

通訊傳播事業法個資法遵教育及 實務案例分享

李怡親 法律研究員
資策會科技法律研究所
2023.09.18





講師介紹



姓名：李怡親（台灣會計師/美國會計師）

學歷：國立政治大學 會計學士

國立政治大學 法學學士

Columbia University 風險管理碩士

現職：資策會

法律研究員

經歷：紐約CIT Bank

風險分析師

安侯建業（KPMG） 審計員

安永（EY）

財務併購顧問



簡報 大綱

01

個資法遵重點提示暨 實務案例解析分享

個人資料保護法重點條文介紹

個資法、個資法施行細則、
個人資料檔案安全維護辦法

個人資料生命週期核心義務

自評表應提供證據

法律責任

裁罰案例

02

個資保護 實務教戰指引

個資盤點表

風險評鑑表

教育訓練

事故通報

紀錄機制

投入個資保護效益



01

個資法遵重點提示



個人資料保護法立法目的

避免人格權
受侵害

促進個人
資料之合理
利用





科技與隱私的兩難



Woman Catches her Boyfriend Cheating after Fitbit Records 'Physical Activity Spiked' at 4 AM

If you are a fitness freak and like to track a record of your physical activities in odd hours on your Fitbit, make sure you have a solid explanation.





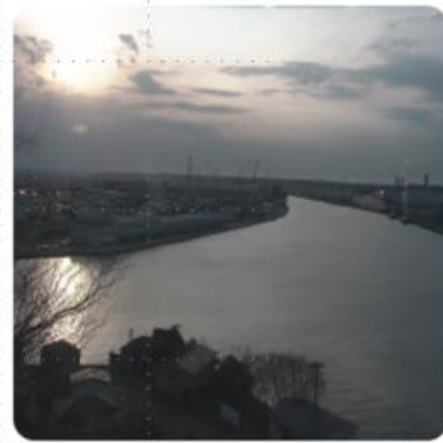
科技與隱私的兩難

《Insecam》
公開全球所有
使用預設密碼
IP網路監視器

台灣高達449
支影像曝光



Live camera in Ventspils, Latvia



Live camera in Ichikawa, Japan



Live camera in Aarau, Switzerland



Live camera in Asahi, Japan



科技與隱私的兩難



卻成為楚門的世界





近年常見重大個資/資安事件

公部門、關鍵基礎設施

2018.4	高雄果菜公司	駭客資料勒索
2018.12	台灣高鐵	高鐵票務系統被駭
2019.1	台北市衛生局	298萬筆市民個資外流
2019.6	銓敘部	59萬筆資料外流、公務員個資曝光
2020.5	中油、台塑	駭客癱瘓支付與內部系統
2021	內政部戶政資料	駭客在暗網兜售2357萬筆戶役資料
2023.3	華航	駭客勒索、會員個資外洩
2023	故宮	數千件國寶約十萬張圖檔遭竊賤賣

金融機構

2016.7	第一銀行	東歐駭客入侵盜領8327萬元
2017.2	13家證券公司	首起集體遭駭客勒索
2017.1	遠東銀行	被盜轉6010萬美元
2021.11	7家證券、期貨商	駭客撞庫攻擊、客戶被異常下單

科技業

2018.8	台積電	生產線停擺、營收損失達52億
2019.3	廣達	東歐駭客冒名詐取貸款
2019.3	華碩	軟體更新檔被入侵影響上萬台電腦
2020.11	鴻海、仁寶、研華	駭客資料勒索
2021	宏碁、日月、光、廣達、技嘉、東元	勒索軟體攻擊
2022	竹科7家半導體廠商	駭客展開持續性滲透威脅 (APT) 行動

民生消費

2017.5	雄獅旅行社	36萬筆個資外洩，導致客戶被詐騙
2023.1	iRent	40萬筆個資外洩
2023.1	誠品等5家電商	刑事警察局點名為高風險賣場
2023.2	微風	90萬筆個資外洩



為何發生個資外洩

臺灣以中小企業為主，個資保護資源少

中小企業由於預算與人力有限，無法投入多餘資源來導入個資保護政策，且發生遭駭事件，怕事跡外洩造成消費者對品牌不信任，多數皆知情不報



電商個資外洩威脅日益嚴重



2022年全台詐欺財損近
新台幣70億

- 電商賣場網站為求快速上架，一般程式設計完成，**未進行完整測試個情境之資安風險**
- **防護機制或防火牆未做好**，少一道資安程序，即成為駭客攻擊程式弱點，輕鬆盜取消費者個資。
- **駭客侵入網站竊取個資**，再將個資販賣給詐騙集團。

常見個資風險態樣

- 1) 因內控稽核或業務過失因素致個資外洩
- 2) 個人資料檔案安全維護措施未臻周延
- 3) 發生個資外洩事件時通報作業未臻周延
- 4) 蒐集個人資料時未盡明確告知義務
- 5) 未經客戶同意將其個人資料提供給第三人使用



電商企業個資保護所面臨困難

- 組織人力精簡，員工多身兼數職
- 人員缺乏足夠個資法遵資訊，無法提供完整個資保護
- 企業資安應變多成為救火，所發生過的個資外洩事件頻頻再現
- 許多單位為了避免遭駭事跡外洩，往往都知情不報，將違反個資法規



哪類個資外洩狀況最嚴重？

- 依據Gogolook 2022年調查報告：台灣前三名分別登入密碼、電話號碼、姓名

	 台灣	 泰國	 馬來西亞	 日本	 韓國
第一名	登入密碼	登入密碼	登入密碼	姓名	姓名
第二名	電話號碼	電話號碼	電話號碼	登入密碼	登入密碼
第三名	姓名	姓名	姓名	電話號碼	電話號碼
第四名	國籍	國籍	地址	國籍	國籍
第五名	Email	地址	國籍	地址	地址
第六名	地址	出生年月日	出生年月日	Email	Email
第七名	出生年月日	Email	Email	出生年月日	出生年月日

資料來源：Gogolook

個資外洩主要態樣

- 帳號資料外洩：實務上常見手法係取得被害人帳號後，利用該帳號出售或購買商品，以詐取金錢或物品。
- 身分資料外洩：實務上易遭外洩之身分資料，通常是個人姓名、出生年月日、身分證統一編號等足使他人辨識特定個人之資料。取得該等個資者往往會出售，或利用該等個資進行交易、開設新帳號（人頭帳戶），以進行身分犯罪（Identity Crime）。



密碼強度不足

- 猜測密碼/暴力破解
- 裝置失竊
- 帳密伺服器資料外洩
- 網路釣魚

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	vip	< 1 Second	27,458
2	123456	< 1 Second	4,110
3	1234	< 1 Second	3,421
4	000000	< 1 Second	1,361
5	1qaz2wsx	< 1 Second	1,219
6	12345	< 1 Second	1,197
7	12345678	< 1 Second	1,059
8	1111	< 1 Second	882
9	123	< 1 Second	847
10	123456789	< 1 Second	800

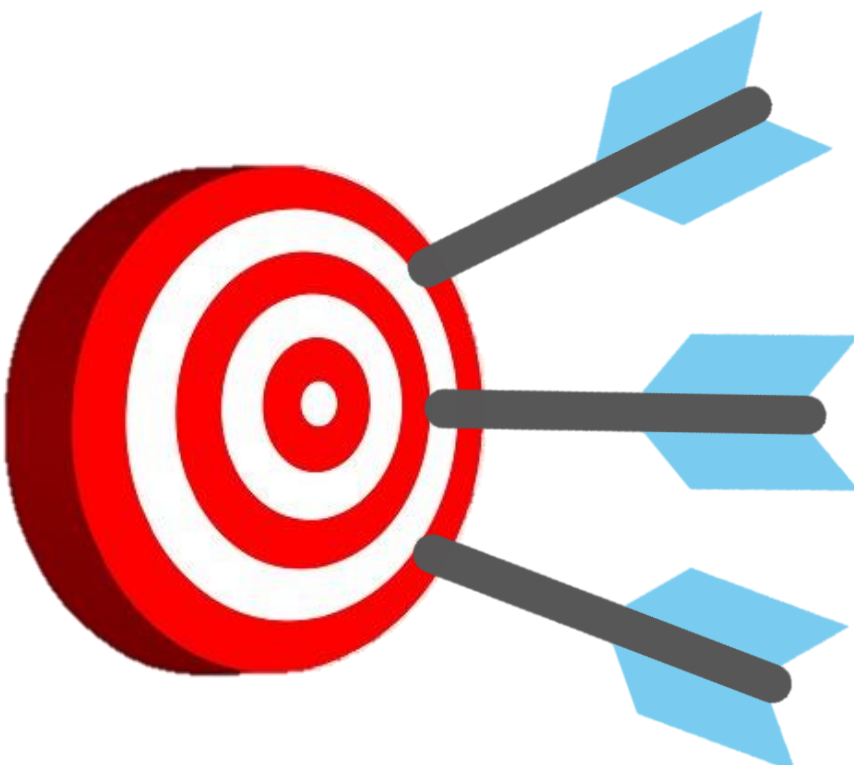


威廉王子意外洩密





防個資外洩 國發會射3箭



設立個資保護獨立監督機關

- 新增個資法第1條之1，成立個人資料保護委會
- 籌備處預計於八月成立
- 具獨立性、專責性及機關性



提高個資法相關罰則

- 非公務機關未善盡安全維護義務，罰鍰提高到新台幣2萬元以上、200萬元以下，屆期末改正將按次處罰；
- 對情節重大者，上修罰鍰為15萬元以上、**1,500萬元以下**



強化聯繫會議功能

- 強化執法能量，提升防護能力
- 精進案件通報與監督程序
- 落實執法及強化**行政檢查**



個資檔案安全維護規範現況-2023年

統計截至2023/08

主管機關	業別	辦法數
數位部	網際網路零售業及網際網路零售服務平台業	1
經濟部	綜合商品零售業、製造業及技術服務業、自來水事業、電業及公用天然氣事業、著作權集體管理團體	5
金管會	金融控股、銀行、證券、期貨、保險、電子支付、其他經金管會公告之金融服務業、財團法人	1
通傳會	國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法	1
交通部	民用航空運輸業、船舶運送業、汽車運輸業、交通部指定非公務機關（觀光旅館業、旅館業、民宿、旅行業、觀光遊樂業）、停車場經營業	5
教育部	短期補習班、私立兒童課後照顧服務中心、私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、運動彩券業、海外臺灣學校及大陸地區臺商學校	6
內政部	交友服務業、殯葬服務業、營建類非公務機關、移民業務機構、祭祀團體、政黨及全國性民政財團法人、宗教團體、地政類非公務機關、合作及人民團體類非公務機關、警政類非公務機關	10
勞動部	私立職業訓練機構、人力供應業、人力仲介業	3
衛福部	醫院、精神復健機構、私立長期照顧服務機構、護理機構、社會福利機構、中藥批發零售業、化粧品批發零售業、醫療器材批發零售業、西藥批發零售業、非輻射電子醫療器材設備製造業、食品業	11
財政部	報關業、保稅倉庫物流中心、記帳士與記帳及報稅代理人、菸酒事業、公益彩券發行機構	5
公平會	多層次傳銷業	1
工程會	工程技術顧問業	1
原能會	游離輻射設備製造業	1
中央銀行	票據交換所	1
農委會	農藥販賣業、農業金融	2
陸委會	大陸委員會指定非公務機關	1
僑委會	僑務委員會指定特定非公務機關	1
合計		



訂定安全維護計畫

- 適用範圍（本辦法§ 2）

本辦法所稱非公務機關包括下列各款：

- 電信事業。
- 用戶數達三千戶以上之提供網際網路接取服務之設置未使用電信資源之公眾電信網路者。
- 有線廣播電視系統經營者。
- 電視事業。
- 訂戶數達三千戶以上之直播衛星廣播電視服務事業。
- 經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業。
- 電信消費爭議處理機構。
- 其他經國家通訊傳播委員會（以下簡稱本會）公告之通訊傳播事業。



