

個人資料保護認知宣導

(含個資事件案例解析及 GDPR 簡介)



輔導顧問師 林信成 (Albert Lin)

ISO27001 / BS10012 / ISO27701 / ISO29100 / ISO9001 主導稽核員

Mobile: 0933-510515

E-mail: bingo1982012@gmail.com

Safelink 博創資訊科技股份有限公司



個人資料，無所不在





層出不窮的個資事件

台視新聞HD

山下智久
日本男星

3.8萬人嗨跳
大巨蛋震

男星山下智久
個資遭曝

日圓
▲ 0.0001
0.2148

12:18:11

外洩山下智久個資 松機貴賓室員工挨轟
即日生效 重大里程碑! "台美21世紀貿易倡議"正式生效



層出不窮的個資事件





層出不窮的個資事件

TVBS新聞台 HD

更多新聞在這裡

TVBS NEWS

個資外流才有詐騙! "駭客"分季入侵"難防

掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道



層出不窮的個資事件

公視
19:43:14

23andMe爭議多

- 做基因測試服務
- 涉足醫療與製藥
- 隱私與數據爭議

PTS NEWS

晚間新聞
PTS EVENING NEWS

找不到買主 生技公司"23andMe"聲請破產

美生技公司23andme聲請破產-龐大基因檢測個資恐遭轉...

00:00:06

上午 07:45
2025/9/17



層出不窮的個資事件

EBC 東森新聞 HD



| 主播 李樺仙



| 記者 楊欣怡

美元
台幣

29.3390

0.0730

工程師非法買個資! 國華微信社竟還公然標售



層出不窮的個資事件

mnews · 鏡新聞

Tiffany遭駭

外部資安專家調查
美國時間5/12前後
未經授權第三方竊入

台北市

畫面來源 | Tiffany & Co.

Tiffany 警備員個資遭駭 烏鴉籠卸·認信陌生電訊郵件



層出不窮的個資事件

公視
19:43:17

23andMe爭議多

做基因測試服務

涉足醫療與製藥

隱私與數據爭議

P T S N E W S



晚間新聞

找不到巴士 生社公司23andMe設法破案



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」。



人工智慧個資管理及保護

人工智慧基本法

第4條第1項第三款

隱私保護與資料治理：應妥善保護個人資料隱私，尊重企業營業秘密，避免資料外洩風險，並採用資料最小化原則；同時在符合憲法隱私權保障之前提下，促進非敏感資料之開放及再利用。



人工智慧個資管理及保護

- 一、在人工智慧應用過程，應避免不必要之個人資料蒐集、處理或利用，倘涉及個人資料蒐集、處理或利用應進行風險評估，規劃風險因應措施，且具有正當利益(合法、合理、且有保護價值)、處理行為是實現該利益所必需，且不得侵害當事人的基本權利（如自由權、平等權）。
- 二、禁止涉及病歷、醫療、基因、性生活、健康檢查及犯罪前科相關個人資料蒐集、處理或利用。



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
- GDPR簡介與因應



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？



個人資料保護法修正重點

- 修正日期：114年11月11日
- 修正重點：
 - 一、明訂向個資會通報個資事故之義務
- 個資法母法對於發生個資事故時是否應向主管機關通報之規定原本付之闕如，本次修正明訂關於個資事故，於符合一定通報範圍時應通報個資會。除前述通報義務以外，本次修正也明文要求發生事故之企業對事故採取即時有效之應變措施並保存紀錄。具體通報的內容、方式、時限與範圍，以及應變措施、紀錄保存等細部事項，將由個資會後續以子法訂定之。



個人資料保護法修正重點

- **二、對於個資當事人通知個資事故之義務**
- 本次修正仍然要求民間企業於發生個資事故時應通知當事人，但未來企業已無法再以事故發生後尚未查明或是企業本身就事故之發生並未違反個資法為理由，而遲誤通知個資當事人。具體通知當事人之細部事項，同樣將由個資會後續以子法訂定之。
- **三、修正行政檢查相關規定**
- 本次修正除微調原本行政檢查規定之文字外，明定未來行政檢查將由個資會決定是否發動，且個資會將與中央目的事業主管機關以及地方政府共同協力進行行政檢查。



個人資料保護法修正重點

• 四、主管機關之權限劃分

- 未來個資法將由個資會統一擔任主管機關，本次修正增加未來個資會需報請行政院公告一定範圍之非公務機關，在個資會成立後之六年內仍由該等行業之中央目的事業主管機關或地方政府負責管轄個資法中若干監理事項；且就該等行業所應適用之個人資料檔案安全維護計畫或業務後個人資料處理方法，仍由其等之中央目的事業主管機關訂定，且得訂定較為嚴格規定。

• 五、明訂相關罰責

- 本次修正針對非公務機關未依規定通報個資會個資事故，以及未訂定或辦理安維事項或安維計畫等行為，皆明訂罰責，且個資會得毋庸先令限期改正即可逕行處罰。



個人資料保護法修正重點

- 六、對個資會之行政處分不服，應逕提行政訴訟救濟
- 由於個資會為獨立機關，除法律另有規定外，不受其他機關指揮監督，是以如對個資會依個資法所為行政處分不服者，應直接適用行政訴訟程序。



