個人資料安全與個資法介紹

講師:李雋元
Email:ericph0617@gmail.com

課程大綱

- 隱私權及個人資料保護法制發展
- 國內個人資料侵害案例
- 我國對個人資料保護的沿革
- 個人資料保護法的架構及相關條文
- 損害賠償及團體訴訟及罰則

隱私權與個人資料保護

- 『隱私權』和『個人資料保護』，常常被當成一件事來談，因為『個人資料』保護不周，就可能會發生『隱私權』侵害的問題。儘管如此，還是得釐清這兩者在根本意義的異同。那就是：
  - **隱私權**；是個人的基本權利之一，受到憲法所保障，個人人格上的利益不受不法僭用或侵害，個人與大眾無合法關聯的私事，亦不得妄予發布公開，而其私人活動，不得以可能做成一般人的精神痛苦或感覺羞辱之方式非法侵入的權利。
  - **個人資料保護**；則是著重於如何確保個人資料之蒐集，處理與利用過程不會侵害到『隱私權』
  - 個人資料檔案；指基於特定目的儲存於電磁紀錄物或其他類似媒體之個人資料之集合。

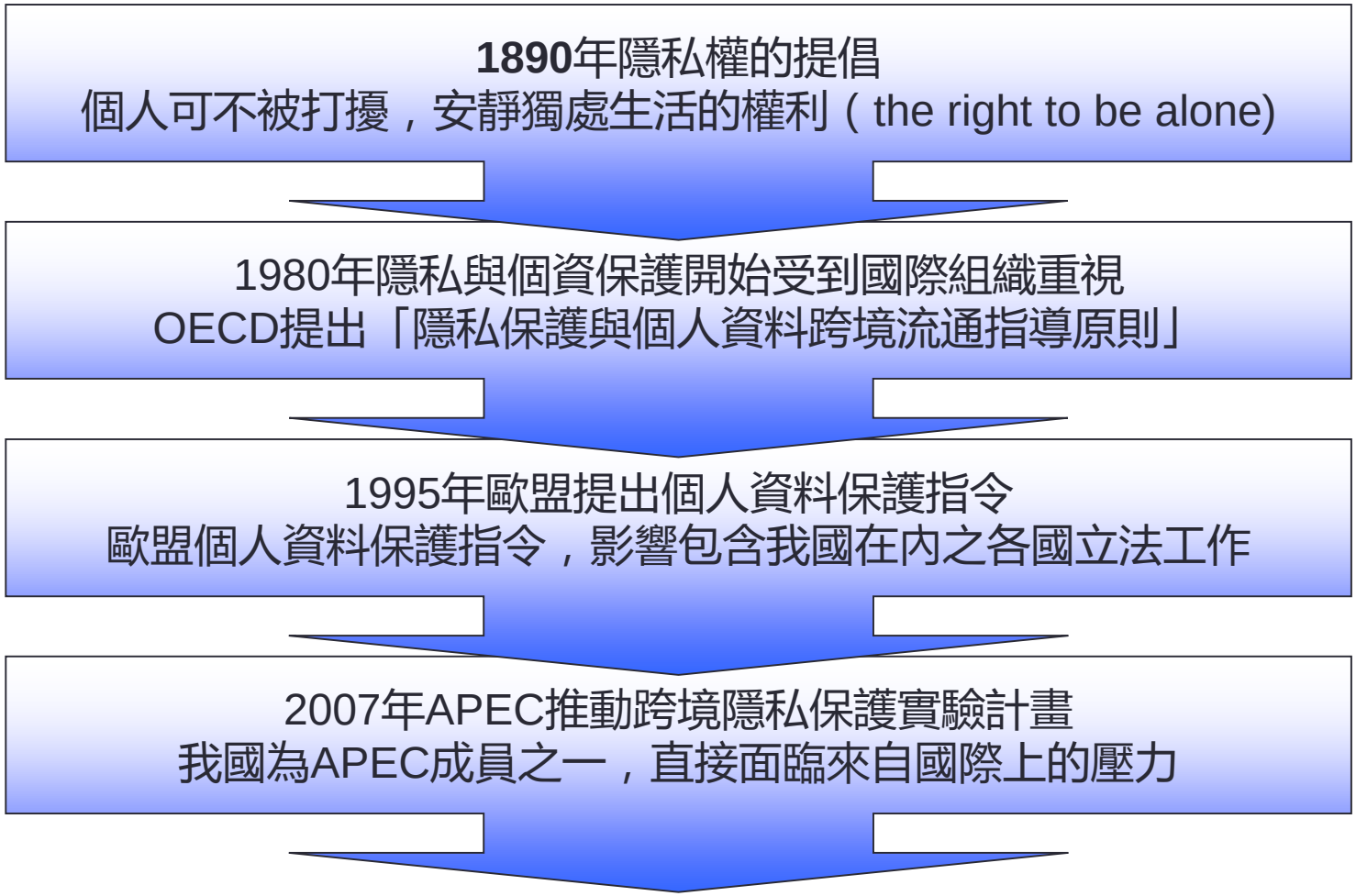
隱私權保護範圍

- 司法院大法官於釋字第585號解釋，明白承認隱私權受憲法所保障，隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。
- 依釋字603號解釋，至於隱私權的保護範圍，可分為「空間隱私」與「私密隱私」兩部分。
  - 所謂私密隱私，指「保障個人生活私密領域免於他人侵擾及個人資料之自主控制」，
  - 所謂空間隱私，指「保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」