國家通訊傳播委員會

指定非公務機關個人資料檔案安全維護辦法

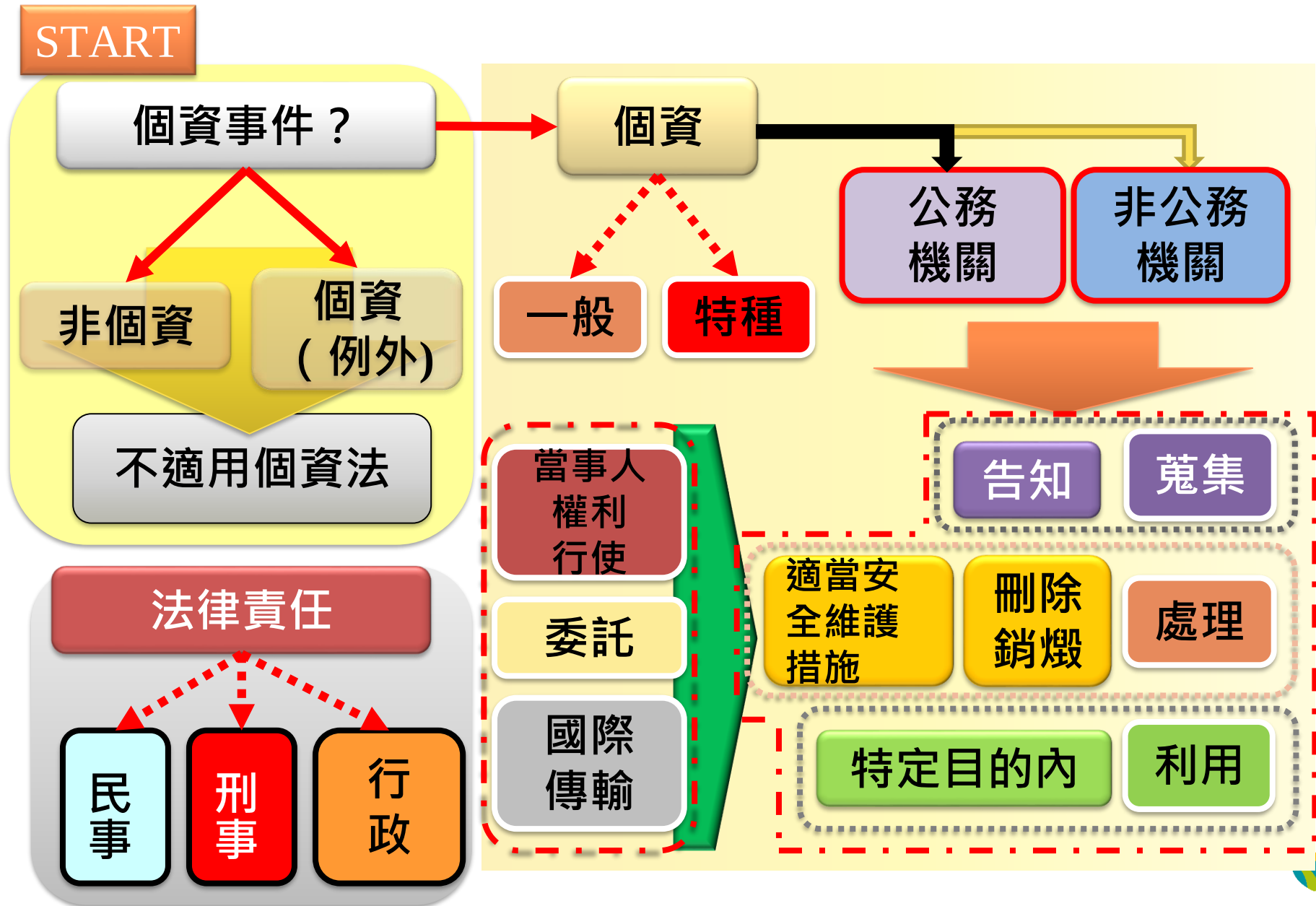
● 非公務機關應就下列事項，訂定個人資料之管理程序（本辦法§5）：

- ◆ 蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其**特定目的**及是否符合相關法令之要件。
- ◆ 檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及**告知**之內容、方式是否合法妥適。
- ◆ 檢視個人資料之蒐集、處理，是否符合本法第十九條規定，**具有特定目的及法定情形**；其經當事人同意者，並應確保符合本法第七條第一項規定。
- ◆ 檢視個人資料之**利用**，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合本法第七條第二項規定。
- ◆ 利用個人資料為**行銷**，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

- ◆ 委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。
- ◆ 進行個人資料**國際傳輸**前，檢視是否受本會相關法令限制並遵循之。
- ◆ 當事人行使本法第三條所定**權利**之相關事項：
 - 當事人身分之確認。
 - 提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。
 - 對當事人請求之審查方式，並遵守本法有關處理期限之規定。
 - 有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。
- ◆ 檢視個人資料於蒐集、處理或利用過程中是否**正確**；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。
- ◆ 檢視所保有個人資料之特定目的是否**消失**，或**期限是否屆滿**；其**特定目的消失或期限屆滿**者，應依本法第十一條第三項規定辦理。
- ◆ 設置聯絡窗口供**當事人申訴與諮詢**。

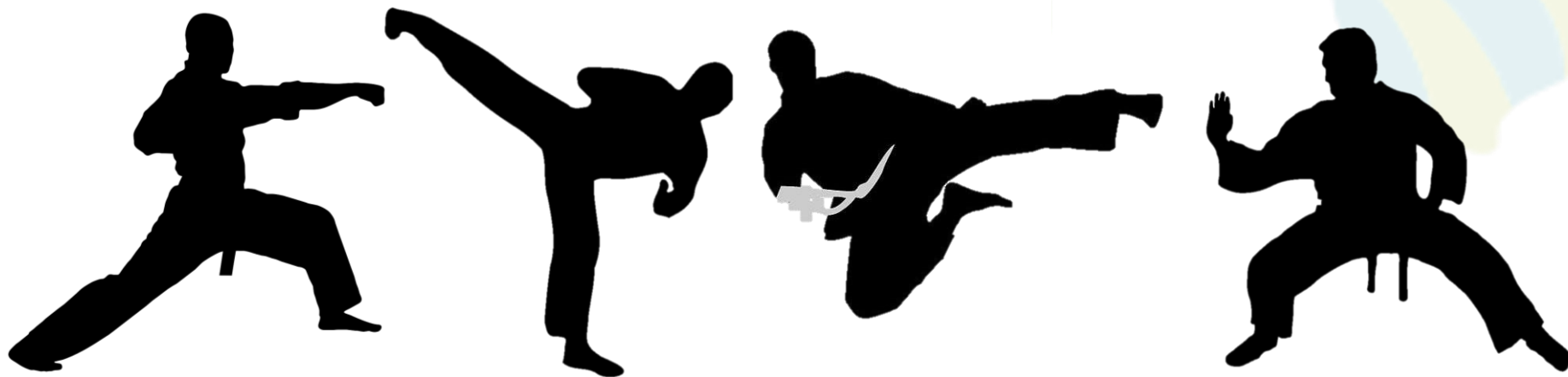


個資法規範架構暨個資全生命週期





個資管理-四字真經





PDCA方法論





臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

個人資料保護規劃



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



指定非公務機關個人資料檔案安全維護辦法

● 配置資源（本辦法§ 3）

- ◆ 非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）。
- ◆ 本計畫及處理方法之訂定或修正，應經非公務機關**負責人或法定代理人**簽署。
- ◆ 非公務機關蒐集、處理及利用達**五千名用戶**之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫。



組織人員配置

- 最高管理階層
 - 核定個資保護政策及安全維護計畫之訂定或修正
 - 決定權限與責任分工
- 管理代表
 - 視組織需求，最高管理階層可指派管理代表，負責執行個資保護管理制度
- 個資管理人員
 - 於日常業務執行個資保護管理制度

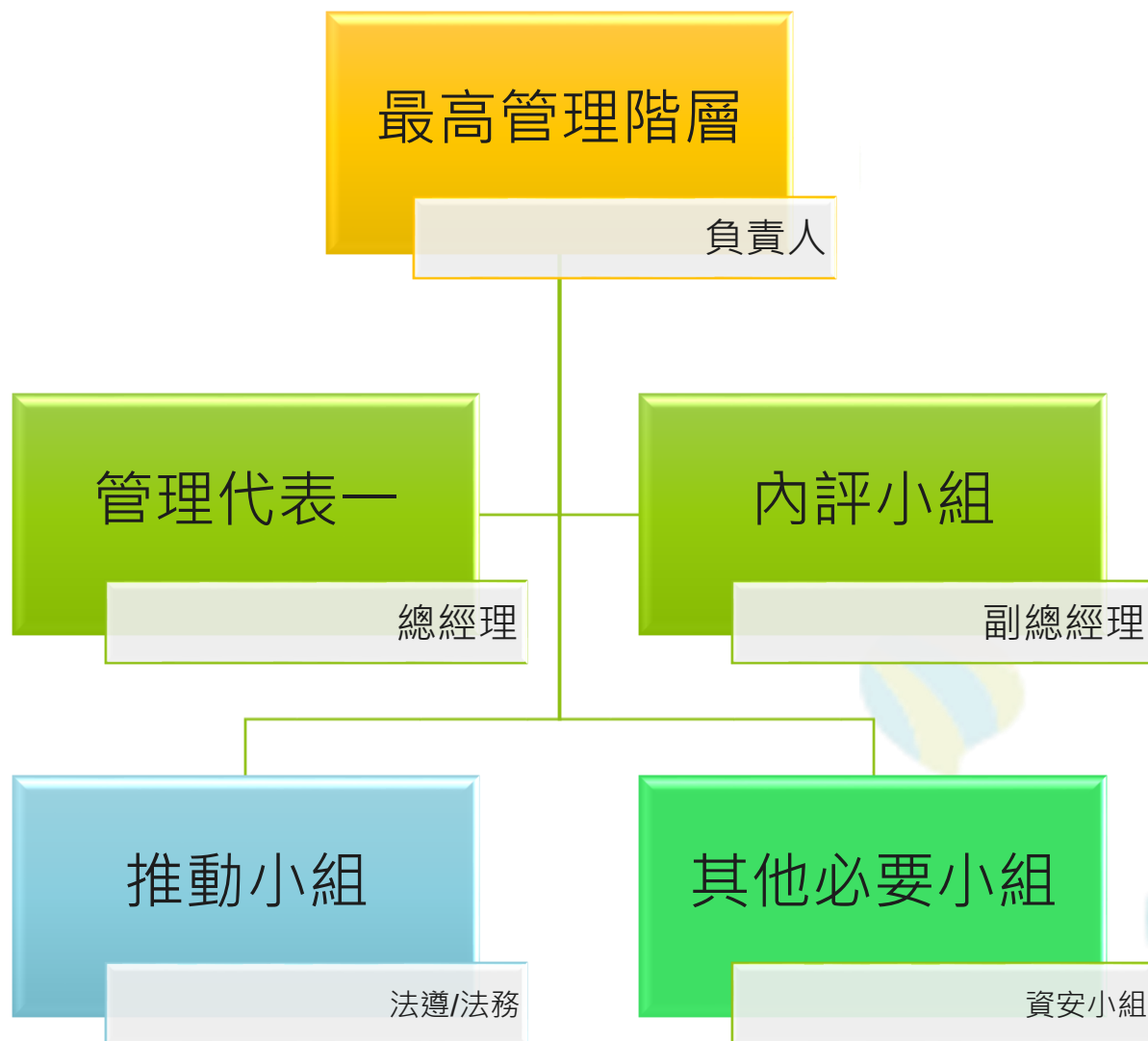


最高管理階層

- 最高管理階層之責任應包括：
 - 決定個人資料管理制度目標，確保符合組織需求與發展策略。
 - 決定個人資料保護管理政策。
 - 決定資源管理。
 - 決定個人資料保護管理組織架構及權責劃分。
 - 定期檢視管理制度，確保管理制度達成預期效果。
 - 建立有效的溝通機制，適時指導與支援組織人員。
 - 傳達落實個人資料管理制度之重要性。

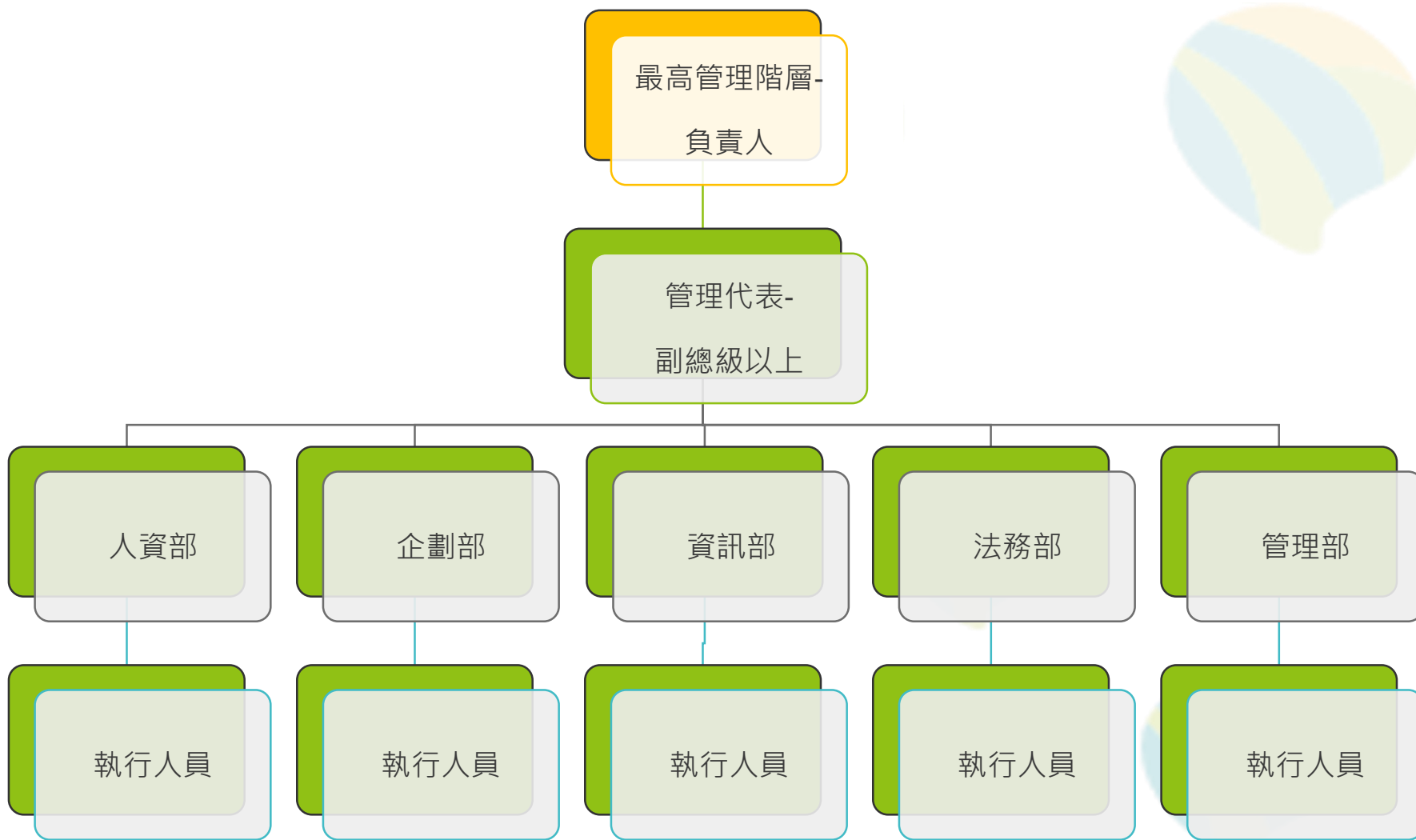


參考架構-任務型





參考架構-組織型





自評表

填表公司：

填表人（及聯絡電話）：

編號	查核項目(相關規定)	建置(執行)情形	具體措施(含佐證資料)及補充說明 (參考依據或說明)
1※	公司是否投入必要資源，以訂定適當之個人資料(以下簡稱個資)保護管理措施及配置管理人員？ (相關規定：個資法第27條第1項、施行細則第12條第2項、辦法第3條第12項)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件*) 1.管理規範 2.各管理措施SOP