個人資料保護法整體架構

- 個人資料保護法：共55條條文
– 修正日期：民國114年11月11日

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

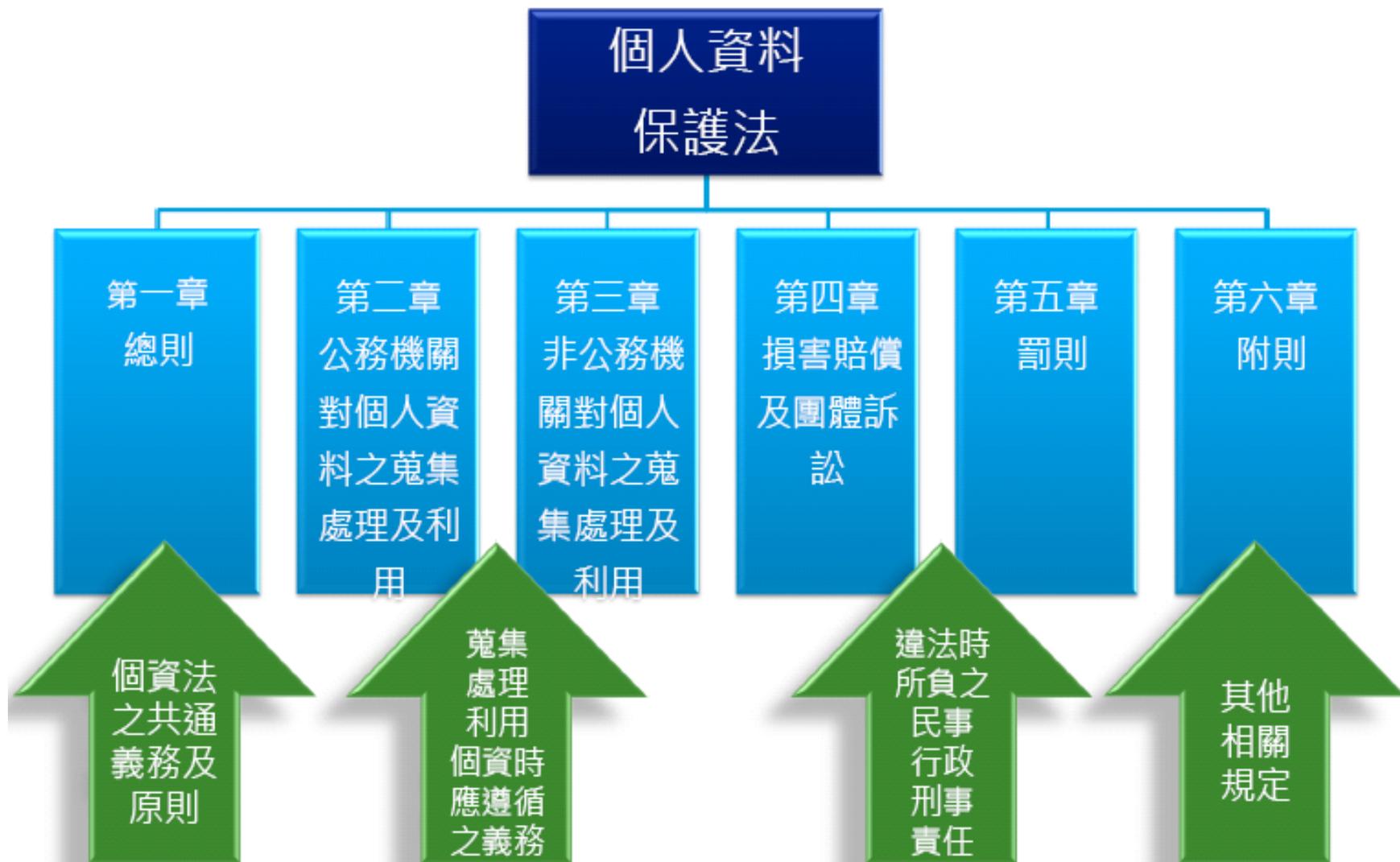
罰則

第六章

附則



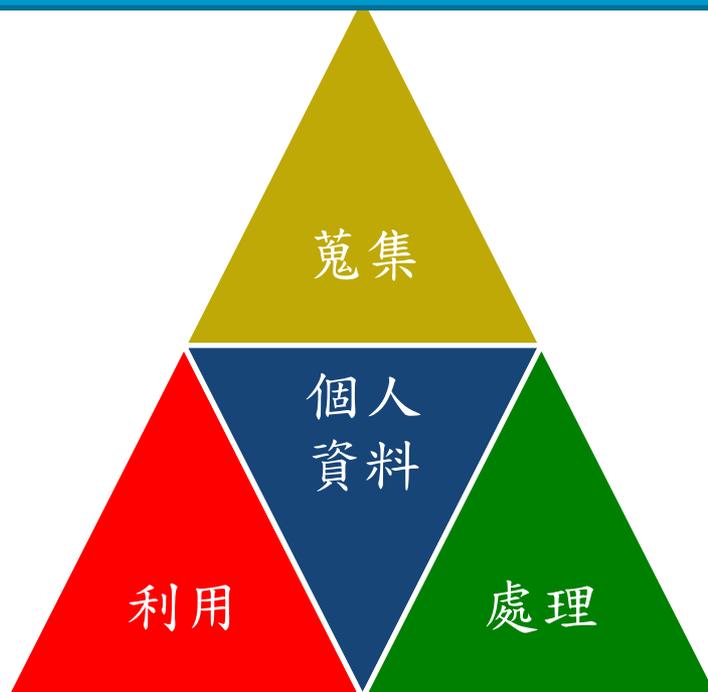
個人資料保護法整體架構



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





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。
 - 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。



當事人法定請求權利

- 個資法第3條
- 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
 - 一、查詢或請求閱覽。
 - 二、請求製給複製本。
 - 三、請求補充或更正。
 - 四、請求停止蒐集、處理或利用。
 - 五、請求刪除。



當事人法定請求權利

- 個資法第10條
- 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：
 - 一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
 - 二、妨害公務機關執行法定職務。
 - 三、妨害該蒐集機關或第三人之重大利益。



當事人法定請求權利

- 個資法第11條
- 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。
- 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。
- 個人資料蒐集之特定目的消失或期限屆滿時，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。但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。
- 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。
- 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。



當事人法定請求權利

- 個資法第13條
- 公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。
公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。



當事人法定請求權利

- 個資法第14條
- 查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。



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

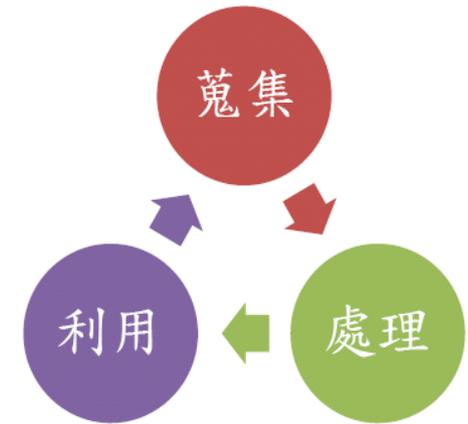
- 為建立或利用個人資料檔案所為之紀錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結、或內部傳送

• 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
- 同意要件
- 委外監督
- 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)



非公務機關個人資料之蒐集、處理及利用

- 個資法第 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。
 - 三、當事人自行公開或其他已合法公開之個人資料。
 - 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。
 - 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。
 - 八、對當事人權益無侵害。