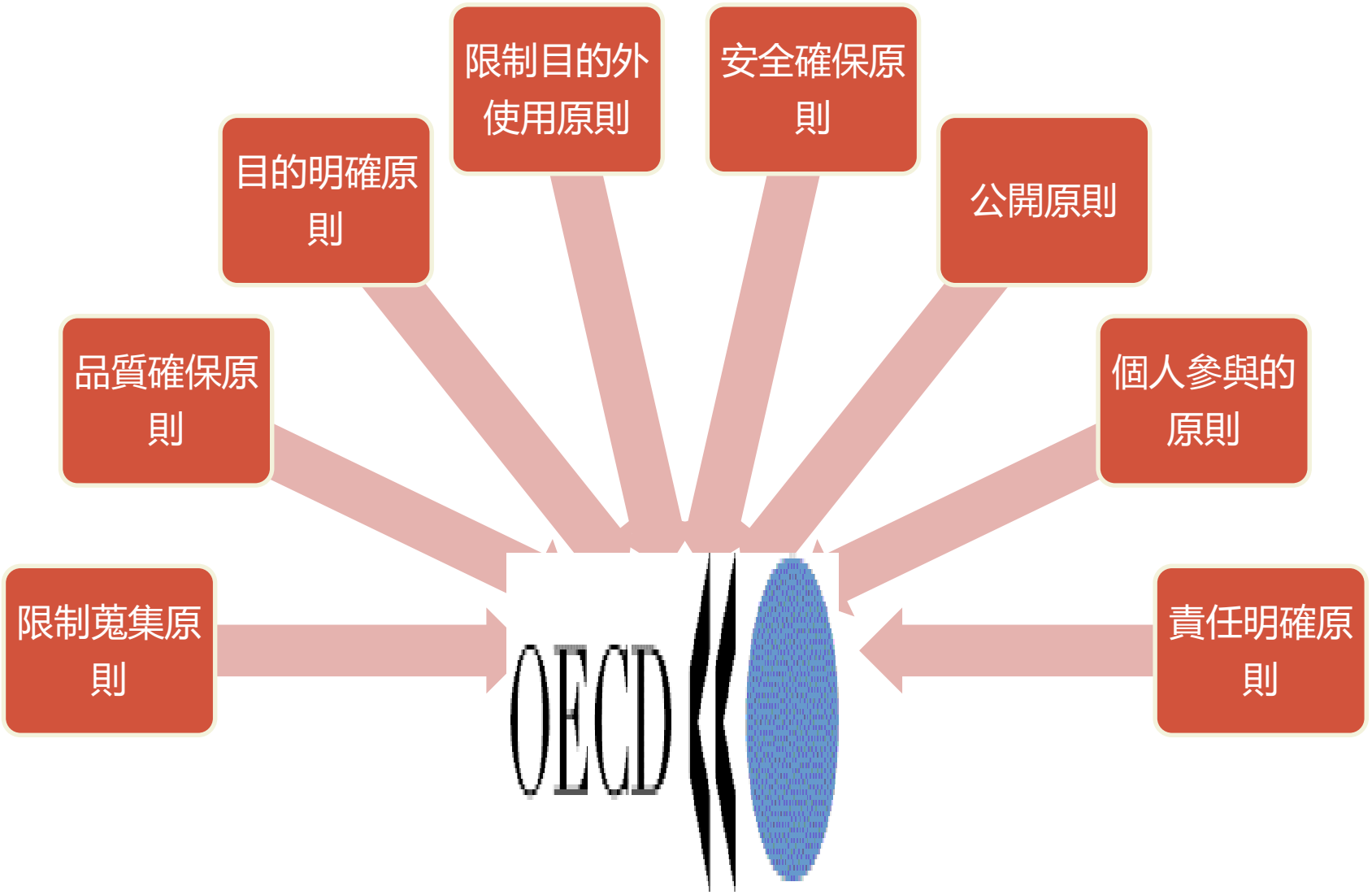
個人資料保護法進度


2010年
04/20 新版個人資料保護法二讀通過
04/27 新版個人資料保護法三讀通過
05/26 總統公布新版個人資料保護法
2011年
10/27公布個資法施行細則草案
2015年
正式施行個資法

個人資料保護之國際發展



OECD指導原則


限制目的外使用原則
安全確保原則
目的明確原則
公開原則
品質確保原則
個人參與的原則
限制蒐集原則
責任明確原則
OECD

歐盟提出個人資料保護指令

- 歐盟對網際網路應用以及電子
  權利保護相當重視並有立法與
  洲議會完成了有關保護個人資
  資料公約」
- 並已於1985年10月1日正式生
  加入，為目前世界第一個有拘
  際公約。

各國落實個人資料保護採取之策略—歐洲(1/2)

- 《**一般資料保護規範**》（英語：General Data Protection Regulation，縮寫作 GDPR；歐盟法規編號：(EU) 2016/679），是在歐盟法律中對所有歐盟個人關於資料保護和隱私的規範，涉及了歐洲境外的個人資料出口。GDPR 主要目標為取回公民以及住民對於個人資料的控制，以及為了國際商務而簡化在歐盟內的統一規範。
- GDPR取代了歐盟在1995年推出的歐盟個人資料《資料保護指令》（Data Protection Directive）95/46/EC，該條例包含有關處理歐盟內部資料主體的個人可識別資訊的條款和要求，適用於與歐洲做生意的所有企業，無論位置如何。

各國落實個人資料保護採取之策略—歐洲(2/2)

- 個人資料處理者必須清楚地披露任何資料收集，聲明資料處理的合法基礎和目的，保留資料的時間以及是否與任何第三方或歐盟以外的國家共享資料。
- 用戶有權以通用格式請求處理器收集的資料的便攜式副本，並有權在特定情況下刪除其資料。公共主管部門和以核心活動為中心定期或系統地處理個人資料的企業需要雇用資料保護官員（DPO）負責管理GDPR的合規性。如果資料洩露對用戶隱私產生不利影響，企業必須在72小時內報告任何資料洩露。
- 本法案在2016年4月27日通過，兩年的緩衝期後，在2018年5月25日強制執行[4]。根據歐洲聯盟運作條約第288條第2項，因為GDPR屬於歐盟條例（英語：regulation；德語：Verorderung），不是指令（英語：directive；德語：Richtlinie），所以不需經過歐盟成員國立法轉換成各國法律，而可直接適用。隨著英國在2019年脫離歐盟，它於2018年5月23日御准批准了2018年資料保護法案（Data Protection Act 2018），該法案包含了相應的法規和保護措施。

各國落實個人資料保護採取之策略—美國(1/2)

- 不同於歐盟重視以立法方式保護個人資料，美國向來強調業者自律，聯邦層級至今並無一部統一適用之個人資料保護法制，而是散見於各個不同部門之立法
  - 醫療及保險業紀錄：「健康保險流通與責任法案」（Health Insurance Portability and Accountability Act ）
  - 電話通聯記錄：「電子通訊隱私權法」（Electronic Communications Privacy Act ）
  - 有線電視用戶消費記錄：「有線通訊政策法」（Cable Communications Policy Act ）
  - 其他

各國落實個人資料保護採取之策略—美國(2/2)

- 為成為歐盟指令所稱之具「適當」資料保護法制之國家，2000年7月，美國與歐盟達成「安全港架構協議」（Safe Harbor Framework），並於同年11月生效¯參與本協議之美國業者可在美國商務部的監督管理之下，傳輸歐盟會員國國民的個人資料
- 安全港架構協議七大原則規範
  - 通知
  - 選擇
  - 同時傳遞
  - 安全
  - 資料之真實性
  - 存取
  - 執行