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

個資法規介紹



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



個人資料保護法施行後再次修正

2010.04.27

個人資料
保護法
三讀通過

2010.05.26

總統令
公布
個人資料
保護法

2012.09.26

施行細則
正式公告

2012.10.01

個人資料
保護法
正式施行

2015.12.30

個人資料
保護法
修正

2016.03.15

個人資料
保護法修
正條文暨
細則施行

2023.05.31

個人資料
保護法
增修部分
條文

個資母法>>>施行細則>>>各機關辦法>>>行業標準

行為規範

新增特種個
資病歷
&例外特定
情形

行為規範

同意不再侷
限於「書面
同意」

行為規範

增、修訂免
告知事由&
法定情形

行為規範

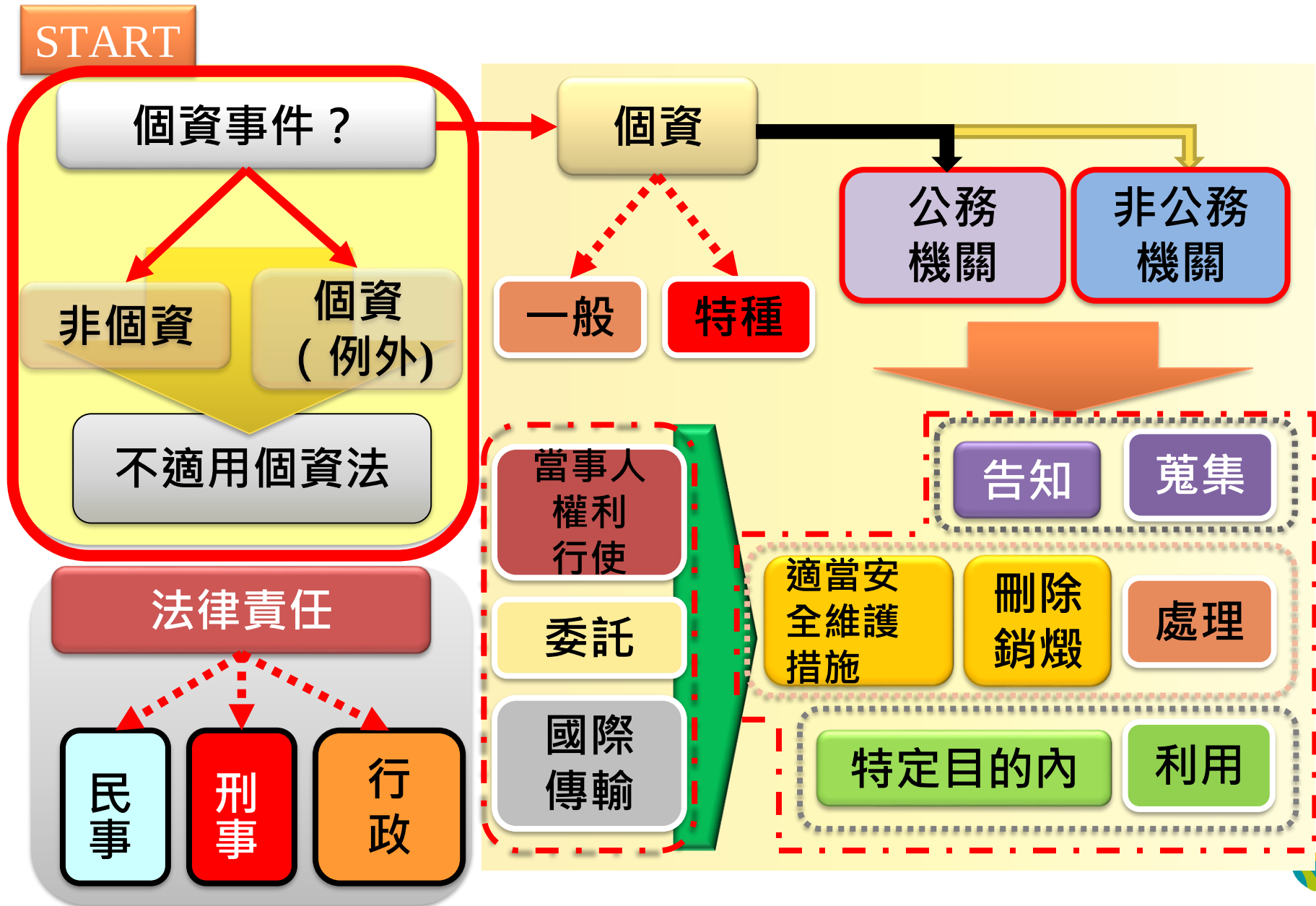
間接蒐集
告知義務

責任內涵

與意圖營利
相關之刑責
修正



個資法規範架構暨個資全生命週期





Q：照片於上網分享，是否適用個資法？



乾隆皇帝

1小時前



這幾年 終究是錯付了



甄環、孫答應、沈眉庄和其他13位小主說這個讚

A：親友照片於網路上分享，是否適用個資法？

法律字第 10203502790 號函：

自然人為單純個人活動目的，而將其親友個人資料（例如：照片、影片或電話），於網路上分享予其他友人等利用行為，**尚無本法之適用**。

但是若上開行為若有侵害民眾人格權或隱私權者，受害人仍得根據民法第 18 條、第 184 條及第 195 條等規定，請求法院除去侵害或防止侵害及損害賠償，併予敘明。



Q：肉搜OL波多野，有個資法適用？

- 陳姓男子搭捷運，赫見滑手機女子，貌似日本AV女優波多野結衣，拍下後請吳姓女友人PO上Ptt表特版，發動請鄉民代為「神人」，其中坐在博愛座的蕭姓女乘客也入鏡，獲知上了表特版，卻發現主角不是她，更有鄉民消遣說「第二張那阿婆在看你」，蕭女怒不可遏，告陳男及吳女妨害秘密及違反個資法。是否有個資法之適用？





A：公開場所照片，無法識別個人

- 士林地檢署以照片是在公開場所拍攝，未拍到蕭女隱私部位，且沒註明蕭女姓名及電話，不構成妨害秘密及違反個資法，因罪嫌明顯不足，並未傳喚陳男及吳女到案說明，全案不起訴處分。（個資法第51條第1項第2款）