非公務機關個人資料之蒐集、處理及利用

- 個資法第 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、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。(§7)
 - 七、有利於當事人權益。

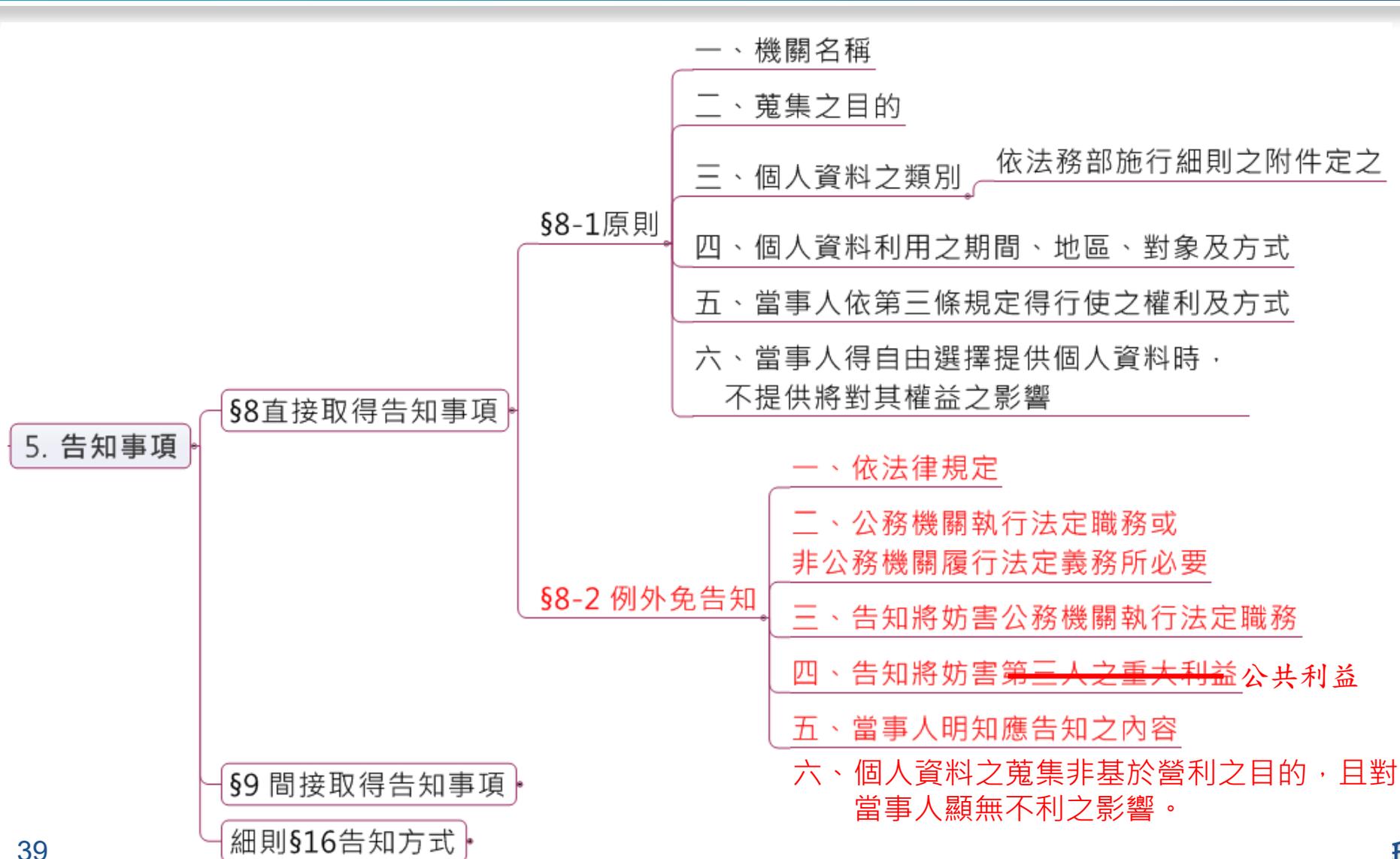


蒐集個資時，應告知當事人哪些事項？

- 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)