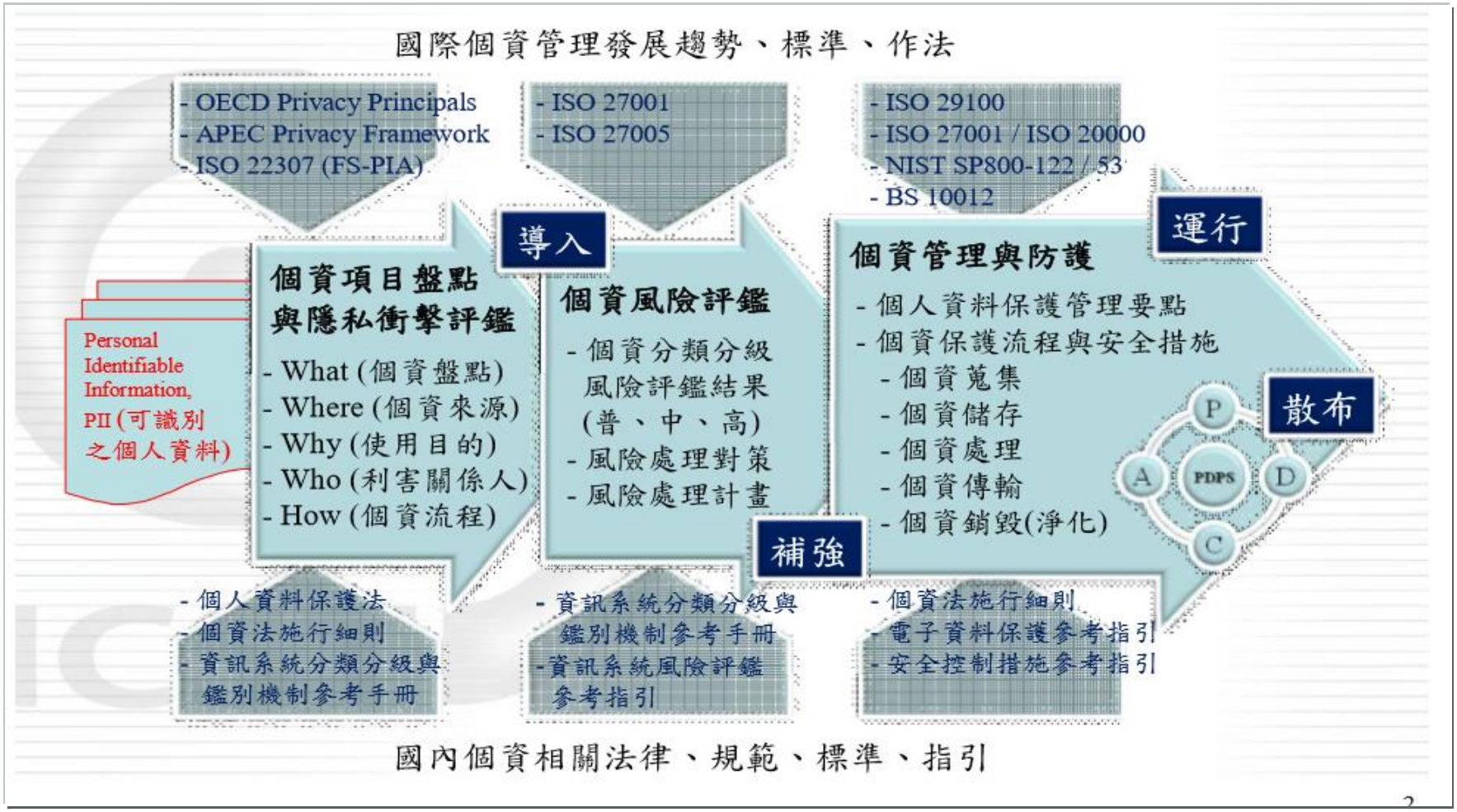
APEC推動跨境隱私保護

- 2004年10月通過「APEC隱私保護綱領」(APEC Privacy Framework)，針對APEC各會員體，推動整合性的個人資料保護措施
  - 2007年1月通過「跨境隱私保護規則」(Cross Border Privacy Rules, CBPR)，制定業者於跨國傳輸個人資料時所須遵循之規則
  - 2007年6月起，針對前述的跨境隱私保護問題，推動「開路者倡議實驗計畫」(Pathfinder)
  - 我國自1991年起成為APEC會員體，直接面對來自APEC及其他會員體的壓力

APEC推動跨境隱私保護

- **APEC跨境隱私保護開路者倡議計畫**
  - 1、建立企業自我評量準則
  - 2、建立信賴標章組織參與跨境隱私保護規則之準則
  - 3、檢視各組織遵守跨境隱私保護規則之狀況
  - 4、盧列協助進行跨境交易糾紛處理組織之名單
  - 5、盧列各經濟體掌管跨境資料隱私保護之官方單位及負責人名單
  - 6、建立界定跨境組織間合作之合約或備忘錄範本
  - 7、建立處理跨境交易糾紛之表單範本
  - 8、建立各經濟體主管單位執行跨境隱私保護之指導原則及程序
  - 9、發展執行跨境隱私保護準則及行動綱領之前導個案。