個人資料的定義

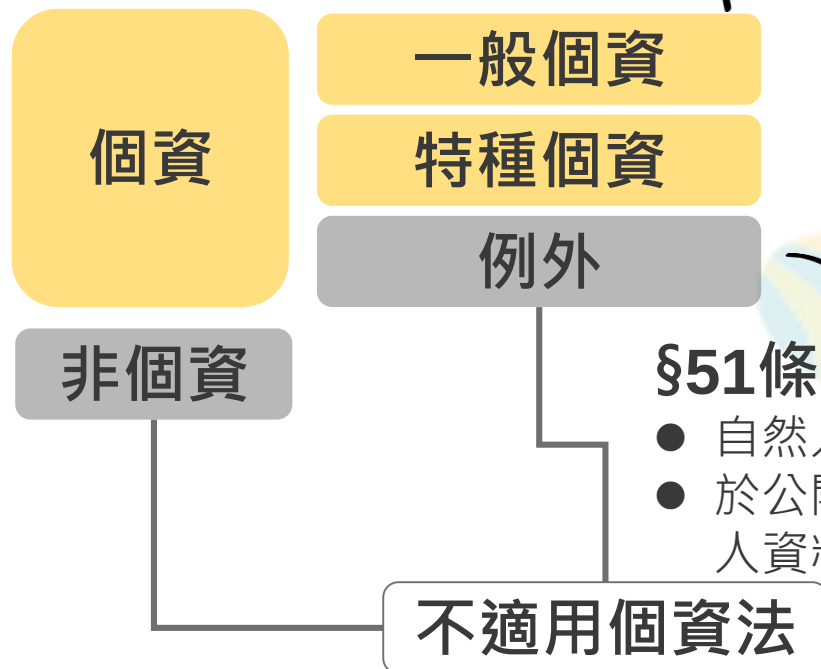
亡者資料？

§2條

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

§6條

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，原則上不得蒐集、處理或利用。



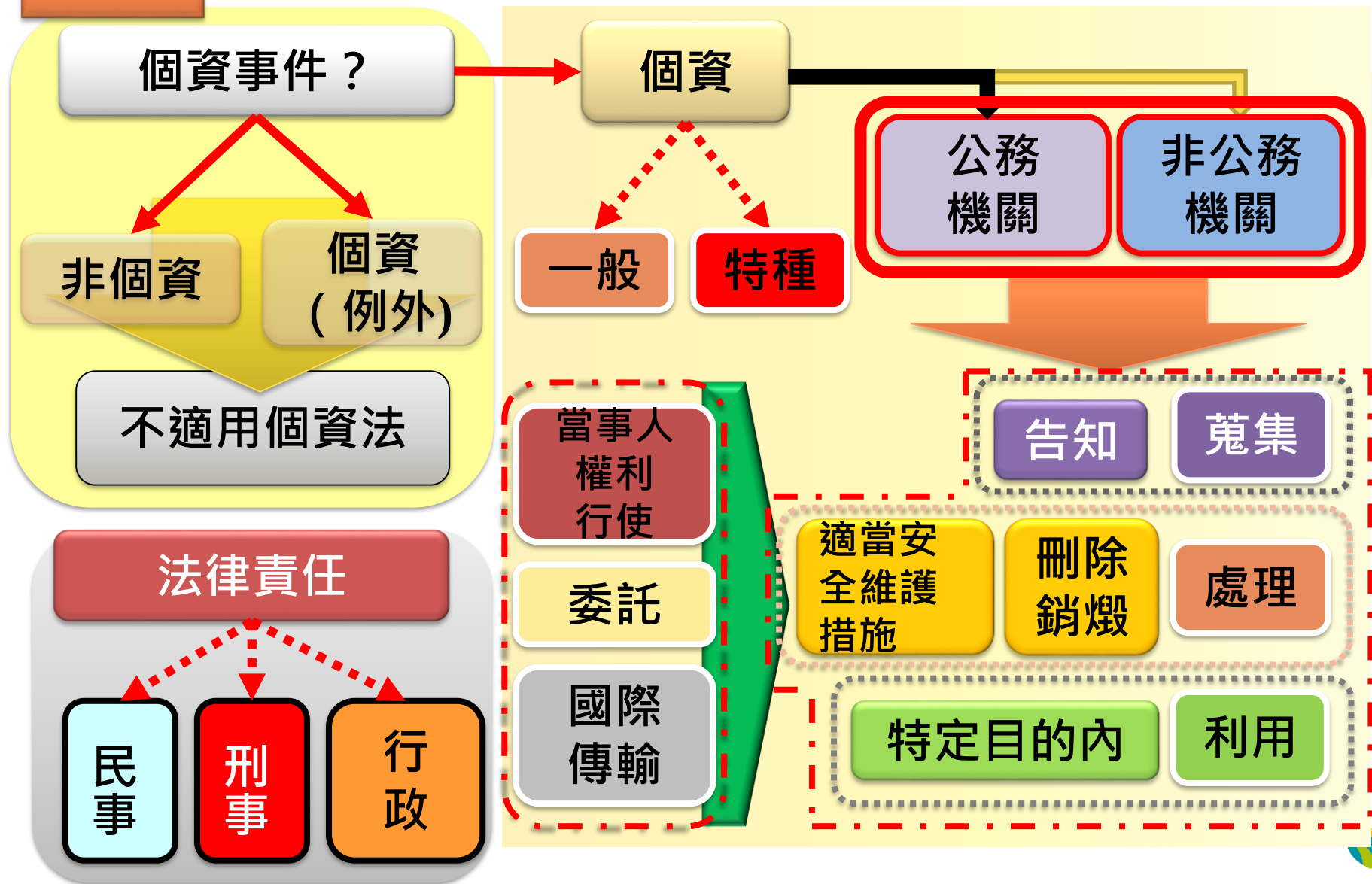
§51條

- 自然人 + 單純個人或家庭活動之目的
- 於公開場所或公開活動 + 未與其他個人資料結合+影音資料。



個資法規範架構暨個資全生命週期

START





公務機關與非公務機關

- 區分實益

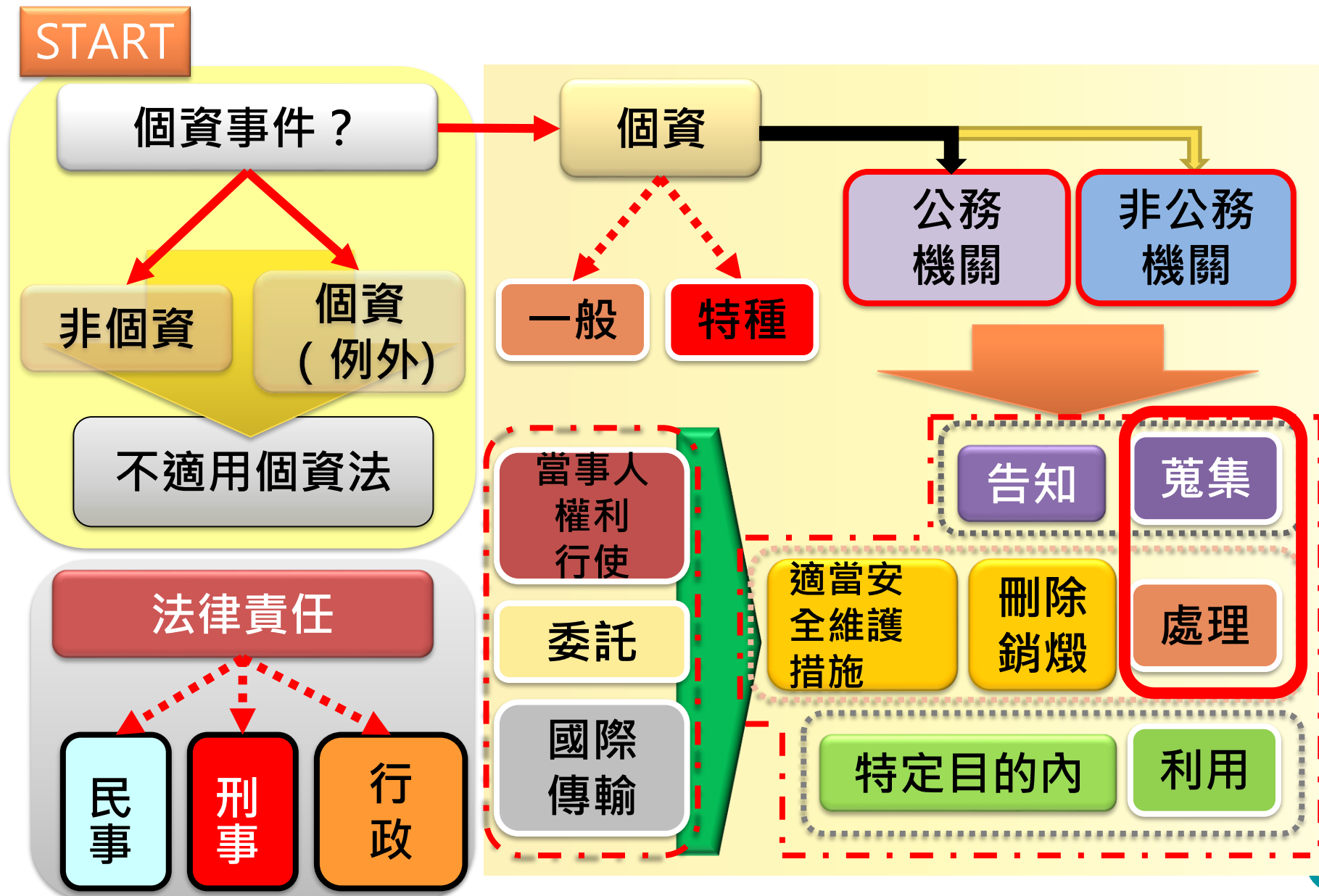
	公務機關	非公務機關
定義	指依法行使公權力之中央或地方機關或行政法人。	指公務機關以外之自然人、法人或其他團體。
蒐集、處理及利用	第二章 (個資法第15 - 18條)	第三章 (個資法第19 - 27條)
賠償責任的免除	不可抗力	無故意或過失
損害賠償責任依據	個資法+國賠法	個資法+民法

- 適用範圍

對象/行為主體		我國人民	外國人民
我國公務&非公務機關	我國境內為之	適用	適用
外國公務&非公務機關			
我國公務&非公務機關	我國境外為之	適用 (第51條第2項)	不適用
外國公務&非公務機關		不適用	不適用



個資法規範架構暨個資全生命週期





蒐集、處理與利用？

蒐集

指以任何方式取得個人資料。

處理

指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。

利用

指將蒐集之個人資料為處理以外之使用。

如：依據顧客所留之地址資料來遞送貨物，或依客戶資料檔案所留電話號碼進行資訊聯繫等行為，均屬於對個人資料之利用。



非公務機關蒐集、處理要件

■ 個人資料保護法§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（八款）情形之一者：
 - 一、法律明文規定。
 - 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。
- ◆ 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。

注意：蒐集要件亦為處理要件

特種個人資料之蒐集、處理及利用限制

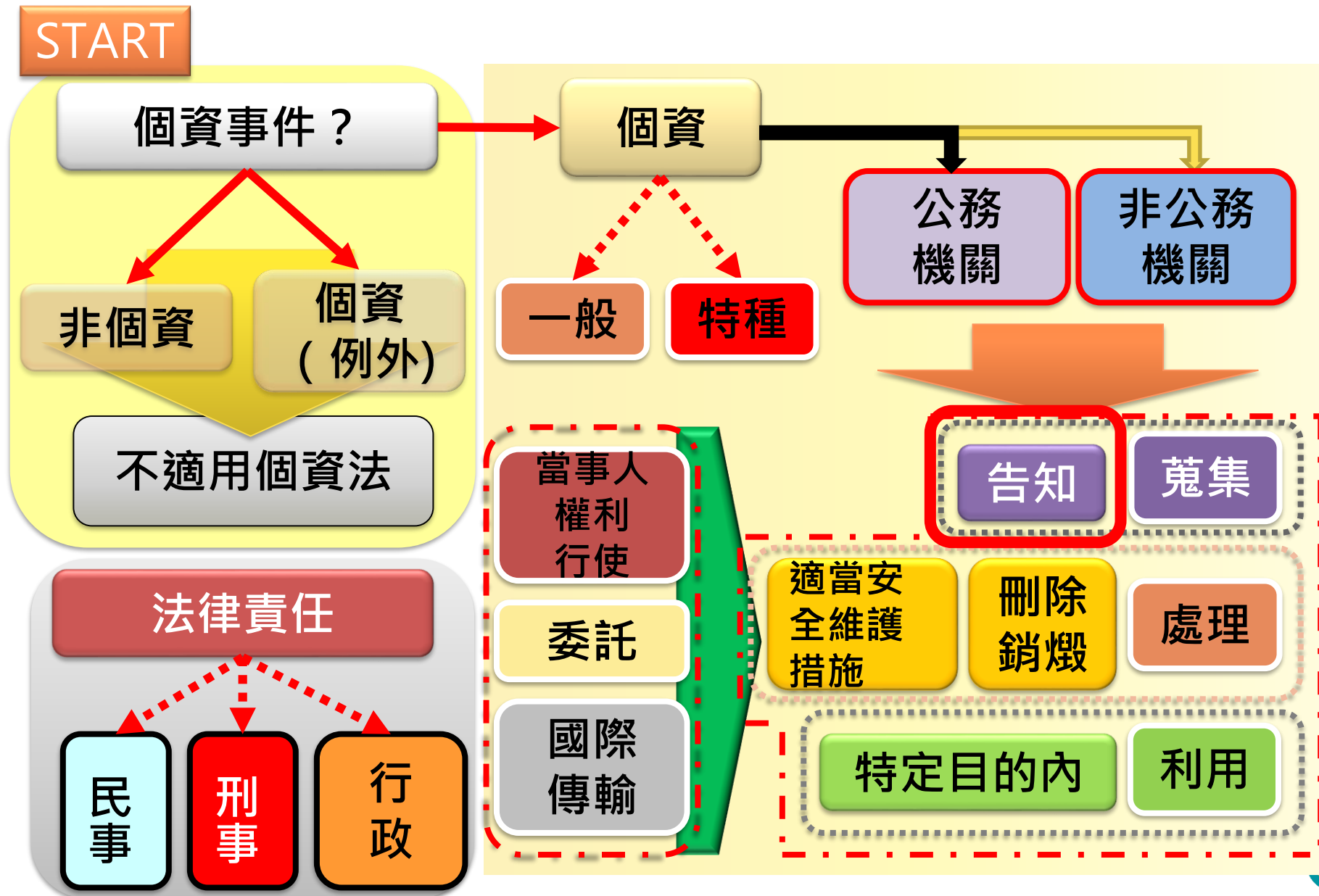
■ 個人資料保護法§6 I

有關**病歷、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。
- 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。
- 三. 當事人自行公開或其他已合法公開之個人資料。
- 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。
- 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。



個資法規範架構暨個資全生命週期





直接/間接告知義務

	直接蒐集時之告知義務	間接蒐集時之告知義務
法源依據	個人資料保護法§8	個人資料保護法§9
告知時機	直接蒐集	間接蒐集
告知內容	(1)蒐集機關名稱 (2)蒐集目的 (3)個資類別 (4)利用地區、期間對象與方式 (5)當事人權利行使之方式 (6)得自由提供時，不提供對當事人權益之影響 (7)間接蒐集時之資料來源	
例外規定	• 法律規定得免告知 • 係機關執行法定職務或履行法定義務所必要 • 告知將妨害法定職務執行 • 告知將妨害<u>公共利益</u> • 當事人明知應告知之內容 • 蒐集<u>非基於營利之目的</u>且對當事人<u>無不利影響</u>	• 有左列情形 • 當事人自行公開或已合法公開之個資 • 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等 • 大眾傳播業者基於新聞報導之公益目的而蒐集個資



中華電信股份有限公司行動寬頻服務 個人資料蒐集告知聲明

(1) 蒐集機關名稱

感謝您成為本公司行動寬頻服務(以下稱為「本服務」)客戶，本公司重視您的隱私與個人資料保護，並尊重您的個人資料控制權。以下說明本公司如何蒐集、處理、利用您的個人資料，以及您有哪些權利可以行使。請留意，如您不是申辦本服務之人(非契約當事人)但使用本服務時(由他人申辦但供您使用)，以下內容也對您適用。申辦本服務之人有義務讓實際使用本服務之人詳閱以下內容。

1. 誰在蒐集您的個人資料：中華電信股份有限公司(以下稱為「我們」)
2. 我們為什麼蒐集您的個人資料(蒐集目的)

(2) 蒐集目的

● 履行契約義務及行使契約權利	● 履行法定義務
● 消費者、客戶管理與服務	● 資(通)訊服務/資料庫管理/安全管理
● 調查、統計與研究分析	● 電信業務/電信增值網路業務
● 廣告或商業行為管理	● 經營傳播業務
● 訂位、住宿登記與購票業務	● 影視、音樂與媒體管理
● 電子商務服務	● 會員管理
● 行銷	● 其他諮詢與顧問服務
● 其他經營合於營業登記項目或組織章程所定之業務	● 個人資料之合法交易業務



中華電信股份有限公司行動寬頻服務 個人資料蒐集告知聲明

3. 我們蒐集您的哪些個人資料，例如：

(3) 個資類別

- ◆ 帳務資訊：包含您於本申請書填寫的識別類及特徵類個人資料(須依法提供身分證明文件)、我們指配給您的號碼、通信紀錄、帳單紀錄與繳費方式、服務歷程紀錄，以及其他與您的帳號相關的個人資料。
- ◆ 網路使用資訊：包含您如何使用我們的行動寬頻服務以及我們的行動寬頻服務之功效的資訊。
- ◆ 網頁或多媒體內容瀏覽資訊/行動裝置應用程式資訊：包含您使用我們的行動寬頻服務所瀏覽之網頁資訊(例如網址、時間等)，以及您的行動裝置應用程式使用資訊(例如應用程式名稱、使用情形等)。
- ◆ 位置資訊：指您使用我們的行動寬頻服務所連結網路的地理位置資訊。
- ◆ 其他服務資訊：如您已經或將要成為我們其他服務的客戶/會員，我們可能會將您的個人資料與其他服務之資料串接整併，以便我們對您更加瞭解，並提供更優化、貼切的服務。
- ◆ 其他資訊：其他您使用我們服務時所產生的資料。



如何確認個資目的及類別

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

中華民國 101 年 10 月 1 日

個人資料保護法之特定目的及個人資料之類別（修正名稱）		電腦處理個人資料保護法之特定目的及個人資料之類別（原名稱）	
修正代號	修正特定目的項目	原代號	原特定目的項目
○○一	人身保險	○○一	人身保險業務（依保險法令規定辦理之人身保險相關業務）
○○二	人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）	○○二	人事行政管理
○○三	入出國及移民		
○○四	土地行政	○○三	土地行政
○○五	工程技術服務業之管理		