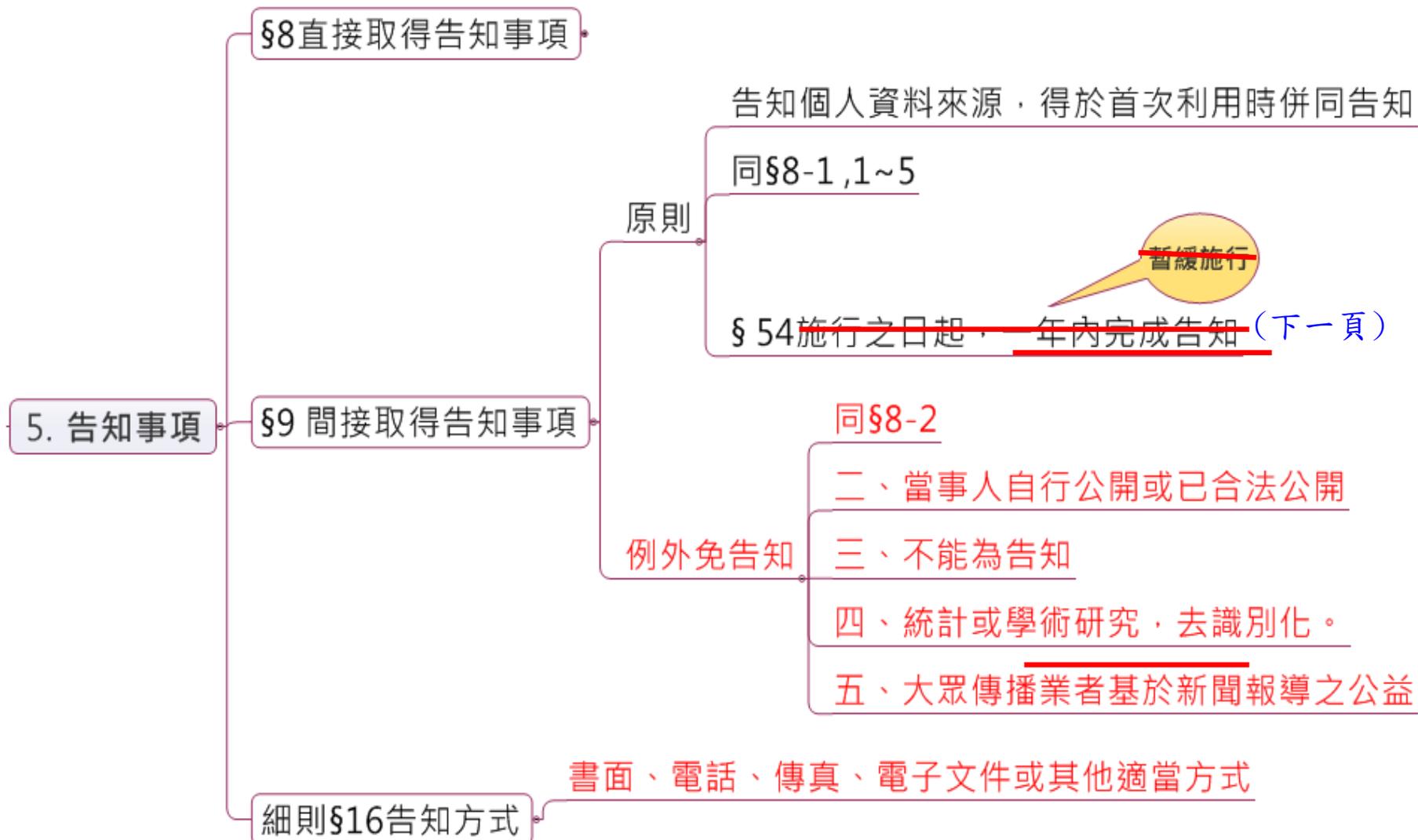


直接蒐集個資-告知之義務





間接蒐集個資-告知之義務





間接蒐集個資-告知之義務(續)

- 個資法第 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

- 本校（單位，如教務處），基於（特定目的，如教育或訓練行政、學生（員）（含畢、結業生）資料管理），將依個人資料保護法蒐集、處理及利用您的個人資料。蒐集之個人資料類別為（如辨識個人者、政府資料中之辨識者、學生(員)、應考人紀錄），範圍包括（如姓名、地址、身分證統一編號、電話／手機／傳真、E-mail、考試紀錄）等。
- 本單位蒐集之個人資料依法令規定，在您使用本服務的地區內及（委外廠商、海外姊妹校、執行法定職務之機關，如無，請略過）利用您的個人資料，供本單位業務承辦人員及（委外廠商、海外姊妹校、執行法定職務之機關，如無，請略過）所處理及利用，除此之外，本單位不會將您所提供的個人資料提供給他人，個人資料利用期限為（以法令規定優先、單位規範或業務目的所需次之），且經由紙本、電子形式利用您所提供之個人資料（請確認資料形式）。
- 您依法得行使當事人權利，包含查詢或請求閱覽、製給複製本、補充或更正、刪除、停止蒐集、處理或利用個人資料等權利，並可前往本校各單位辦公處所行使本項權利。
- 為保障您的權利，您可以選擇是否提供個人資料，若選擇不提供個人資料或提供不完全時，本單位可能無法提供您完善的服務。
- 我已了解、接受上述告知內容，並同意提供個人資料。
- 當事人簽名 年 月 日
- 若當事人未滿18歲，需請法定代理人表示同意並署名。
- 我瞭解並同意上述內容 法定代理人簽名 年 月 日



同意要件

- 個資法第 7 條
- 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。
- 第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，獨所為之意思表示。
- 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。
- 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。



委外監督(個資法施行細則 第8條)

委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

- 前項監督至少應包含下列事項：
 - 一、**預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。**
 - 二、受託者就第十二條第二項採取之措施。
 - 三、有複委託者，其約定之受託者。
 - 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
 - 五、委託機關如對受託者有保留指示者，其保留指示之事項。
 - 六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。
- **第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。**
- 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。



委外監督(個資法施行細則 第8條)

合約範本

- 一、乙方因履行本契約僅得於甲方指示之範圍內蒐集、處理或利用個人資料，且應符合本契約條款、個人資料保護法及其他相關法令，並受甲方之監督。
- 二、甲方委託乙方處理及利用個人資料之範圍、類別、特定目的及期間如下：
範圍：雙方契約內容所涉及之個人資料範圍（如姓名）。
類別：雙方契約內容所涉及之個人資料類別（如辨識個人者）。
特定目的：該項業務蒐集個人資料之特定目的（如學生（員）（含畢、結業生）資料管理）。
期間：以契約有效期間為原則，但甲方配合法院、檢調單位依法調閱及當事人查詢等例外情形，不在此限。
- 三、乙方(包括但不限於乙方之代表人、代理人、受僱人、委任人等)就履行本契約所對各項個人資料之蒐集、處理、利用，均須符合個人資料保護法之相關規定及甲方所訂之資訊安全政策規定，並依個人資料保護法施行細則第12條第2項事項（依委託單位需求及受委託單位實際能辦理為原則考量安全維護措施，如詳個人資料委外管理監督檢核表檢核項目），並每年至少定期回報一次其遵循之結果。



委外監督(個資法施行細則 第8條)

合約範本

- 四、乙方如有將當事人資料再委託第三方進行蒐集、處理或利用者，應事前徵得甲方同意授權後，使得為之，且乙方應依個人資料保護法施行細則第8條之規定，對複委託廠商執行監督之責，並對第三方蒐集、處理或利用當事人資料或檔案之行為負完全責任。
- 五、倘乙方發現有違反個人資料保護法、其他個人資料保護法律或其法規命令時或個人資料被竊取、洩漏、竄改等其他侵害之情事導致違反個人資料保護相關法律或其他法規命令，或導致他人權益遭受損失之可能，應即刻以電話、Email通知甲方，且辦理函報甲方作業，並立即調查事故原因、過程與影響範圍及採行必要之控制與預防措施，必要時協助甲方進行和解或訴訟程序。如由甲方發現者，亦應即時以電話、Email通知乙方按前述辦理，且辦理函報乙方作業。
- 六、乙方如認甲方之指示有違反個人資料保護相關法令者，應立即以電話、Email通知甲方，且辦理函報甲方作業，並留下書面通知之佐證資料。



委外監督(個資法施行細則 第8條)