國際間個資管理的發展趨勢

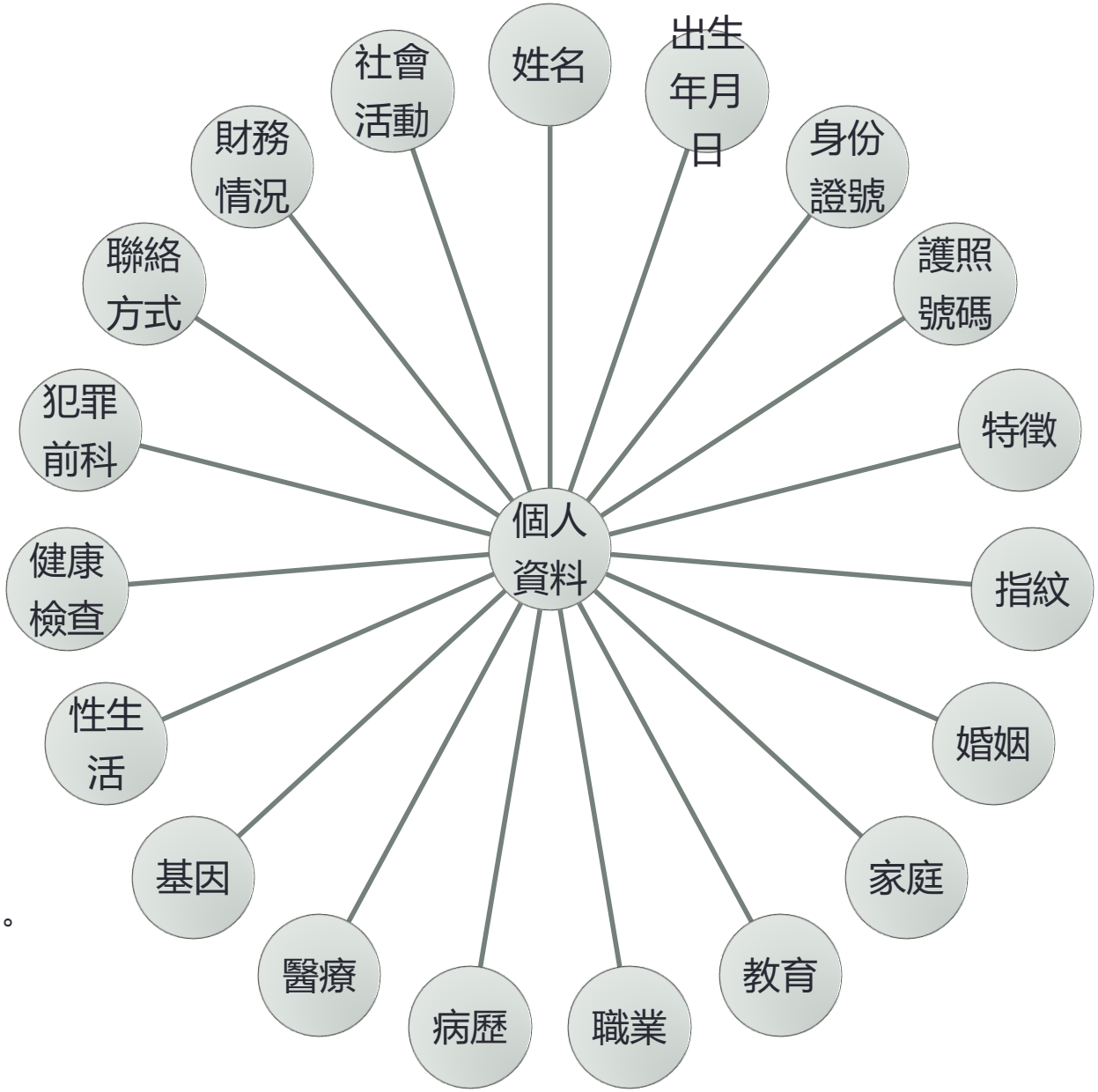


課程大綱

- 隱私權及個人資料保護法制發展
- 國內個人資料侵害案例
- 我國對個人資料保護的沿革
- 個人資料保護法的架構及相關條文
- 損害賠償及團體訴訟及罰則

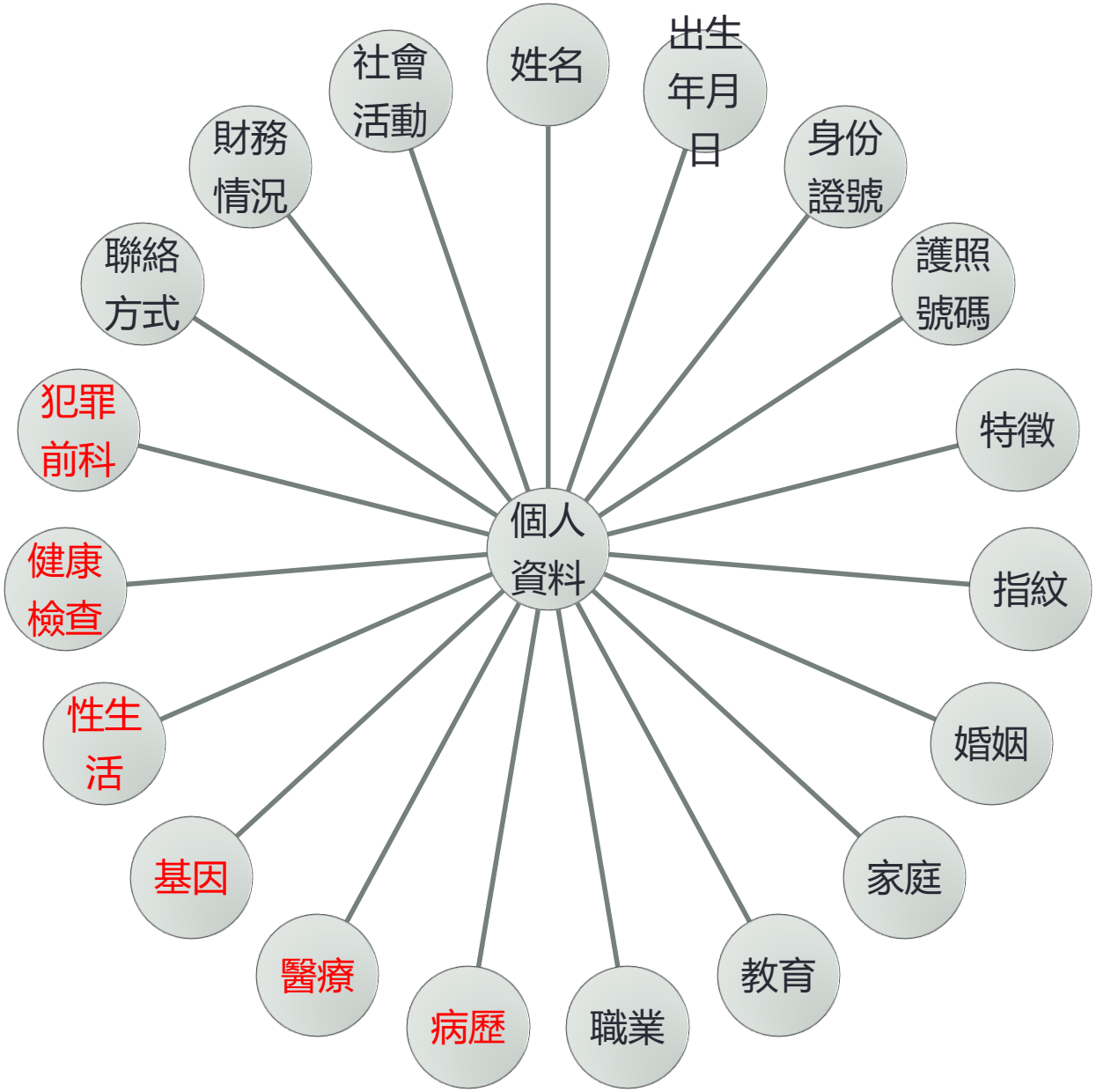
個人資料

- 依據個人資料保護法第二條
- 個人資料係指(生存)自然人之；
  - 姓名、出生年月日、身份證號、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。
- 其他可以直接或間接方式識別個人的各種資料。



特種個人資料

- 其中以紅色標示之項目，包含；
  - 醫療、基因、性生活、健康檢查、犯罪前科
  - 依據個人資料保護法第六條，原則上不得蒐集、處理、或利用特種個人資訊，即使經過當事人同意也不行。
    - 例外：法律規定或醫療、衛生、犯罪預防目的
- 法務部後新增列符合「增進公共利益所必要」、「蒐集者依規定取得當事人書面同意」兩要件，即可蒐集利用。



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	是否有結婚、配偶或同居人之姓名、前配偶或同居人之姓名、結婚之日期、子女之人數等。
教育	學校紀錄：大學、專科或其他學校等。
	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。
聯絡方式	傳統的聯絡方式：電話、地址。
	時尚的聯絡方式： Email、MSN、SKYPE、FaceBook、微博等。
	其他的聯絡方式：個人部落格、批踢踢(PTT)的帳號、Mobile01的帳號等。

類別	內容
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。
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。
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。

間接識別個資的定義

- 僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。
  - 如查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限

個資外洩發生的產業

- 2019/2發布「2019 4iQ Identity Breach Report」報告。報告中指出，2018年總計有12,449起新的身分外洩事件，比2017年增加424%。
- 若從外洩事件發生的產業別來看，論壇以27.5%位居第一，居次的是政府機關12.2%，遊戲產業占11.8%，電子商務網站占11.7%，教育/學術界則占9.2%。
- 2018年最大宗的個人身分資料外洩事件為澳洲安全專家Troy Hunt在駭客論壇上所發現的Collection ，包含逾11億組的電子郵件+密碼，以及超過7.7億個不重覆的電子郵件帳號。
- 值得注意的是，這些在網路上流竄的個人身分資訊只有37%是因為遭到駭客攻擊而外洩，卻有63%是因為意外才曝光。

歐盟《一般資料保護規範》GDPR實施

- 《一般資料保護規範》（General Data Protection Regulation，以下簡稱GDPR）號稱史上最嚴格的個資法規範，違法者最高可被判罰2千萬歐元（約合7.2億元新台幣）或全球營業總額的4%，兩者取其高。正因罰款近乎天價，全球企業無不繃緊神經。
- GDPR之所以成為全球企業共同關心的話題，除了影響範圍廣闊，只要蒐集、處理與利用歐盟公民個資的企業，不論是否設點於歐盟都受到規範之外，高額罰款更是最讓企業心驚膽顫的因素
- 處理個人資料的業務流程必須在設計和默認情況下構建資料保護，這意味著個人資料必須使用假名(pseudonmisation)或完全匿名(data anonymisation)進行存儲，並且默認使用盡可能最高的隱私設置，以避免公開資料未經明確同意，並且不能用於識別沒有單獨存儲附加訊息的主題。任何個人資料除非在法規規定的合法基礎上完成，否則資料控制者或處理者已經從資料所有者那裡獲得明確的選擇同意。資料所有者有權隨時撤銷此權限。
- GDPR的罰款根據規範分為兩種情境：若沒有合法理由，拒絕當事人刪除個資的請求、也沒有建立資料保護管理系統時，最高可罰3.6億元新台幣或全球年度營業總額2%作為罰款。
- 更嚴重的違規，如非法處理個資、資料外洩沒有主動通報、沒有任命資料保護長、違法向第三國傳輸個資等，最高將處7.2億元新台幣或全球年度營業總額4%作為罰款。不論是定額的3.6億元、7.2億元或營業總額比例，都將取其高者作為處罰。