中華電信股份有限公司行動寬頻服務 個人資料蒐集告知聲明

4.我們如何利用您的個人資料

(4)利用地區、期間對象與方式

- ◆ 4.1期間及地區：我們會在您使用本服務（保有帳戶）的期間與地區內利用您的個人資料。當本契約終止或解除（您不再使用本服務）後，我們會在法令要求或許可的範圍與期限內保留及利用您的個人資料，並在該期限後，以無法識別您的身分之形式保存您使用本服務期間所產生的（非個人）資料。
- ◆ 4.2提供 / 揭露個人資料之對象：我們絕對不會將您的個人資料揭露予第三人，除非取得您的同意或依其他法令特別規定。
 - ◆ 如您同意，我們可能會將您的個人資料提供給受我們委託的關係企業或第三人（例如行銷 / 分析 / 廣告 / 公關業者、物流業者、金流業者、資訊服務業者等），在受委託的範圍內協助我們達成蒐集目的。我們會對委託的關係企業或第三人執行必要的監督，以確保您的個人資料安全。
- ◆ 4.3利用個人資料之方式：我們會以必要的方式利用您的個人資料以達成蒐集目的，例如：
 - ◆ 為您建立客戶 / 會員檔案以便我們管理帳戶。
 - ◆ 以您的各項聯繫方式與您業務聯繫，或向您通知與本服務有關之資訊。
 - ◆ 寄送帳單 / 催繳訊息至您或實際使用本服務之人的地址或電子郵件信箱；藉由電話聯繫或簡訊通知您或實際使用本服務之人有關繳費 / 催繳之資訊。
 - ◆ 以您的各項聯繫方式向您提供行銷資訊，例如優惠方案、促銷活動、市場或使用調查、其他更適合您的電信及增值服務方案等。
 - ◆ 分析您的個人資料以優化我們的各項服務，並可能依分析結果向您推薦適合您的商品 / 服務。
 - ◆ 分析您的個人資料，並以統計數據、趨勢或其他無法識別您的身分之形式產出結果，對外提供給我們的企業客戶或內容提供者，作為商業判斷的依據(例如讓內容提供者瞭解消費者之點閱狀況、消費者年齡 / 性別分布、消費者停駐其內容時間等)。



中華電信股份有限公司行動寬頻服務 個人資料蒐集告知聲明

- ◆ 4.4蒐集目的以外的利用：我們只會在蒐集目的之必要範圍內，依前述說明利用您的個人資料，除非：

加碼：目的外利用（單獨告知）

- ◆ 法律明文規定。例如受司法機關或主管機關依法要求提供個人資料。
- ◆ 為增進公共利益所必要或為防止他人權益之重大危害。例如偵測 / 預防詐欺或網路犯罪等違法行為。
- ◆ 為免除您的生命、身體、自由或財產上之危險。例如當您行蹤不明時，將您的位置資訊提供給有權得知之第三人。
- ◆ 受公務機關或學術研究機構請託，基於公共利益為統計或學術研究而有必要，以無法識別您的身分之形式，提供資料給該公務機關或學術研究機構；或以可識別您的身分之形式提供資料，但該公務機關或學術研究機構保證所產出並對外揭露之結果無法識別您的身分。
- ◆ 依法得到您的同意。
- ◆ 有利於您的權益。



中華電信股份有限公司行動寬頻服務 個人資料蒐集告知聲明

5. 您有哪些權利可以行使:

(5)當事人權利行使之方式

- ◆ 您有權請求查詢、閱覽我們保有您的個人資料，或請求我們提供複製本。但我們依法得酌收必要的成本費用。
- ◆ 您有權向我們補充或更正您的個人資料
- ◆ 當本契約終止或解除後，或您認為我們不再需要您的個人資料時，您有權請求我們刪除、停止處理或利用您的個人資料。但我們因執行業務所必須（例如法令已規定保存期限），或另外取得您的書面同意時，仍得保存或繼續處理、利用您的個人資料。
- ◆ 如您認為我們違法蒐集、處理或利用您的個人資料時，您有權請求我們刪除、停止處理或利用您的個人資料。但我們會檢視是否有違法情形，並回覆您結果。
- ◆ 如您不願再收到我們的行銷資訊，您有權通知我們拒絕接受行銷。
- ◆ 如您要行使上述各項權利，其行使方式依法令及本公司相關規定，洽本公司各服務中心或直撥免費客服電話(市話:123、0800-080-123、行動:0800-080-090)、「我的服務中心」網站(<https://my.cht.com.tw/>)諮詢辦理。本公司得依個資法第10條、11條規定，執行業務所必須及法定保存期間等考量，決定是否接受申請。



中華電信股份有限公司行動寬頻服務 個人資料蒐集告知聲明

6. 若您不提供個人資料的影響: (6)得自由提供時，不提供對當事人權益之影響

- ◆ 申請書中所列的個人資料均為必填欄位，如未正確、完整填寫，可能無法申辦本服務，或將無法即時收到與本服務相關的必要資訊。
- ◆ 其他個人資料是您在**使用本服務的過程中(自動)產生並紀錄**，若您不願意我們處理或利用，請依上述權利行使方式辦理。

您是否同意（未勾選者視為不同意，若不同意並不影響使用我們的服務）**目的外利用（單獨取得同意）**

- 我們向您寄送第三人(關係企業或企業客戶)的商品/服務資訊。☐同意 ☐不同意。
- 建議您勾選「同意」，才不會錯過好康的機會、折扣資訊、優惠方案及更多的服務。

簽章:_____ 代理(辦)人簽章:_____ 日期:____年____月____日

2022-10-20 版



自評表

5	公司蒐集個資，是否訂定管理程序以確保依照個資法第八條、第九條規定履行告知義務？(相關規定個資法第8、9條、辦法第5條第2款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.告知義務範圍(個人資料類別；蒐集目的(包含告知特定目的外)；利用之期間、地區、對象及方式；特定目的(內、外)利用範圍) 2.前揭是否納入契爭內容(\$19/1/2)?或另取得當事人同意(書)? (法務部106年10月11日法律字第10603509640號函釋參照) 3.特定目的內之運作的情形(請一併注意已有前述1之告知範圍)；蒐集方於蒐集、處理時，於後續特定目的外之利用情形(請一併注意個資法第7條規定)
---	--	--	--

發文字號：	法律字第 10603509640 號
發文日期：	民國 106 年 10 月 11 日
要 旨：	個人資料保護法第 19 條第 1 項規定所稱「同意」，係指當事人經蒐集者告知該法所定應告知事項後，所為允許意思表示，而基於契約關係蒐集個人資料， <u>原則上僅能於契約事務特定目的必要範圍內為之</u> ；又非公務機關使用基於契約或類似契約關係下取得之個人資料，對其進行行銷應合乎社會通念下當事人對隱私權合理期待；同法第 7 條第 3 項規定所稱「 <u>明確告知</u> 」方式， <u>任何足以使當事人知悉或可得知悉方式均屬之</u> ，惟為達到「明確告知」目的，蒐集者仍應以個別通知方式使當事人知悉，不得以單純擺設公告或上網公告概括方式為之，須足以使當事人知悉或可得知悉該公告內容方式始屬之；同法第 8 條第 1 項立法意旨在使當事人能充分瞭解個人資料被他人蒐集情形，告知有關「個人資料利用之對象」時，以告知時已知資訊進行適度描述已足，尚無須詳列未知資訊



當事人之「同意」

■ 個人資料保護法§7

- ◆ 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，**單獨所為之意思表示**。
- ◆ 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。



案例思考-當事人之「同意」

- 甲公司於協助小明宅配所購電腦之際，告知甲公司蒐集小明個資之目的（包括宅配、行銷等）、範圍、當事人權利行使方式及其他應告知內容。
 - ✓ 小明表示OK
 - ✓ 小明不置可否
 - ✓ 小明「喔」了一聲
 - ✓ 小明詢問接到行銷電話的頻率，聽到甲公司的回答後，說了一句「還好不會太常打」
 - ✓ 小明自行拿走甲公司放在櫃臺上，包裝上清楚印有「電話行銷客戶贈品」之刮鬍刀一支



推定同意？

問題：預設同意是否屬於推定當事人同意？

國家發展委員會民國 107 年 11 月 21 日發法字第1072002136號函

按個資法第7條第3項規定「公務機關或非公務機關明確告知當事人第8條第1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15條第2款、第19條第1項第5款之規定表示同意」。
。因此業者如欲透過「推定同意」之方式取得個人資料，除應盡告知義務且明確告知外，尚須符合「當事人未表示拒絕」及「當事人已提供其個人資料」兩項要件，始得為之。

本件若欲符合推定同意要件之「當事人已提供其個人資料」，應係指當事人有自行提供個人資料之積極行為(例如：自主開啟藍芽設定並選擇同步資料，並將資料傳送予業者)；倘業者預設自動上傳資料之功能，在當事人未有任何積極行為之情形下即取得個人資料，則縱使當事人未表示拒絕，仍不得視為當事人已提供其個人資料，因此應不符合推定同意之要件。



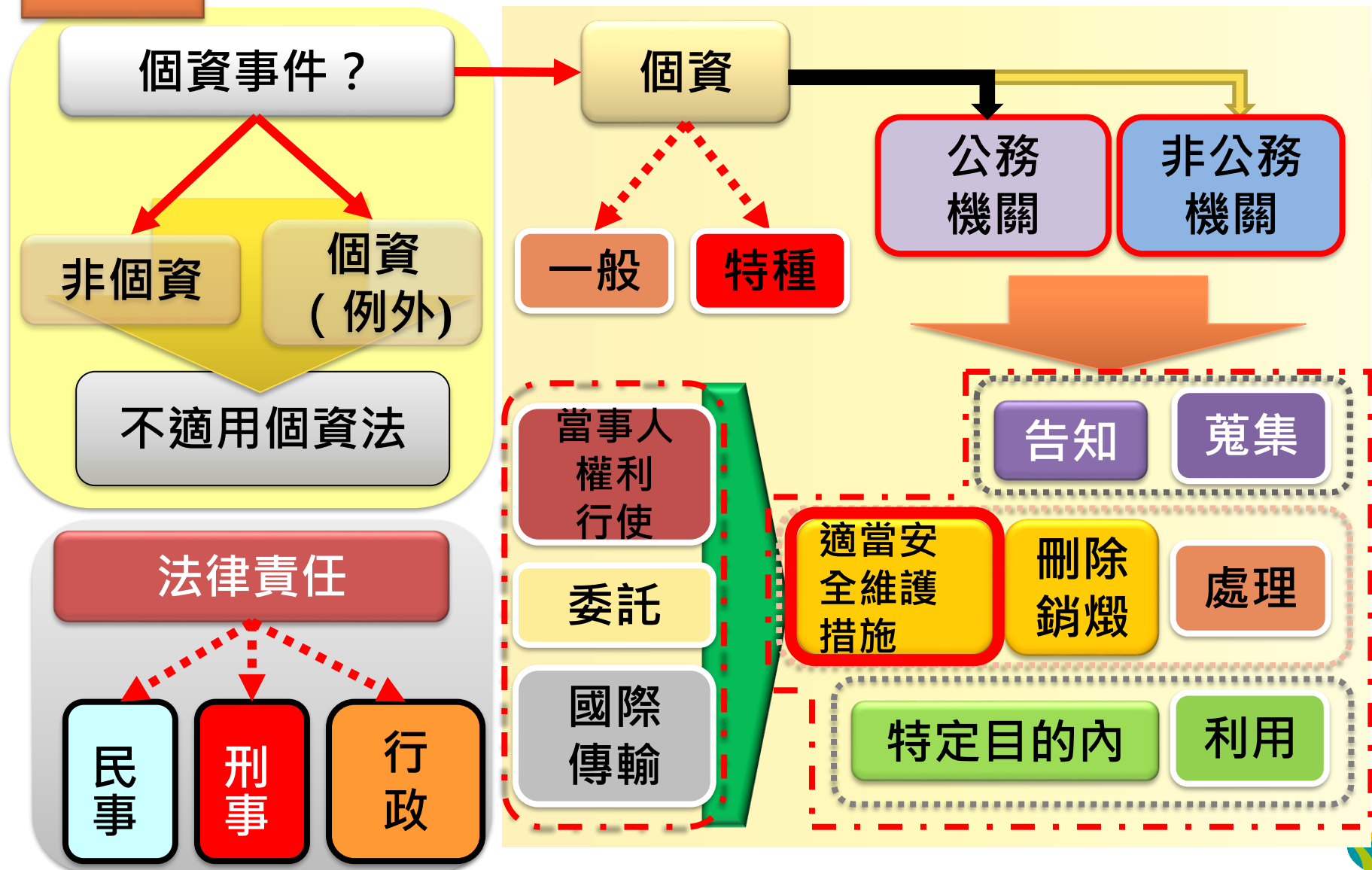
自評表

6	公司蒐集、處理個資，是否訂定管理程序以符合個資法第十九條規定，具有特定目的及法定情形；而其經當事人同意者是否確保符合個資法第七條第一項規定？(相關規定：個資法第19、7條、辦法第5條第3款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) (與編號5關聯) 1. 蒐集及處理時，針對跨業務、跨業者、跨系統(包含前編號5告知作為之利用項目範圍)是如何經取得消費者的同意(請一併注意個資法施行細則第8條規定，編號9)。 2. 是否規範於B2B或B2C之契約(\$19/1/2)或另取得當事人同意？
---	---	--	--