合約範本

- 七、就甲方委託蒐集、處理或利用的個人資料，甲方有權保留指示之事項，乙方僅得於甲方指示之範圍內進行蒐集、處理或利用。
- 八、本契約期滿、終止或解除時，乙方應於報請核銷經費時，依甲方之指示，將因履行本契約所持有之個人資料載體返還予甲方指定人員，並採用永久有效之方法銷毀、刪除個人資料（包含但不限於以電磁紀錄、紙本或其他任何形式儲存者），乙方並應提出相關證明文件，內容包括返還資料載體、銷毀、刪除資料之項目、數量、時間、地點、方式、執行及監督人員簽核確認等，同時應以書面具結其並未持有因履行本契約而保有之個人資料，惟資料保有廠商持續辦理同一業務，且範圍、類別、特定目的皆未改變，則仍可持續保有原蒐集個人資料，非屬持續辦理同一業務，但仍於法令規定保存期限內且甲方明確同意時，乙方仍可持續保有原蒐集個人資料。由乙方自行保管之個人資料，屆法規要求之保存期限即應銷毀、廢棄及(或)刪除個人資料，銷毀、廢棄及(或)刪除之項目、數量、時間、地點、方式、執行及監督人員簽核確認等相關證明文件及書面具結文件應函報甲方，但甲方因執行職務或業務所必須、配合法院及(或)檢調單位依法調閱及當事人查詢等例外情形，得發函請乙方延長保管期間。



委外監督(個資法施行細則 第8條)

合約範本

- 九、乙方同意配合甲方基於法令之要求實施定期或不定期稽查以監督乙方執行之狀況，並於甲方進行稽查時，負有提供甲方稽查所需相關文件資料之義務。
- 十、乙方因履行本契約而保有個人資料檔案者，應指定專人辦理個人資料安全維護事項，且該人員應具有管理及維護個人資料檔案之能力或相關經驗，並足以擔任本契約個人資料檔案安全維護經常性工作。



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？

- 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)



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。



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



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

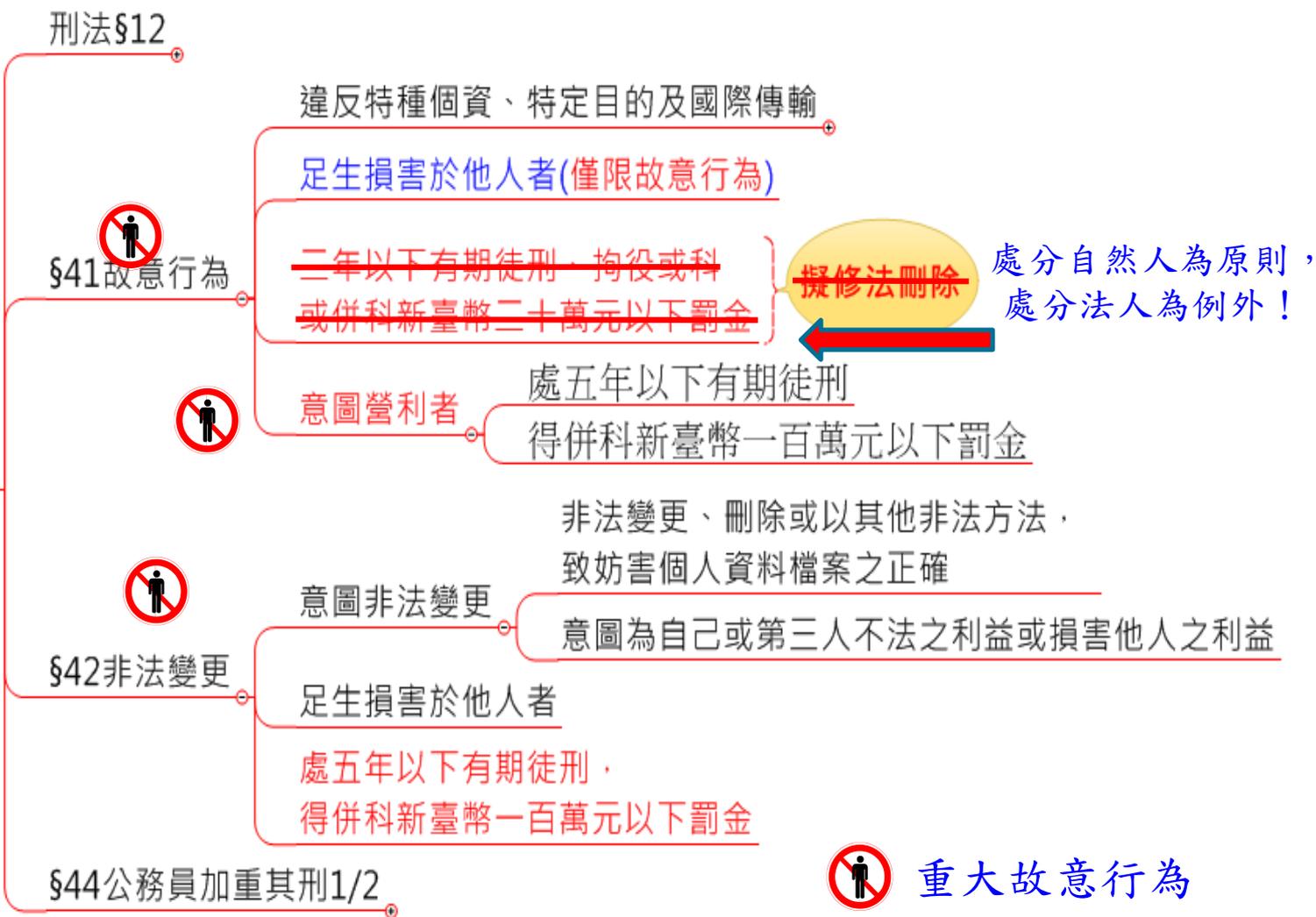
§42非法變更

§44公務員加重其刑1/2



意圖營利、非法變更

§§41~44刑事責任





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
- GDPR簡介與因應



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，長度及變更頻率應遵照本校規定辦理。



個資檔案防護實務

- 個人保管的紙本個資(包括名片)建議存放於上鎖的櫃子裡。
- 個人電腦設備裡的個資檔案最好進行加密，可使用免費加密軟體如TrueCrypt、AxCrypt等。
- 個人電腦設備裡已不再使用的個資檔案，應採用徹底刪除的軟體予以刪除，如 Eraser。
- 透過網路(E-mail、即時通訊等)傳輸個資之前，應先進行加密，並以其他管道傳送加密的密碼。
- 隨身碟因易遺失或遭偷竊盜用，應確保內含個資資料經過加密保護。
- 社群網站上，不要隨意透漏個資，包括電話、地址、家人資訊、個人習慣、旅遊計畫等，且除非必要，儘量不要同意網站使用個人資料在其他用途及分享，另使用各種社交網站需進行相關「隱私設定」。
- 收到各種訊息(簡訊、即時通訊、電子郵件)，若其中含有附檔或網址，應特別留意是否詐騙，點選前最好確認。
- 個人的電腦設備和手機，應安裝防毒軟體，並注意軟體更新至最新版本。
- 勿使用P2P軟體，不安裝非公務使用及非法不明之軟體。