GDPR法規提出的新三項權利解析

- 「被遺忘權」。歐盟對於被遺忘權的定義為：即資料當事人（Data subject) 在特定條件下，有要求資料控制者（Datacontroller）刪除其個人資料之權利，而且這裡的刪除規定相當嚴格，指的是資料當事人有權要求進行資料處理的第三方，刪除任何個人資料的連結（Links）、複本（Copy）或是再製（Replication）。
- 「資料可攜權」民眾對於自己的個資擁有更大的操控權，可以在不同的服務組織之間移動自己的個資，把資料從網路服務供應商（ISP）轉移至其他的服務廠商。
- 「個資自動化決策反對權」，能有避免「演算法歧視」的深刻含義。自動化決策意指：以自動化方式處理個人資料的分析與決策活動，此法條主要是為了避免演算法歧視，因此不能標示性傾向、宗教與種族等因素為決策標準，也因此企業在使用機器學習等自動化決策技術時，有責任告知資料當事人，電腦演算法決策的採用評判標準或依據。

Google違反GDPR遭罰

- 2019年1月29日間，法國個資監管機關CNIL(Commission Nationale de l'Informatique et des Libertés) 依據歐盟個資法GDPR(General Data Protection Regulation)對Google裁處了高達5,000萬歐元的罰鍰，主要針對Google在對用戶進行個人化廣告行為(ads personalization)時，就其所蒐集來的個人資訊，並未有公開處理的透明度、充足資訊以及有效的同意。
- 該案是由法國兩大民間團體「NOYB(None Of Your Business，其宗旨口號就是：” My Privacy is none of your Business”)」以及「LQDN(La Quadrature du Net)」，於2018年5月25日及28日GDPR甫施行後，立即向CNIL所提出之申訴；其中，LQDN還是受高達10,000名資權利受害者所委任。
- CNIL於接收該等申訴並確認其具有管轄權力後，旋即於同年9月就本進行在線檢查(online inspections)，以分析Google用戶瀏覽模式，佐以用戶使用Android手機建立Google帳戶時所得接觸之文件，來確認Google在個資蒐集、處理及利用程序上，有無違反法國當地個資法規以及GDPR之相關規定。
- 最終，CNIL於今年1月21日作出處分，認定Google在個資處理程序上違反了GDPR相關規定，並對其處以高達5,000萬歐元的罰鍰（依照GDPR規定，就罰鍰之裁處，最高可達2,000萬歐元或是違法公司全球營業額的4%，於本案，CNIL明顯是以後者來計算罰鍰）。
- 本案可說是GDPR施行後，具有指標性意義的鉅額裁罰，尤其在CNIL針對Google個資處理手法上的違反認定，更值得在歐盟國營運的台灣企業借鏡及關注。

個資外洩醜聞，Facebook 遭英國開罰

- 2018 年 3 月劍橋分析公司（Cambridge Analytica）被爆出非法從 Facebook 獲取超過 5 千萬人的個資，後來 Facebook 將受害人數上修到 8,700 萬。Facebook 早在 2015 年就得知劍橋分析公司違規，卻未公布這項訊息，反而將相關的資料銷毀。
- 英國資訊專員辦公室在 7 月 10 日宣布，由於 Facebook 沒有妥善的保護用戶的資料將裁罰 50 萬英鎊，約相當於台幣 2,000 萬元
- 歐盟已經生效的一般資 料保護規定(General Data Protection Regulation, GDPR)，針對資訊洩漏對個人、企業及政府所造成的影 響與日俱增
- 號稱「史上最嚴格個資法」的歐盟《一般資料保護規範》(General Data Protection Regulation, GDPR) 在 2018年 5月上路了

個資外洩集體訴訟

- 美國加州舊金山一份法庭文件顯示，因一宗觸犯隱私權之集體訴訟，Google 已同意支付 U.S.$ 8,500,000.的合解金。7位原告指控 Google 免費電子郵件服務之 Gmail 內建的 Buzz 社交網路工具，侵犯其隱私權。
- Google 於 2010 年 2 月 9 日推出將 Gmail 連絡人自動掛到 Buzz 之連絡人名單中的新功能，引發網友疑慮；目前 Google 已改變其組態，Gmail 用戶必須在 Buzz 工具下，另建可以公開的連絡人名單，隨時可以瀏覽、編輯、隱藏或封鎖。
- 和解金中 30%歸律師，7 位原先每人至多可獲得 U.S.$ 2,500.，其餘金額將存入專戶，資助致力於網路隱私或教育之相關機構。
- 資料來源：http://zh.wikipedia.org/zh-tw/Google_Buzz/ (2010-09-11)。

課程大綱

- 隱私權及個人資料保護法制發展
- 國內個人資料侵害案例
- 我國對個人資料保護的沿革
- 個人資料保護法的架構及相關條文
- 損害賠償及團體訴訟及罰則

我國對個人資料保護的沿革

- 電腦處理個人資料保護法之目的
- 為規範電腦或自動化機器處理個人資料，以保障人民權益，並促進個人資料之合理利用。（第一條）
- 中華民國八十四年八月十一日制定公布全文

電腦處理個人資料保護法之要點

- 參考限制蒐集、資料內容正確、目的明確化、限制利用、安全、保護、公開、個人參加、責任等各國通採之原則訂定本法。
- 明訂個人資料指自然人之姓名、出生年月日、身分證統一編號、特徵、家庭 、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。

公務/非公務機關

- 公務機關對個人資訊之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符
- 非公務機關對個人資料之蒐集或電腦處理，非有特定目的且經當事人書面同意或對當事人權益無害者，不得為之。（第六、八條）
- 非公務機關部分，除由法務部會同目的事業主管機關指定之事業、團體或個人外，受到現行法規範的對象，事實上僅有下列八者：
  - 徵信業；蒐集或電腦處理個人資料為主要業務者
  - 醫院
  - 學校
  - 電信業
  - 金融業
  - 證券業
  - 保險業
  - 大眾傳播業

電腦處理個人資料保護法修正案

- 近年來詐騙案件層出不窮，手法亦不斷翻新，不僅造成人民財產的損失，擾亂人民正常之作息，甚且威脅到人民生命之安全
- 在飽受不法詐騙集團的迫害後，一般人在驚恐之外，不禁會思索，為何歹徒對其家庭狀況能瞭若指掌，而質疑係公務機關將個人資料洩漏所致，引起政府對「電腦處理個人資料保護法」修訂之重視。

個人資料保護法修正原因

- 相關犯罪事件起訴成功率偏低
- 個資外洩單位不在法案列管範圍
- APEC組織要求成員國銜接
- 遏止及嚇阻詐騙事件

個人資料保護法進度


2010年
04/20 新版個人資料保護法二讀通過
04/27 新版個人資料保護法三讀通過
05/26 總統公布新版個人資料保護法
2011年
10/27公布個資法施行細則草案
2012年
10/01預計正式施行個資法