個資法規範架構暨個資全生命週期

START





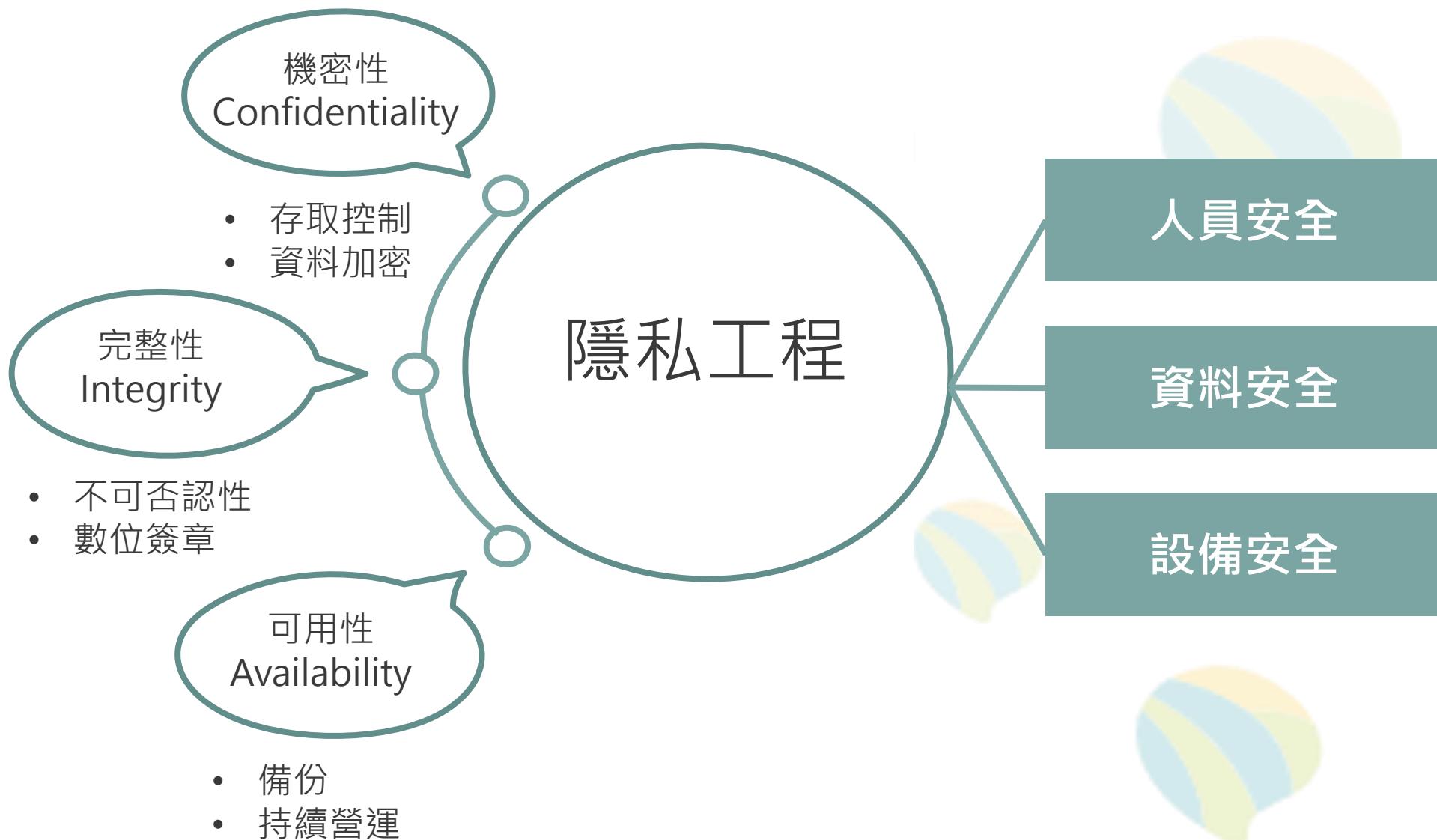
適當安全措施？

- 個人資料保護法施行細則第12條2項

- 所謂適當安全措施，**得**包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：
 - 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。



安全管理目標





相關實務案例（一）

臺灣臺北地方法院107年度北小字第266號民事判決

當事人

1. 當事人於105年5月25日報名公司同年6月26日舉辦的多益測驗。
2. 當事人於同年7月4日遭詐騙集團來電詐騙約15萬元。
3. 詐騙集團清楚說明所有報考資料，導致當事人不疑有他。

公司

- 公司於事件前即採取：
1. 防火牆。
 2. 電子加密系統。
 3. 封包加密處理。
 4. 防毒軟體。
 5. 制訂有電腦使用管理辦法。
 6. 舉辦資安教育訓練。

法院

1. 判賠新台幣2萬元。
2. 考量公司營運規模、蒐集處理利用大量個人資料。公司所稱之防護措施僅為基本配備。
3. 公司並未說明電腦使用紀錄、軌跡資料係如何保存、有無對資訊系統及電腦設備進行定期安全稽核、或對經手客戶資訊之員工建置完善之稽查制度。



相關實務案例（二）

臺灣士林地方法院107年度湖簡字第644號民事簡易判決

當事人

1. 當事人於106年4月6日，透過公司官網線上消費列印DM，而提供個人資料予公司告知，及線上信用卡支付費用。
2. 106年8月3日，當事人先後接到詐騙集團假冒公司員工與花旗銀行員工來電，導致當事人遭詐騙14萬多。

公司

1. 公司採用微軟Azure雲端系統，該系統有提供資安防護。
2. 配合微軟公司政策，相關個資網頁均有SSL加密。
3. 防駭系統於期間內成功阻擋來自同一IP的34,800次異常入侵。
4. 106年3月29日即於網站首頁顯示防詐騙宣導，寄送防詐騙DM。
5. 透過資安公司進行資安補強、加強網站防駭邏輯。

法院

1. 駁回當事人請求。
2. 無法證明詐騙集團使用的個人資料來自於公司。
3. 公司於接到會員通知接到詐騙電話後即報警備案，並已採取左列措施，可認已採取相當措施。



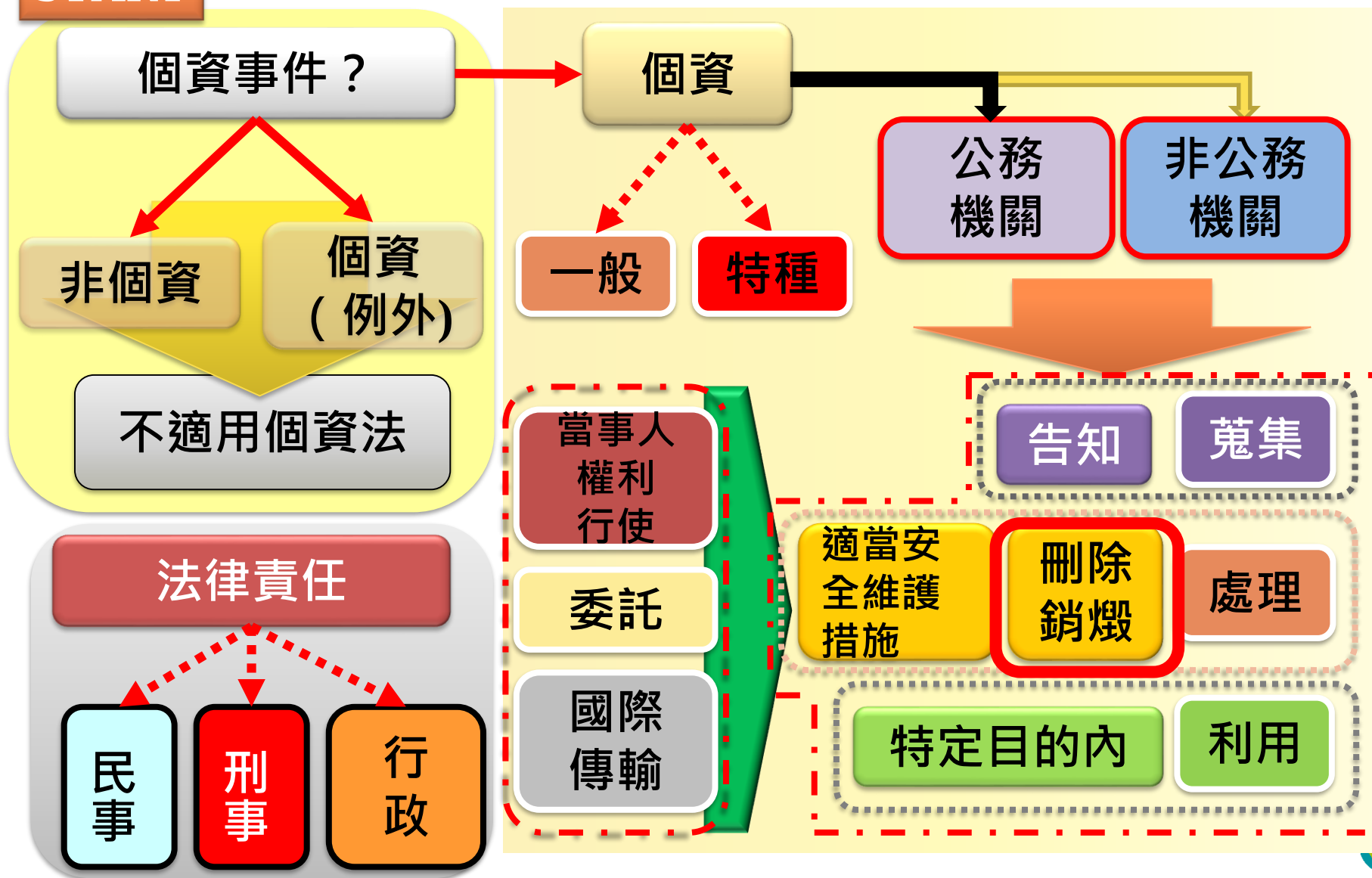
自評表

18	公司是否依其業務規模及特性或本會相關業管法規(如業務管理規則之資安專章)建置適當的資安管控措施，以確保資訊安全的要求？ (個資法施行細則第12條第2項第6、8款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.各業務的落實程度 2.資安管理
----	--	--	---



個資法規範架構暨個資全生命週期

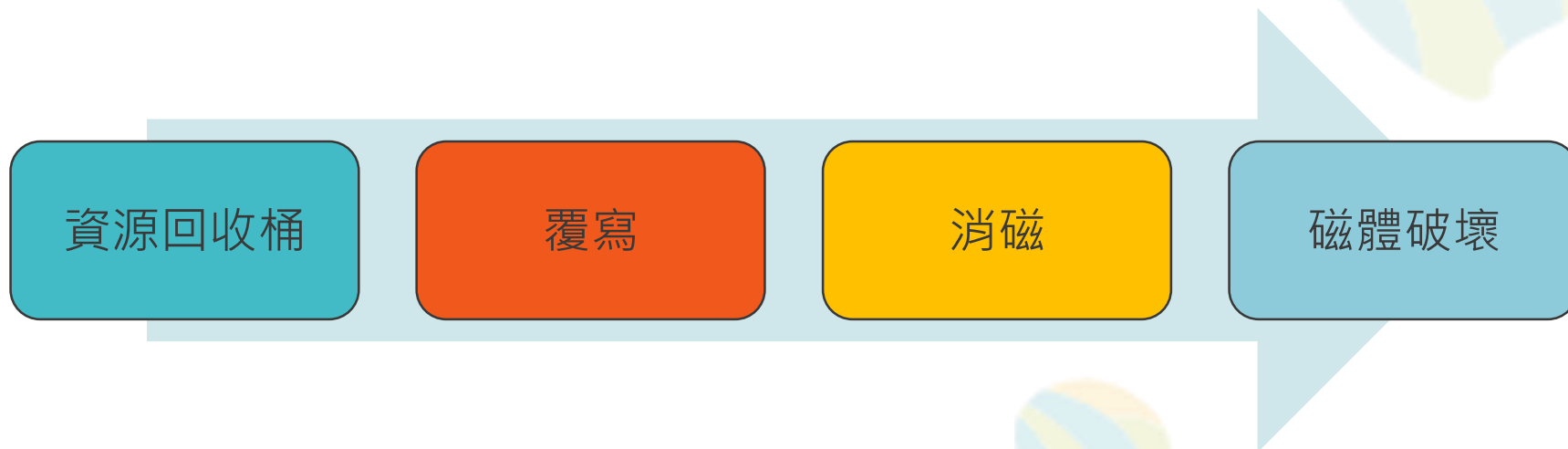
START





刪除、銷燬

刪除，指使已儲存之個人資料自個人資料檔案中消失



刪除行為之認定，應以一般人得以利用一般商業軟硬體所為使個人資料消失之行為，作為參考標準，無需以「不復存在」，始謂符合本法所稱之刪除



指定非公務機關個人資料檔案安全維護辦法

- 刪除銷毀（本辦法§ 6）

- 非公務機關應就下列事項，訂定相關紀錄、證據保存機制：

- 因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之個人資料使用情況、軌跡資料及相關證據。
- 依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄：
 - 刪除、停止處理或利用之方法、時間。
 - 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。