Https://pdpc.gov.tw

個人資料保護委員會籌備處-歷史

https://www.pdpc.gov.tw/News/49/

網站導覽 | 回首頁 小 中 大

個人資料保護委員會籌備處

關於我們 最新消息 法令及執行措施 為民服務 資訊專區 國際資訊

資訊專區
政府資訊公開專區
歷史專區

首頁 > 資訊專區 > 歷史專區

歷史專區

關鍵字：

全部 法務部 (84年 ~ 107年) 國發會 (108年 ~ 112年)

上版日期	主題
109-12-29	國發會109年編印「個人資料保護法規及參考資料彙編」
107-09-20	國發會向產業界舉辦GDPR宣導說明會
107-08-22	國發會舉辦GDPR研討會·強化公部門因應作為
107-05-02	歐盟資料保護一般規則(General Data Protection Regulation · GDPR)與我國個人資料保護法之重點比較分析
107-02-26	106年12月1日公務機關個人資料保護法實務研習會

31°C 多雲時晴 下午 02:10 2024/7/8



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
- GDPR簡介與因應



GDPR 簡介與因應

一. GDPR 簡介

二. 需要做甚麼





GDPR簡介

1. **GDPR管轄範圍**
2. 個人資料及主管機關
3. 章節介紹
4. 罰則





GDPR 簡介





GDPR管轄範圍

規定個人，公司或組織處理與歐盟個人有關的個人資料的處理。

一家在歐盟設立公司的公司向波羅的海國家的客戶提供旅遊服務，並在這方面處理自然人的個人數據。

不適用於處理已故之人或法律實體(legal entity)的個人資料

個人使用他們自己的私人通訊錄通過電子郵件邀請朋友到他們正在組織的團體（家庭例外）。



GDPR管轄範圍

- 不適用於由個人出於純粹個人原因或在家中進行的活動處理的資料，只要與專業或商業活動無關。當個人在個人領域以外使用個人資料，例如社會文化或金融活動時，則必須遵守。



GDPR 簡介

1. GDPR 管轄範圍
2. 個人資料及主管機關
3. 章節介紹
4. 罰則



個人資料及主管機關

個人資料

個人資料是指與識別或可識別的活人有關的任何信息。收集在一起的不同信息可以導致識別特定的人，也構成個人資料

YES：姓名、地址、
EMAIL(**name.surname@company.com**)、
ID Number、電話、職業

NO：公司註冊資訊、匿名化資訊、
EMAIL(**info@company.com**)



主管機關 (DPA)

DPA是獨立的公共當局，通過調查和糾正權力監督保護法的適用。他們就個資保護問題提供專家意見，並處理對違反“一般資料保護規則”和相關國家法律的申訴。

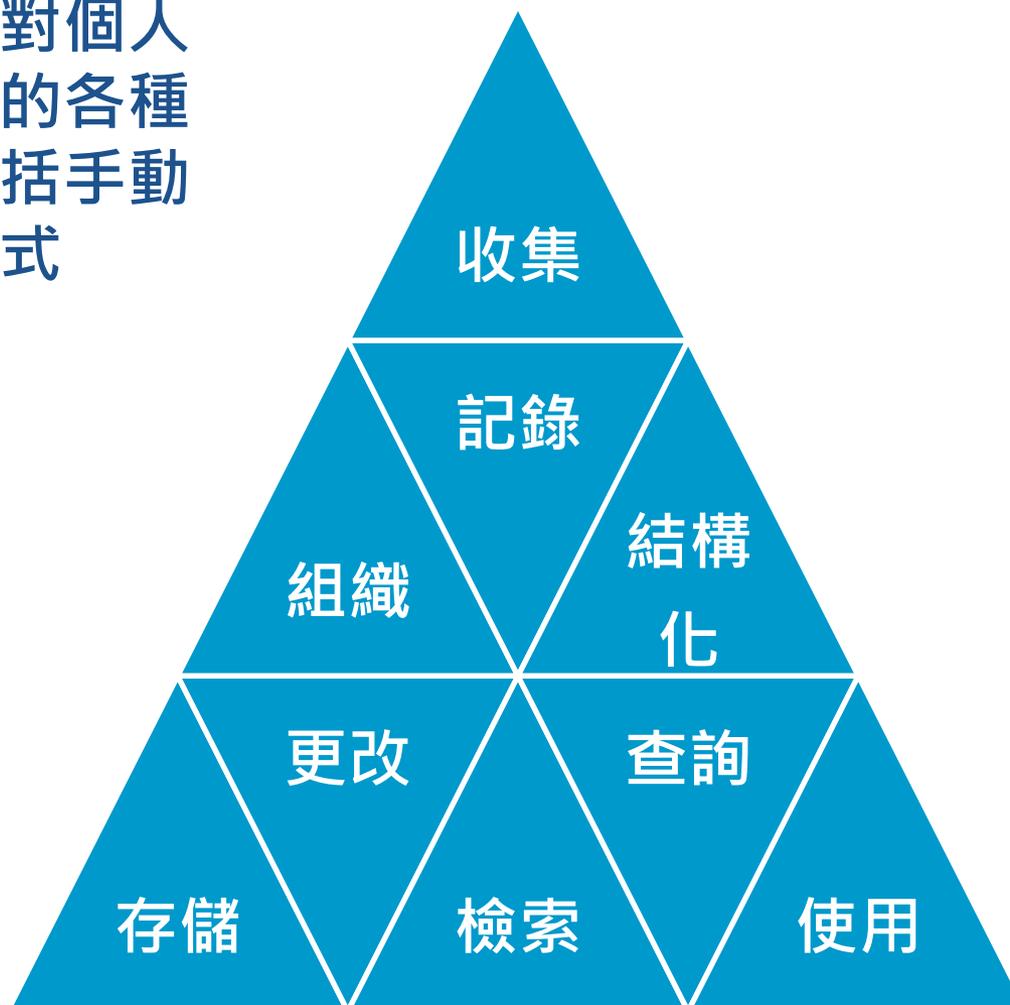
每個歐盟成員國都有一個DPA

一般來說，關於個資保護問題的主要聯絡點是貴公司/組織所在歐盟成員國的DPA。但是，如果您的公司/組織在不同的歐盟成員國處理數據，或者屬於在不同歐盟成員國建立的公司集團的一部分，則該主要聯繫點可能是另一個歐盟成員國的DPA。