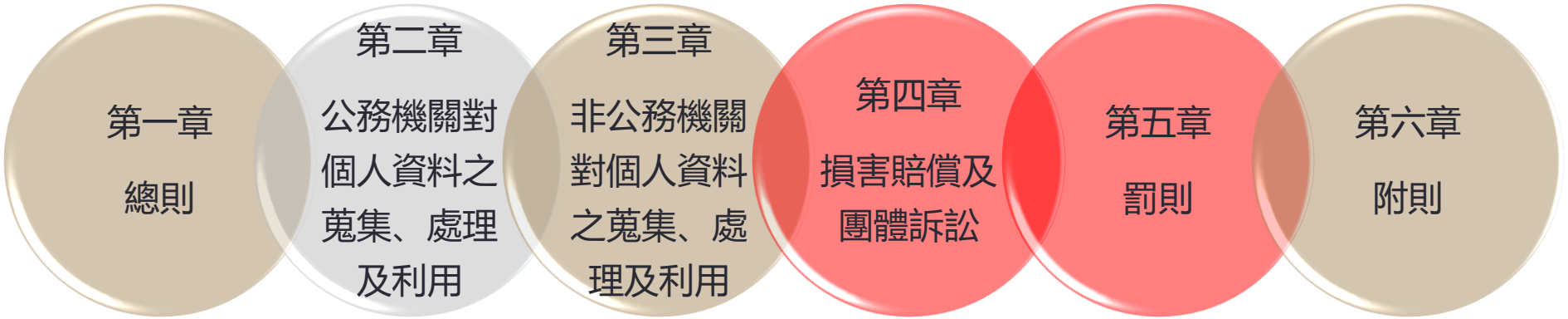
APEC資訊與隱私保護與個資法的對照

APEC資訊隱私保護9項原則	個資法條款
預防損害(Preventing Harm)	§12、§18、§27~§40
告知(Notice)	§7~§9
蒐集限制(Collection Limitations)	§6、§15、§19、§53
個人資料之利用(Uses of Personal Information)	§5、§16、§20
當事人自主(Choice)	§3、§10、§11、§13
個人資料之完整性(Integrity of Personal Information)	§11
安全管理(Security Safeguards)	§27
查閱和更正(Access and Correction)	§3、§10~§11、§13、§17
責任(Accountability)	§21

電腦處理
個人資料保護法施行細則

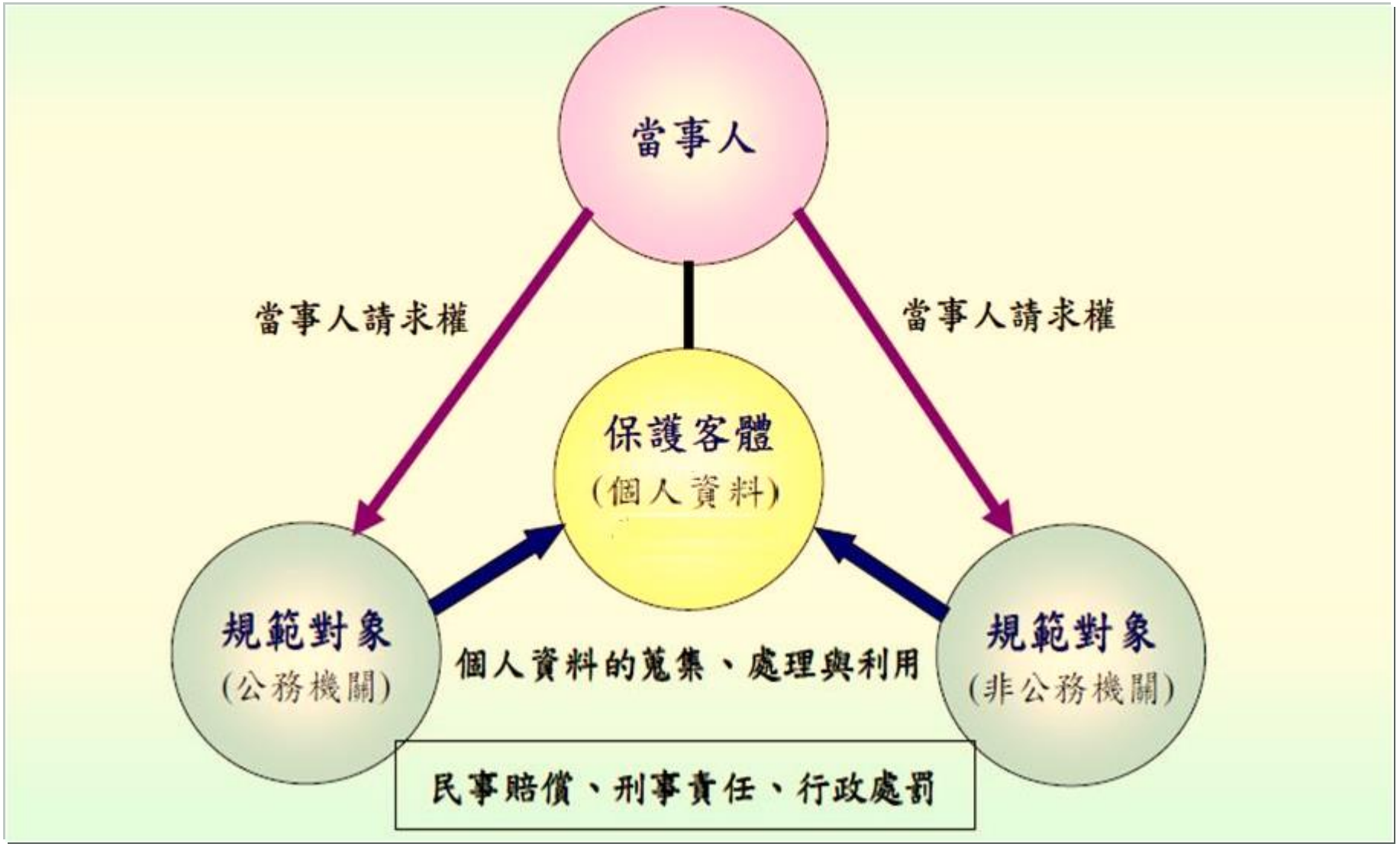
個人資料保護法施行細則

新版《個人資料保護法》的架構



個人資料保護法
(共56條)

個人資料保護法的主要架構



個人資料保護法的重要立法意旨(1/2)

1 擴大保護客體

納入人工與其它類型資料

以往外洩資料，企業辯稱是紙本而非“電腦資料”，本次從過去的「電腦處理個人資料保護法」修正為「個人資料保護法」，以避免這種現象產生。

2 普遍適用主體

刪除行業別之限制, 我國自然人/法人/公私機構一體適用

以前僅針對特定產業加以限制，但個資外洩的事件常發生在這些產業以外（如：電視購物業者），因此刪除行業別的限制，使大家一體適用。

3 增修行為規範

以往針對外洩才有裁罰，但現在針對特定的行為，如告知義務、書面同意方式等，企業如果未針對個資法要求的項目制定對應作法，即便個資未外洩，仍有行政裁罰的可能。

個人資料保護法的重要立法意旨(2/2)

4 強化行政監督

未來主管機關若懷疑公司有問題時，可以執行強制檢查，因此對業務將造成較大的影響。

5 促進民眾參與

建立團體訴訟機制

民眾滿20人可以提出團體訴訟，如此可增加民眾的參與，共同監督企業。

6 調整責任內涵

加重刑事責任、提高民事損害賠償總額限制、提高行政罰緩外，還可能對負責人(代表人,管理人)加以裁罰監督責任,，此外，公司還得自我舉證沒有個資外洩的情形，因此對企業將造成影響。

電腦處理個人資料保護法施行細則修正重點(1/2)