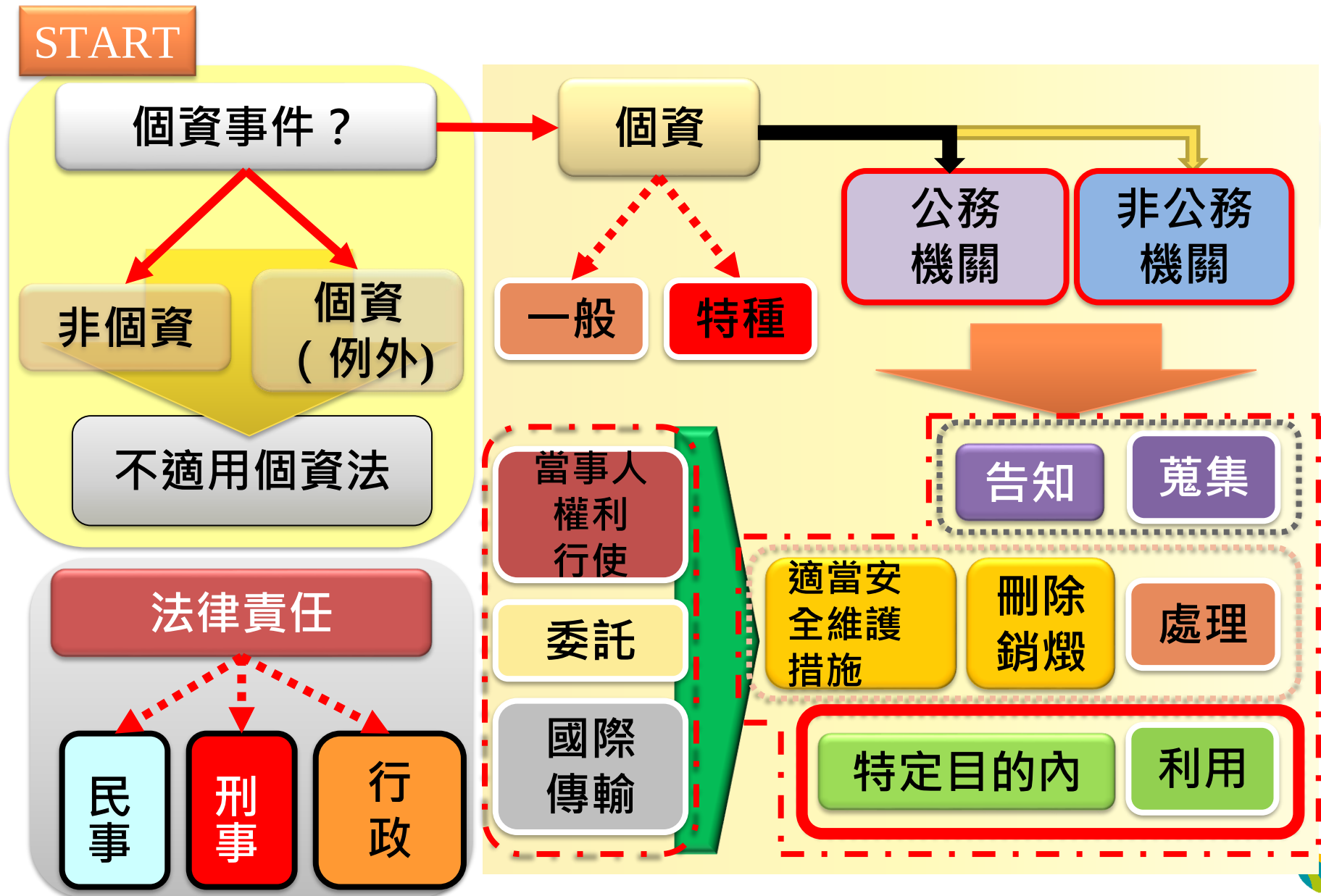
伺服器報銷未清除客戶資料 摩根史坦利以6千萬美元和解

摩根士丹利（Morgan Stanley）因資料處理不當，公司舊硬碟沒有清乾淨就轉手，導致千萬名客戶個資曝露外洩風險，2022年1月以6,000萬美金與消費者和解，另於同年9月同意支付3,500萬美元罰款。

這樁案件自2016年多達1,500萬名客戶對該銀行提起的集體控訴。2016年，摩根史坦利關閉美國境內二座財富管理業務部門的資料中心時，未能將伺服器上未加密的客戶資料刪除乾淨、就賣給了第三方業者。2019年這家銀行又出了一次類似的包，把內有客戶資料的網路系統賣給了外部業者。



個資法規範架構暨個資全生命週期





利用之法定要件

個資法§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：
 - 法律明文規定。
 - 為增進公共利益所必要。
 - 為免除當事人之生命、身體、自由或財產上之危險。
 - 為防止他人權益之重大危害。
 - 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。
 - 經當事人同意。
 - 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。



當事人之「同意」

■ 個人資料保護法§7

- ◆ 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，**單獨所為之意思表示**。
- ◆ 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。



線上告知事項

※須將卷軸拉至底部完成閱讀，方可點選瞭解才進下一步(以下所有告知事項)

1.線上投保注意事項

一、要保人與被保險人聲明事項：(本聲明事項僅針對投保傷害險部分適用)

1. 本人(被保險人)同意富邦產物保險公司得蒐集、處理及利用本人相關之健康檢查、醫療及病歷個人資料。
2. 本人(被保險人、要保人)同意富邦產物保險公司將本要保書上所载本人資料轉送產、壽險公會建立電腦系統連線，並同意產、壽險公會之會員公司查詢本人在該系統之資料以作為核保及

2.直接蒐集個人資料告知事項

一、蒐集之目的：

- (一) 093財產保險(依保險法令規定辦理之財產保險相關業務)。
- (二) 001人身保險(依保險法令規定財產保險經許可辦理之相關業務)。
- (三) 040 行銷(包含金控共同行銷業務)。
- (四) 181其他經營合於營業登記項目或組織章程所定業務之需要。

☒ 我已閱讀並瞭解上述相關告知事項



本人同意所蒐集之聯絡資料作為富邦產險日後進行共同行銷之特定目的使用。如未勾選不會影響本次投保權益，可直接進行下一步，視為不同意上述說明。



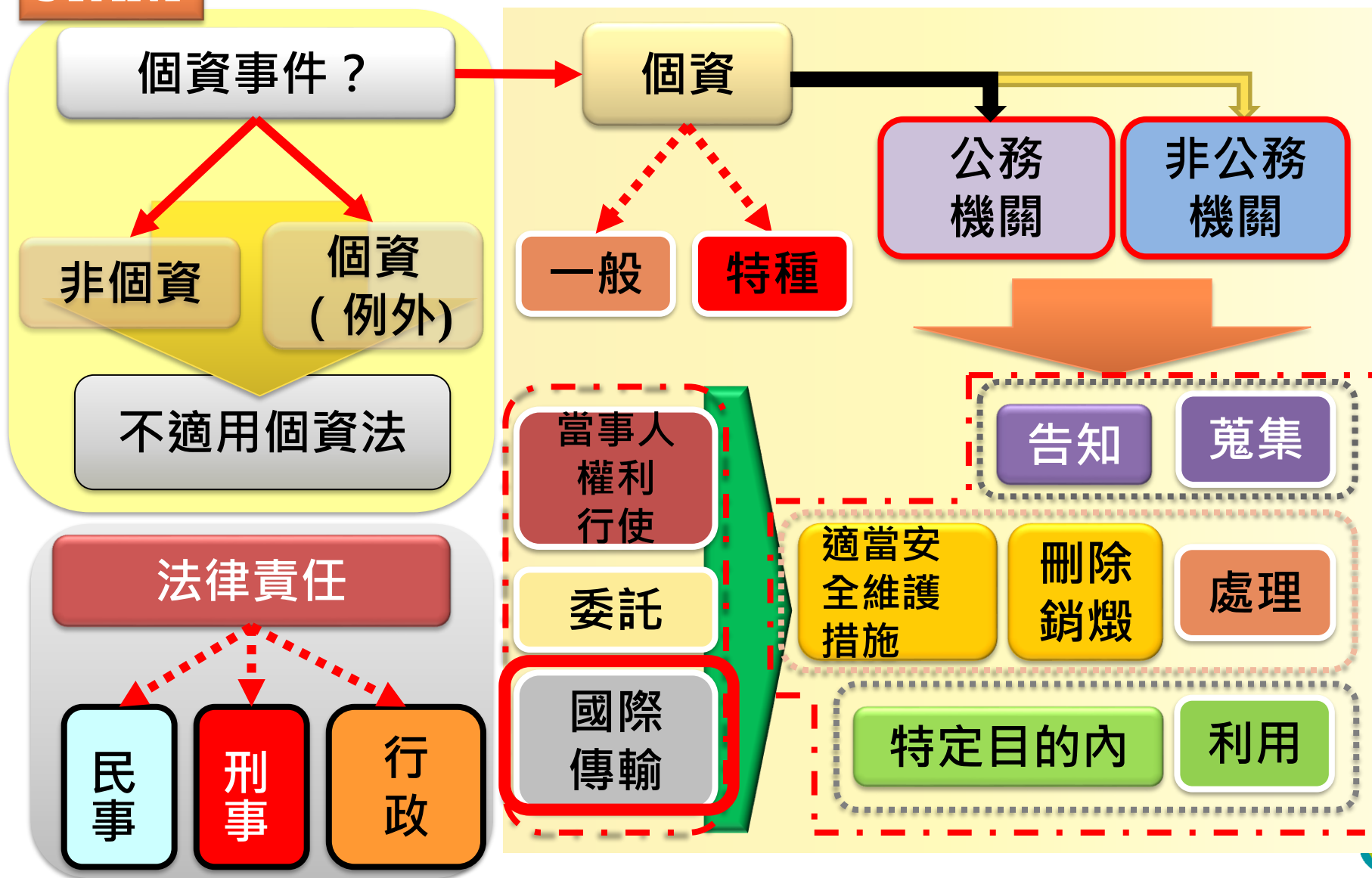
自評表

7	公司是否訂定管理程序以符合個資法第十九條規定，於特定目的必要範圍內利用個資；其為特定目的外之利用者，是否符合法定情形；而目的外利用係經當事人同意者，是否符合個資法第七條第二項規定？(相關規定：個資法第19、7條、辦法第5條第4款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) (與編號5關聯) 1.利用時， 針對跨業務、跨業者、跨系統 (包含前編號5告知作為之利用項目範圍)是如何經取得消費者的同意(請一併注意個資法施行細則第8條規定，編號9)。 2.是否規範於B2B或B2C之契約(§19/1/2)或另取得當事人同意？
8	公司對當事人進行行銷，經其 表示拒絕時 ，是否訂定管理程序以確保立即停止利用其個資行銷？另於 首次行銷時 ，是否提供當事人 免費表示拒絕 接受行銷之方式？(相關規定：個資法第19條第2、3項、辦法第5條第5款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.SOP 2.內部稽核有否發現，並有否即時改善情形？
20	公司同時 經營電商平台或與電商平台合作 ，用戶個資如有相互交流，是否符合個資法第八條、第二十條規定？	是 ☐ 否 ☐	配合「新世代打擊詐欺策略行動綱領」作業



個資法規範架構暨個資全生命週期

START





國際傳輸相關條文

- 個資法第21條。

- 原則：不另設限制（但仍須符合蒐集、處理、利用相關規定）。

- 例外：

非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

- 一、涉及國家重大利益。

- 二、國際條約或協定有特別規定。

- 三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

- 四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。



國際傳輸之原則與例外



原則：許可



例外：中央目的事業主管機關得限制

限制要件：國家重大利益/ 國際條約協定規定/ 接受國個資法規不完善/ 迂迴方式傳遞

通訊傳播業

金融業

醫院

社會工作師

蘋果日報

人力仲介業

西藥批發零售業



國際傳輸的潛藏樣態與風險

僅規範非公務機關



國際傳輸 - 對通訊傳播事業之限制

- 國家通訊傳播委員會101年9月25日通傳通訊字第10141050780號令

「限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區」衡酌大陸地區之個人資料保護法令尚未完備，通訊傳播事業於國際傳遞及利用個人資料時，應考量接受國家或地區對個人資料有完善之保護法令，爰依「電腦處理個人資料保護法」第24條第3款規定，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。



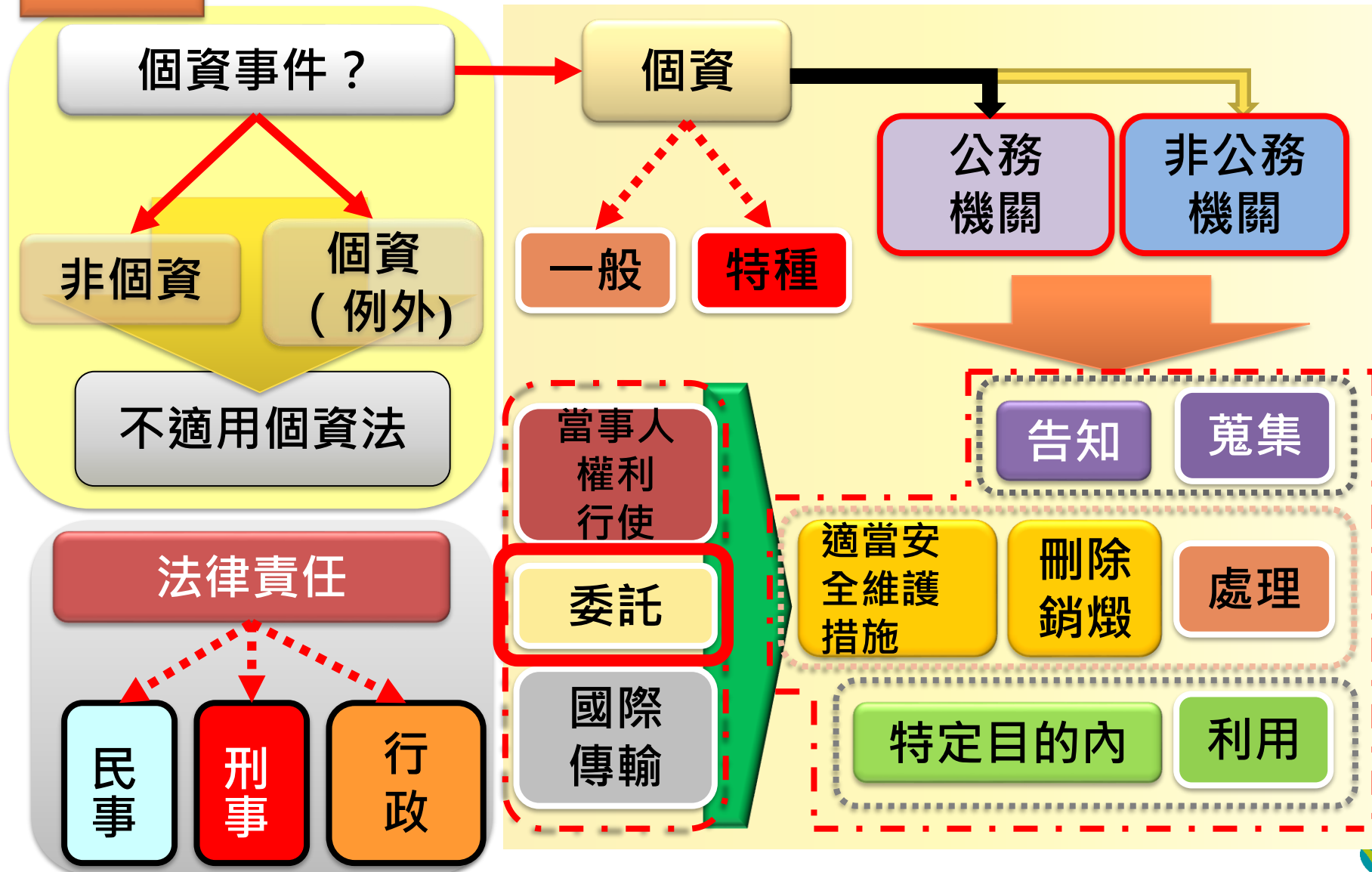
自評表

10	公司將個資進行國際傳輸者是否訂定管理程序以確保符合本會相關法令之要求？(相關規定：個資法第21條、辦法第5條第7款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.有否國外VPN的點，如何管理(SOP)? 2.國外委託設置VPN時如何管理(SOP)?
----	--	--	---