個人資料處理

- 處理包括對個人資料執行的各種操作，包括手動或自動方式





個人資料處理

員工管理和工資管理

查詢包含個人資料的聯繫人資料庫

發送促銷郵件

銷毀含有個人資料的文件

在網站上張貼/放置一個人的照片

存儲IP 位址或MAC位址

錄影 (CCTV)



GDPR 簡介

1. GDPR 管轄範圍
2. 個人資料及主管機關
3. 章節介紹
4. 罰則



章節介紹

第一章
總則

第二章
原則

第三章
資料主體之權利

第四章
控制者及處理者

第五章
個人資料傳輸至第三
國或國際組織



章節介紹

第六章

獨立監管機關

第七章

合作及一致性

第八章

救濟、義務及
處罰

第九章

特殊處理之規範

第十章

授權法及施行法

第十一章
附則



個人資料處理之一般性原則（第 5 條）



合法性、公正
性及透明度



目的限制



資料最少蒐
集



正確性



儲存限制



完整及保密



課責



個人資料處理之合法要件（第 6 條）





同意之合法要件（第 7 條）

- 同意之給予必須是資料主體依其意思決定就其個人資料處理所為具體、肯定、自由、明確、受充分告知及非模糊之指示，如：口頭或書面之聲明，包括以電子方式為之者。如單純沉默、預設選項為同意（pre-ticked boxes）或不為表示等，均不構成同意。同意須涵蓋基於相同之一個或多個目的所為之全部處理活動，如資料之處理具有多重目的時，全部目的均應取得同意。



資料主體（當事人）之權利

★ 透明原則（第 12 條至第 14 條）

★ 接近使用權（第 15 條）

★ 更正權及刪除權（「被遺忘權」）（第 16 條、第 17 條）

★ 資料可攜權（第 20 條）

★ 拒絕權（第 21 條）

★ 自動決策及建檔之相關權利（第 22 條）



關於兒童之特別保護（第 8 條）

- 鑑於兒童未能完全知悉其個人資料處理之風險、後果、相關保護措施及權利，兒童之個人資料值得受特別保護，尤其在為行銷或建立使用者檔案之目的。任何提供予兒童之資訊及溝通，應採用兒童易於理解且清晰簡易之語言。
- 資料主體同意之要件適用於直接向兒童提供資訊社會服務之情形，如兒童年滿 16 歲，兒童之個人資料處理應屬合法；如該兒童未滿 16 歲，僅限於父母或監護人授權或同意之範圍內，該等處理始為合法。



特種個資之處理（第 9 條）

- 揭露種族、政治意見、宗教或哲學信仰之個人資料、基因資料、用以識別自然人之生物特徵識別資料、涉及前科及犯罪之個人資料、與健康相關或性生活或性傾向等有關個人資料之處理，原則上應予以禁止。但依本規則或會員國法律規定，資料主體已明確同意或已自行公開；為履行義務及行使控管者特定權利之目的；為行使法律上請求或司法機關執行司法權；或為保障資料主體之基本權及利益而有必要之處理等，不在此限。



個人資料之國際傳輸（第 44 條、第 45 條）

- 在任何情況下，向第三國或國際組織之個人資料移轉僅得於完全遵循本規則之前提下執行，唯有當控管者或處理者已遵守本規則所定關於個人資料移轉至第三國或國際組織之規範，且受本規則所定其他條款之拘束時，個人資料之移轉始得為之。第三國應確保有效而獨立之資料保護監督機制（effective independent data protection supervision）、對人權、法治與自由之基本尊重，且應提供資料主體有效且可實現的權利及有效的行政與司法救濟。



GDPR 簡介

1. GDPR 管轄範圍
2. 個人資料及主管機關
3. 章節介紹
4. 罰則



個人資料侵害之通報及損害賠償 (第 33 條、第 82 條)

- 個人資料侵害發生，應即向監管機關通報，不得無故遲延。若可能，應於發現後 **72 小時** 內通報，控管者如證明依歸責原則，該個人資料之侵害不可能造成當事人權利與自由的風險者，不在此限。當該通知無法於 72 小時內到達時，**遲延之原因應與通知一併提交**，並且不得更進一步遲延。因違反本規則而遭受物質上或非物質上之損害時，任何人應有權自控管者或處理者就其損害獲得賠償。**惟如控管者或處理者可證明其對於損害之造成不可歸責時，得免除賠償責任。**



行政罰鍰之裁處（第 83 條）

- 違反本規則有關控管者及處理者之義務、認證機構之義務或監管機構之義務者，最高處以一千萬歐元之行政罰鍰；如為企業，最高處以前一會計年度全球年營業額之百分之二，並以較高者為準。
- 違反有關資料處理之基本原則、個人資料國際傳輸之規定、侵害本規則所定資料主體之權利、或違反依照本規則通過之會員國法律所定之任何義務者，最高處以二千萬歐元之行政罰鍰；如為企業，最高處以前一會計年度全球年營業額之百分之四，並以較高者為準。