- 修正刪除之定義
  - 指使已儲存之個人資料自個人資料檔案中消失
  - 明定為事後查核、比對或證明之需要而留存軌跡者，得不予刪除 (LOG)
- 明定委託人應受託人為適當之監督
  - 建議明訂於委託契約
    - 個人資料之範圍、類別、特定目的及期間
    - 受託人應採取個人資料安全維護之必要措施
    - 複委託之受託人約定
    - 委託人保留指示之事項
    - 委託關係終止或解除之資料載體返還與資料刪除
- 書面之方式
  - 本法所規定之書面，如其內容可完整呈現，並可於日後取出供查驗者，經蒐集者及當事人同意，得以電子文件為之
  - 所稱單獨所為之書面意思表示，如係與其他意思表示於同一書面為之者，應於適當位置使當事人得以知悉其內容後並確認同意

「電腦處理個人資料保護法施行細則」修正重點(2/2

- 告知之方式
  - 本法第8條、第9條及第54條所定告知之方式，基於同一法律，應為相同之解釋 ；得以書面、電話、傳真、電子文件或其他適當方式為之
- 何謂執行職務或業務所必須而得不刪除或停止處理或利用個人資料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
  - 儲存方式特殊致不能刪除或耗費過鉅始能刪除
- 資料外洩之通知義務
  - 時間：即時
  - 方式：以電話、信函、傳真、電子文件或其他足以使當事人知悉之方式為之，但耗費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他足以使公眾得知之方式為之。
  - 通知內容：個人資料被侵害之事實及已採取之因應措施
- 過渡條款及施行日期
  - 本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得依本法有關個人資料保護之規定，繼續為處理及特定目的內之利用。其為特定目的外之利用者，應依本法修正施行後之規定為之。

課程大綱

- 隱私權及個人資料保護法制發展
- 國內個人資料侵害案例
- 我國對個人資料保護的沿革
- 個人資料保護法的架構及相關條文
- 損害賠償及團體訴訟及罰則

個資法適用範圍

蒐集

- 指以任何方式取得個人資料(包含直接或間接)

處理

- 指為建立或利用個人資料檔案註所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

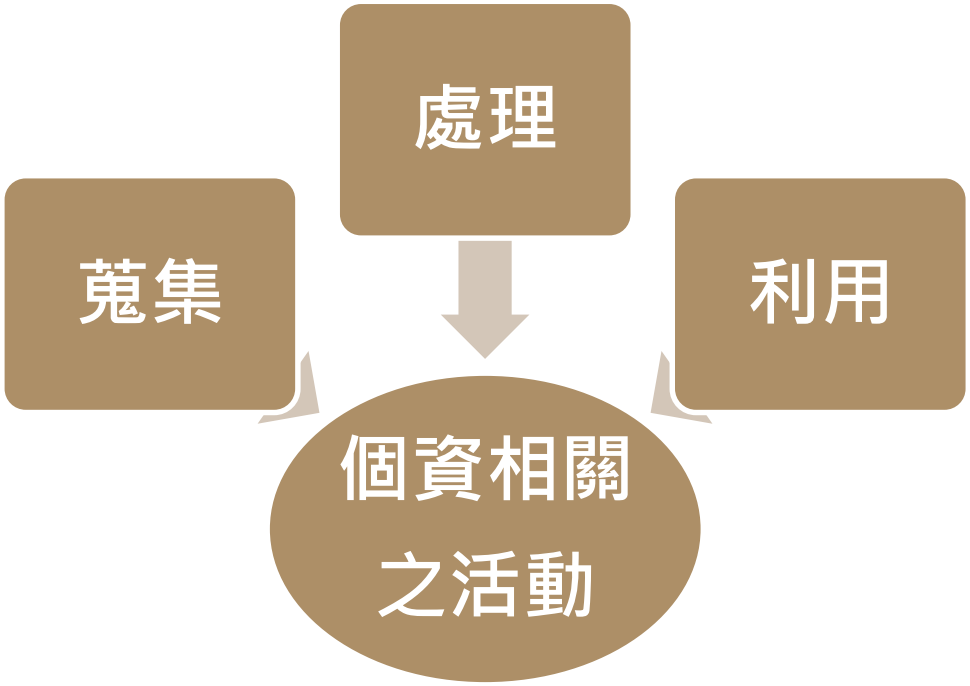
利用

- 指將蒐集之個人資料為處理以外之使用

國際傳輸

- 指將個人資料作跨國(境)之處理或利用

公務機關個人資料之蒐集、處理及利用



- 第18條-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。

個資法對公務機關的特別規範-蒐集與處理

- 第十五條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：
  - 執行法定職務必要範圍內
  - 經當事人書面同意
  - 對當事人權益無侵害

個資法對公務機關的特別規範-個資直接蒐集之免告知情形

- 依據個資法第八條，下列情形得免告知，直接向當事人進行資料蒐集：
  - 一、依法律規定得免告知
  - 二、個人資料之蒐集係公務機關執行法定職務
  - 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
  - 五、當事人明知應告知之內容

個資法對公務機關的特別規範- 直接個資蒐集之告知事項

- 依據個資法第八條，除上頁情形外，公務機關直接向當事人蒐集資料時，應告知當事人：
  - 一、公務機關名稱
  - 二、蒐集之目的
  - 三、個人資料之類別
  - 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

個資法對公務機關的特別規範-間接個資蒐集之告知事項

- 間接蒐集呢？
- 就是當我們不是直接向當事人(如民眾、客戶)直接蒐集個人資料，而是由從第三人、其他公司或是中央及地方其他行政單位索取資料時...

- 在處理或利用並非由當事人提供之個人資料**之前**，原則上都有義務告知當事人以下事項：
  - 個人資料來源。
  - 自己(對方)機關名稱。
  - 蒐集個人資料的目的。
  - 個人資料之種類或項目。
  - 個人資料利用之期間、地區、對象及方式。
  - 當事人依《個人資料保護法》第三條規定得行使之權利及方式。
- 當我們在業務上詢問民眾的個人資料時，**也得告知民眾以上資訊喔**！
- 如果對方沒有主動告知以上資訊，**我們可以要求對方先行告知喔！**

間接蒐集的個資

- 第54條；企業間接蒐集的個資，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。

處理或利用者，應於處理或利用前。

否則將按次使用個資，
處新臺幣2萬元以上、20萬元以下罰鍰

向非當事人間接蒐集時.....

- 第9條；第1項-公務機關或非公務機關依第15條或第19條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知下列事項：
  - 個人資料來源。
  - 公務機關或非公務機關名稱
  - 蒐集之目的。
  - 個人資料之類別。
  - 個人資料利用之期間、地區、對象及方式。
  - 當事人依第三條規定得行使之權利及方式。
- 第9條；第2項-但有下列情形之一者，得免為告知：
- 第8條第2項所列各款情形之一。
  - 當事人自行公開或其他已合法公開之個人資料。
  - 不能向當事人或其法定代理人為告知。
  - 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。
  - 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料

個資法對公務機關的特別規範

- 第15條-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。
  - 二. 經當事人書面同意
  - 三. 對當事人權益無侵害
- 第十六條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：
  - 一. 法律明文規定
  - 二. 為維護國家安全或增進公共利益
  - 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蒐集者依其揭露方式無從識別特定之當事人
  - 六. 有利於當事人權益
  - 七. 經當事人書面同意

個資法對公務機關的特別規範-公開事項

- 第十七條公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：
  - 一、個人資料檔案名稱
  - 二、保有機關名稱及聯絡方式
  - 三、個人資料檔案保有之依據及特定目的
  - 四、個人資料之類別

