決定

§20 II,III 當事人拒絕行銷之決定

§27 I,II 個人資料檔案安全維護計畫

限期改正，屆期未改正者，
按次處新臺幣二萬元以上二十萬元以下罰鍰

限期改正！
誰會被罰？



§49

規避、妨礙或拒絕行政檢查

§50 連帶處罰



規避行政檢查、連帶處罰

§47違反特定目的外之利用

§48

§49

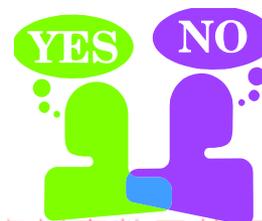
規避、妨礙或拒絕行政檢查

§50 連帶處罰

受前三條之罰鍰處罰

代表人、管理人或其他有代表權人，

除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰



處新臺幣二萬元以上
二十萬元以下罰鍰

§§47~50行政責任
(僅限**非**公務機關)

第五十條 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。



刑事責任

刑法§12

行為非出於故意或過失者，不罰。

過失行為處以刑事處分，以有特別規定者，為限。

個資法並未特別規定，過失之行為須處以刑事處分！

§41故意行為

§§41~44刑事責任

違反特種個資、特定目的及國際傳輸

§6-I 特種個人資料蒐集、處理、利用

§15 公務機關蒐集、處理應有特定目的

§16 公務機關特定目的外之利用

§19 非公務機關蒐集、處理應有特定目的

§20-1 非公務機關特定目的外之利用

§21 國際傳輸之限制

足生損害於他人者(僅限故意行為)

~~二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金~~

擬修法刪除

← 僅處分故意行為

意圖營利者

處五年以下有期徒刑

得併科新臺幣一百萬元以下罰金

§42非法變更

§44公務員加重其刑1/2



意圖營利、非法變更

§§41~44刑事責任

刑法§12

§41故意行為



違反特種個資、特定目的及國際傳輸

足生損害於他人者(僅限故意行為)

~~二年以下有期徒刑、拘役或科
或併科新臺幣二十萬元以下罰金~~

擬修法刪除

處分自然人為原則，
處分法人為例外！

意圖營利者

處五年以下有期徒刑

得併科新臺幣一百萬元以下罰金

§42非法變更



意圖非法變更

非法變更、刪除或以其他非法方法，
致妨害個人資料檔案之正確

意圖為自己或第三人不法之利益或損害他人之利益

足生損害於他人者

處五年以下有期徒刑，

得併科新臺幣一百萬元以下罰金

§44公務員加重其刑1/2



重大故意行為



民事責任



§28,29損害賠償

當事人非財產上之損害，得請求賠償；名譽被侵害，得請求適當處分

損害賠償，每人每一事件500~2萬，總額2億

所涉利益超過新臺幣2億元者，以該所涉利益為限

舉證責任倒置

公務機關採無過失責任主義，損害因天災、事變、不可抗力者除外

非公務機關採過失責任主義，能證明其無故意或過失者除外

§§28~34民事責任

§30 損害賠償請求期限

自請求權人知有損害及賠償義務人時起，

因二年間不行使而消滅；

自損害發生時起，逾五年者亦同



§34團體訴訟

受有損害之當事人二十人以上以書面授與訴訟實施權者，得提起損害賠償訴訟



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



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



情境案例

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」。



情境案例

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。



情境案例

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。



情境案例

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。



情境案例

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。



情境案例

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。



情境案例

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。

- 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。



情境案例

- 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。



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



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**。



Q&A 問題與討論

～如有任何問題・歡迎隨時來電詢問～

SafeLink

博創資訊科技股份有限公司

臺中市西屯區國安一路208巷6號

TEL : (04)2525-0535

FAX : (04)2461-5268

<http://www.safelink.com.tw/>

E-mail: sam@safelink.com.tw