GDPR 簡介與因應

一. GDPR 簡介

二. 需要做甚麼



STEP 1

• 檢查個人資料收集、處理、處理目的及法律依據

聘僱員工

- 您正在根據就業合同和法律義務（例如向稅務機關/社會體系報告）處理他們的個人資料

管理個人客戶列表

- 如果獲得了這些客戶的同意，可以向他們發送關於特殊優惠/廣告的通知

宣傳新產品

- 利用客戶列表以地址宣傳產品。這被稱為合法利益。您必須通知個人您的預期用途，如果客戶不同意，請停止處理這些數據。



STEP 2

- 在收集個人資料時通知您的客戶，員工和其他個人

個資擁有者必須知道你處理他們的個人資料的目的。

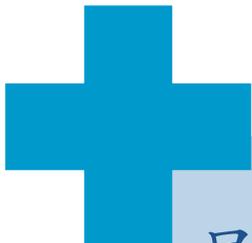
當他們已經掌握瞭如何使用個資的信息時，無需告知個人，例如，當客戶要求您送貨上門時。

依照個人請求告知持有的個人資料，並讓他們存取他們的個資。保持個資的排序性，例如，你的員工會詢問你有什麼樣的個人資料，你可以輕鬆提供，無需額外的麻煩。



STEP 3

- 僅在必要期限內保存個人資料



員工個資：只依僱傭關係和相關的法律義務保存。



客戶個資：只要客戶關係持續和相關的法律義務（例如出於稅務目的）

依照收集的目的，刪除不再需要的個資。



STEP 4

- 確保處理的個人資料安全

資訊
系統

限制存取
權限

密碼管制

實體

無關的人
無法拿到

上鎖



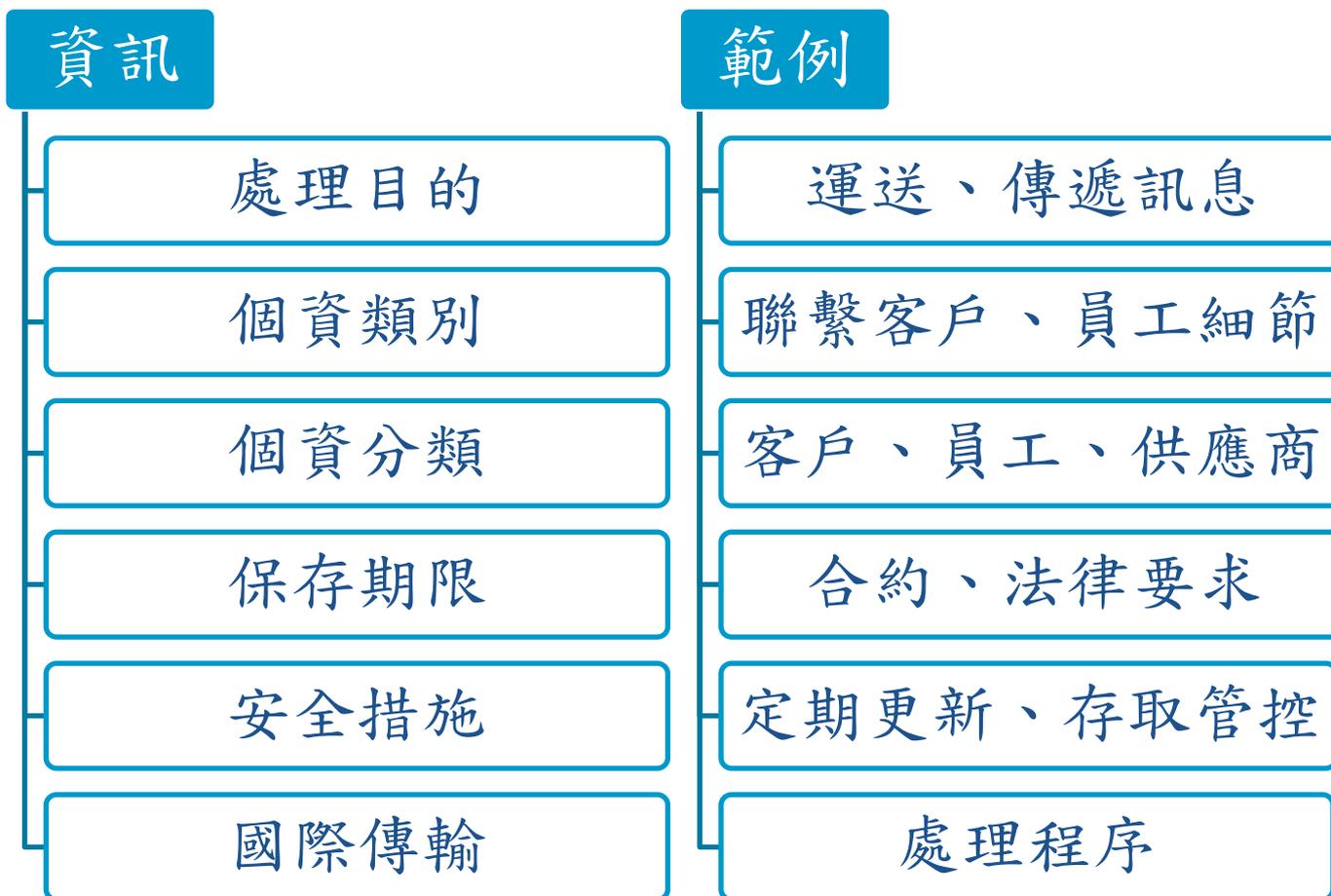
STEP 5

- 處理過程文件化
- 準備一份簡短的文件，說明您持有的個人資料以及原因。您可能需要在您的DPA提出請求時提供文檔。



STEP 5

• 處理過程文件化





STEP 6

- 確保供應商遵守法規
- 如果您將個人數據處理轉包給其他公司，只能使用保證處理符合GDPR要求的服務提供商（例如安全措施）。在簽訂合約之前，檢查他們是否已經改變並調整為GDPR。把它放在合約中。



STEP 7 DPIA

於特別使用新科技之處理方式，且考量該處理之本質、範圍、使用情形及目的後，認為該處理可能導致自然人之權利及自由的高度風險時，控管者應於處理前，實行該處理對於個人資料保護之影響評估。單一評估得針對一系列呈現相似高風險之類似處理

- 系統和廣泛的評估，包括分析：
1. 大規模處理敏感個資。
 2. 大規模系統性監測公共區域。



STEP 7 大規模

資料數量

- 搜尋引擎處理用於行為廣告的個人數據

資料質量 或廣度

- 患者個人資料

處理持續 性

- 客戶的即時地理位置數據，以供專門從事這些活動的處理者進行統計者

地域性

- 公共交通系統的個人旅行資料



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 : 886-4-25250535

FAX : 886-4-24615268

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

E-mail: sam@safelink.com.tw