個資法對公務機關的特別規範-損害賠償

- 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。

「軌跡資料」的保護

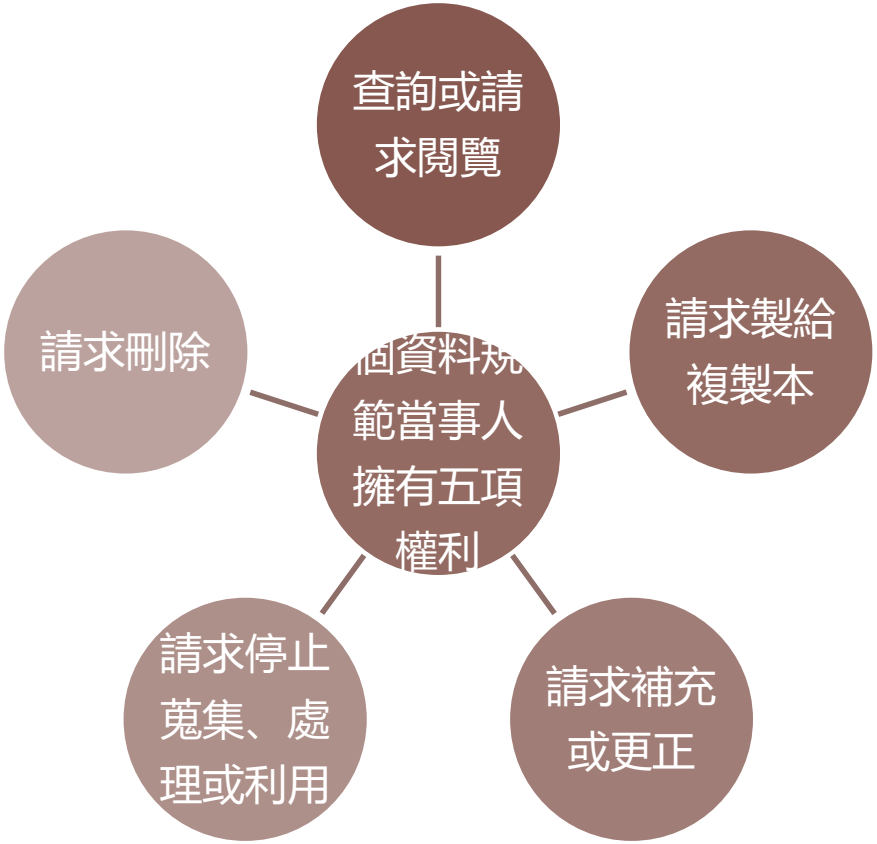
- 個資法施行細則草案，並且新版個資法施行細則修正草案條文中「第五條」，增加了對「軌跡資料」的保護，也就是企業營運環境中，只要與個人資料有牽扯到關系所產生的**「日誌檔案（Log Files）」**，那麼就必須要妥善保存備份以供日後查察（企業須負舉證責任）
- 凡指個人資料在蒐集、處理、利用過程中，所產生非屬於原蒐集個資本體衍生資訊（Log檔案）
- 包括（但不限於）當事人的帳號、存取時間、設備代號、網路IP位址等等。

委託他人(新增)

- 委託他人蒐集、處理或利用個人資料之全部或一部時，委託人應對受託人為適當之監督。
  - 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、受託人就第九條第二項應採取之必要措施。
  - 三、有複委託者，其約定之受託人。
  - 四、受託人或其受僱人違反個人資料保護法規或委託契約條款時，應向委託人通知之事項及採行之補救措施。
  - 五、委託人對受託人保留指示之事項。
  - 六、委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。
  - 第一項之監督，委託人應定期確認受託人執行之狀況，並將確認結果記錄之。
  - 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人

個資法規範當事人擁有權利

- 新版個人資料保護法規範當事人擁有以下五項權利：
  - 查詢或請求閱覽
  - 請求製給複製本
  - 請求補充或更正
  - 請求停止蒐集、處理或利用
  - 請求刪除
- 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」。



個資法規範當事人擁有權利

- 第3條；當事人就其個人資料依本法規定行使之權利，不得預先拋棄或以特約限制之。
- 第10條；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。
- 有下列情形之一者，不在此限：
  - 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 。
  - 妨害公務機關執行法定職務。
  - 妨害該蒐集機關或第三人之重大利益。

依法刪除資料

- 只要符合以下兩個條件，企業就得依法刪除資料：
  - 超過事業主管機關所訂的資料保存期限
  - 企業無執行業務的需求（合約到期）

課程大綱

- 隱私權及個人資料保護法制發展
- 國內個人資料侵害案例
- 我國對個人資料保護的沿革
- 個人資料保護法的架構及相關條文
- 損害賠償及團體訴訟及罰則

損害賠償及團體訴訟

- 團體訴訟
  - 為促進民眾參與個人資料保護事宜及損害發生後方便行使民事賠償權，新法特規定符合一定要件之財團法人或公益社團法人，得代替當事人提起團體訴訟，以節省勞費並保護民眾權益，並定有法院之專屬管轄。(第32-34條)
- 20個人以上就成團體
- 註：提起訴訟之財團法人或公益社團法人，應符合下列要件：
  - 1.財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。
  - 2.保護個人資料事項於其章程所定目的範圍內。
  - 3.許可設立三年以上。

賠償責任

- **公務機關-**提高賠償責任與罰則
  - 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。
  - 於公務機關在非天災等不可抗力因素外，導致個資外洩而侵害當事人權益時，
  - 得依每人每一事件新台幣5百元~**2萬**元以下；若造成多數人權益受損時，則由
  - 2000萬調高至2億。（第4章第28條）
- **非公務機關**
  - 能證明其無故意或過失者，不在此 限

個資損害求償的時效

當事人須於事件發生5年內提出求償

當事人知道損害事件後，於2年內要提出。

違反個資法的罰則

- 違反第六條第一項：有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、 處理或利用。但有下列情形之一者，不在此限：
  - 一、法律明文規定。
- 第十五條：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。
  - 二、經當事人書面同意。
  - 三、對當事人權益無侵害。
- 第十九條：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。

違反個資法的罰則

- 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。
- 第二十條第一項：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。
- 或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分， 足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬 元以下罰金。
- 意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以 下罰金。

違反個資法的罰則

- 公務
- 第44 條；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。
- 第45條 ：本章之罪，須告訴乃論。但犯第四十一條第二項之罪者，或對公務機關犯 第四十二條之罪者，不在此限。

- 非公務
- 第 47 條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（ 市）政府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： 一、違反第六條第一項規定。 二、違反第十九條規定。 三、違反第二十條第一項規定。 四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或 處分
- 第 48 條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（ 市）政府限期改正，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： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項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。
- 第 49 條 非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主 管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。
- 第 50 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。

個人資料保護法(通知)

第12條

非公務機關

個人資料被竊取、洩漏、竄改或 其他侵害者

當事人

應查明後以適當方式通知當事人

企業告知方式

第13條

- 得以書面、電話、傳真、電子文件或其他適當方式為之。

書面告知

- 本法第七條所定書面意思表示之方式，如其內容可完整呈現，並可於日後取出供查驗者，經蒐集者及當事人同意，得以電子文件為之。
- 本法第七條第二項所定單獨所為之書面意思表示，如係與其他意思表示於同一書面為之者，應於適當位置使當事人得以知悉其內容後並確認同意。

- 謝謝您的參與！

Turn Knowledge Into Valuable Services …