個資法規範架構暨個資全生命週期

START





委託機關定義及監督責任彙整

定義（個資法§4）

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**。

監督責任（細則§8）

委託機關應定期確認受託者執行狀況，並將確認結果記錄

預定蒐集、處理或利用個資之**範圍、類別、特定目的及期間**

受託者的**適當安全維護措施**

有**複委託**者，其約定之受託者

受託者違法時應**通知**或採行之**補救措施**

委託者**保留指示**之事項

關係終止或解除時，個資之**返還**或**刪除**

定期**確認**執行狀況與**記錄**結果

有無委外

監督方式

持續管理



複委託的風險

日本市府外包商喝爛醉睡路邊 存有46萬人個資
USB遭「神秘撿屍」！

據日本《產經新聞》與《神戶新聞》報導，尼崎市政府委外處理因新冠疫情生活受影響，必須申請補助金的家庭與低收入戶等資料處理，據悉該承包商是大阪的一間公司。



Biprogy列出四大問題癥結：

1. 資料移轉的審核程序未能落實，由於Biprogy並未說明資料轉移的具體方法與電子媒介，因此尼崎市政府不知道會使用USB隨身碟來轉移資料
2. 應使用有保障的物流運輸公司，而不是由個人攜帶；
3. 完成工作後，USB隨身碟中的資料應該立即刪除，負責執行的員工缺乏這方面的指示與確認；
4. 工作結束後USB隨身碟就應該保存到指定的地方，但這方面並沒有相關指示與確認。



受託者之選擇-自評表

管理重點

判斷個資有無
委外處理等

選擇委外監督方式
，簽約或實地查核

後續處置及內
部管理機制

委外廠商查核之表單設計（例示）

查核項目	查核內容	查核結果	說明
1.人員及資源配置		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	
2.界定個人資料 (若著眼於安全維護，細則12條要求的11款事項就將成為查核重點)		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	
		☐ 符合 ☐ 不符合 ☐ 不適用	



自評表

9	公司是否訂定管理程序以確保依施行細則第八條規定，對委託含有個資業務之廠商為適當監督，並於委託契約或相關文件中，明確約定其內容？(相關規定：施行細則第8條、辦法第5條第6款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.如何與簽約第三方確實實施查核作業？是否符合個資法施行細則第8條規定？ 2.異業合作SOP是否已符合第15、16、19、20條相關規定(是否符合已檢視相關程序，如蒐集+特定目的外利用為甲方，其負特定目的外利用之同意或有法規明定；蒐集+特定目的內之利用為乙方之各所負擔之法定義務)。
---	--	--	--



```

graph TD
    A[個人資料事件?] --> B[個人資料]
    A --> C[非個人資料]
    B --> D[一般]
    B --> E[特種]
    B --> F[公務機關]
    B --> G[非公務機關]
    F --> H[告知]
    F --> I[蒐集]
    G --> J[適當安全維護措施]
    G --> K[刪除銷燬]
    G --> L[處理]
    E --> M[當事人權利行使]
    E --> N[委託]
    E --> O[國際傳輸]
    M --> P[民事]
    M --> Q[刑事]
    M --> R[行政]
    J --> S[特定目的內]
    J --> T[利用]
  
```

個人資料事件？

個人資料

非個人資料

一般

特種

公務機關

非公務機關

告知

蒐集

適當安全維護措施

刪除銷燬

處理

當事人權利行使

委託

國際傳輸

民事

刑事

行政

特定目的內

利用

法律責任

不適用個人資料法



當事人權利行使整理

不得預先拋棄

不得特約排除

告知行使方式

權利類型

處理方式

時限

查詢或請求閱覽

請求製給複製本

可收取必要成本費用

可拒絕的情形：

- 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。

15+15

請求補充或更正

請求停止蒐集、
處理或利用

請求刪除

無爭議

有爭議

正確性問題 *

特定目的消失/期限屆滿 *

違法蒐集處理利用

30+30

* 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



電話錄音是否可要求複製本？

金管會104年03月26日金管法字第0400543491號函

按個資法第3條及第10條等規定，請求查詢、閱覽及製給複製本為個資當事人之法定權利，除有礙重大公共利益等例外情形外，原則上不得要求當事人預先拋棄或以特約限制之。

金融業者依法令規定或取得當事人書面同意所蒐集、留存之錄音錄影資料，客戶既為該等資料之當事人，自得請求業者製作及提供複製本；除有個資法第10條但書所定情形外，不得拒絕之。

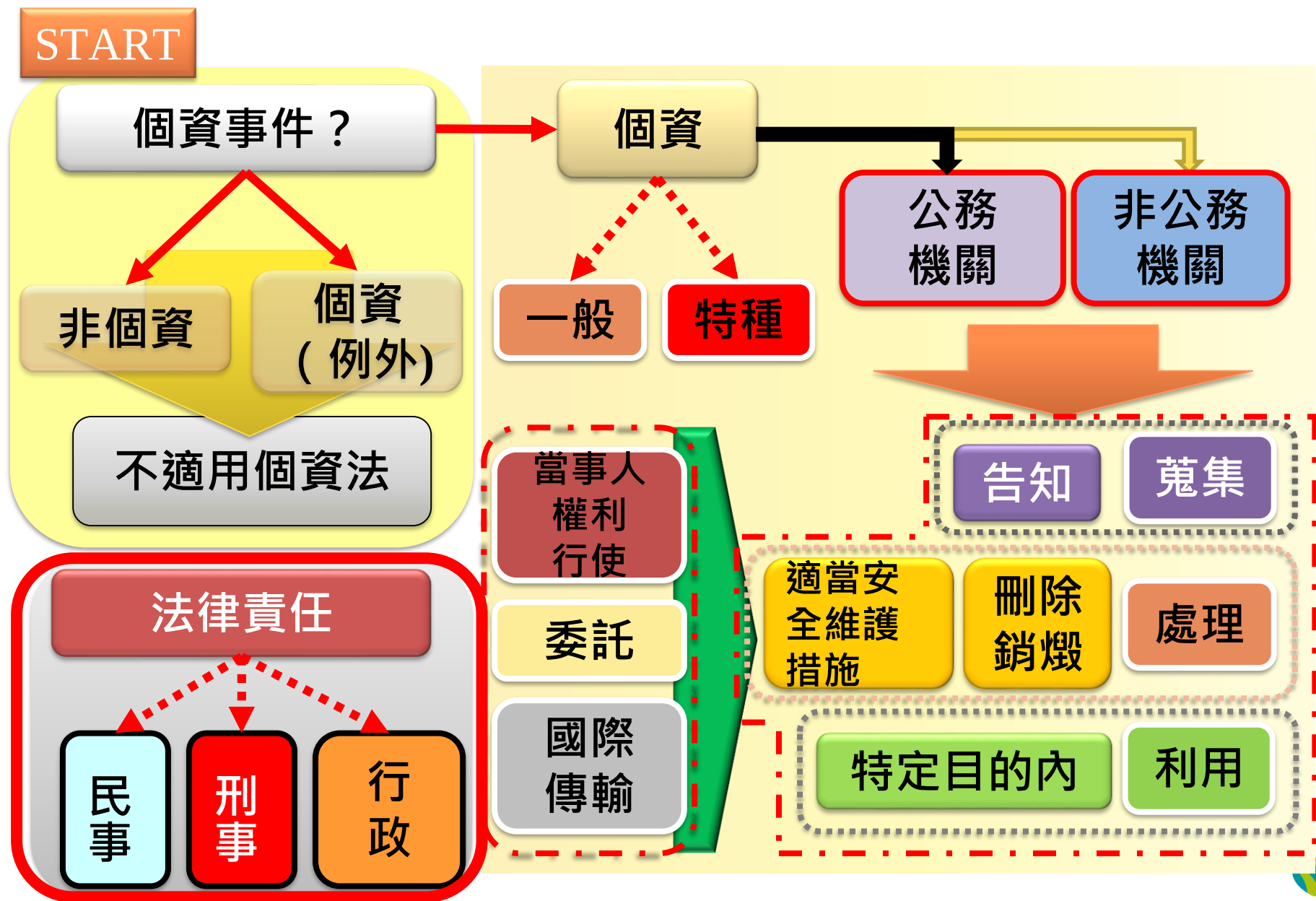


自評表

11	公司是否訂定管理程序以確保提供當事人 行使個資法第三條所定之權利及管道 ？(相關規定：個資法第3條、辦法第5條第8款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.受理變更、停止、刪除等作為，其程序及實務作業。 2.個資蒐集同意書內容不得有「預先拋棄或以特約限制文字」。
12	公司是否訂定管理程序以確保個資之 正確性 ？當其有不正確或正確性有爭議者，是否依個資法第十一條第一項第二項及第五項規定辦理？(相關規定：個資法第11條、辦法第5條第9款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.受理更正SOP。
13	公司是否訂定管理程序以確保就所保有個資之特定目的消失或期限屆滿時依個資法第十一條第三項規定， 刪除停止處理或利用該個資 ？(相關規定：個資法第11條、辦法第5條第10款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.SOP
14	公司是否 設置聯絡窗口供當事人申訴與諮詢 ？(相關規定：施行細則第12條第2項第5款、辦法第5條第11款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.擔任諮詢人員是否具個資法規專長(如個管師法務人員)?



個資法規範架構暨個資全生命週期





違法的後果：總覽

民事責任：§28~§40

刑事責任：§41~§46

行政責任：§25、§47~§50



違法責任種類及其內涵

刑事 –

有期徒刑、罰金

處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。



§41

違法行為態樣

意圖為自己或第三人不法之利益或損害他人之利益，而違反以下規定：

第6條第1項

(違法蒐集、處理、利用特種資料)

第19條

(無特定目的或特定情況而蒐集、處理資料)

第20條第1項

(利用資料逾越特定目的)

第21條

(違反限制國際傳輸之命令或處分)

民事 –

侵權行為損害賠償

每一事件酌定：

新台幣500 - 20,000元

總額：**新台幣2億元**

行政 –

罰鍰等

處新臺幣2-1,500萬元罰鍰
令限期改正，屆期未改正者，按次處罰之。





違法的後果：行政責任（1/2）

條次	違反行為種類	處罰結果
§47	第六條第一項（違法蒐集、處理、利用特種資料） 第十九條（無特定目的或特定情況而蒐集、處理資料） 第二十條第一項（利用資料逾越特定目的） 第二十一條（違反限制國際傳輸之命令或處分）	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
§48	違反第八條或第九條規定。（違反告知義務） 違反第十條、第十一條、 第十二條 或第十三條規定。（妨礙當事人行使權利） 違反第二十條第二項或第三項規定。（違反拒絕行銷之規定）	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
	違反第二十七條第一項（適當安全措施）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。	處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰
	非公務機關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， 其情節重大者	處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰



違法的後果：行政責任（2/2）

條次	違反行為種類	處罰結果
§49	無正當理由違反第二十二條第四項規定者（妨礙行政檢查）	處新臺幣二萬元以上二十萬元以下罰鍰
§50	<u>非公務機關之代表人、管理人或其他有代表權人</u> ，因該非公務機關依前三條規定受罰鍰處罰時， <u>除能證明已盡防止義務者外</u> ，應並受同一額度罰鍰之處罰	<u>受同一額度罰鍰之處罰</u> -> 兩罰主義
§25	上述各項違法行為	禁止蒐集、處理或利用個人資料命令刪除經處理之個人資料檔案沒入或命銷燬違法蒐集之個人資料。 公布非公務機關之違法情形，及其姓名或名稱與負責人。



行政檢查

個資法第22條

中央目的事業主管機關為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

行政檢查會議

- ✓ 緊急案件
 - 蓄意洩漏的業者
 - 湮滅證據
- ✓ 重大矚目案件*
- ✓ 行政裁量案件
 - 顯無改善
 - 6個月內反覆發生外洩

業者進行個資外洩後續改善

觀察2個月

無個資外洩案件

結案

- 後續資安改善作為
- 個資法遵面處理

仍有新個資外洩案件發生

限期改善

應付性或後續作為明顯無效

行政裁罰

- 仍無改善作為
- 有新個資外洩案件發生

*重大矚目案件：

依「行政院及所屬各機關落實個人資料保護聯繫作業要點」第2點第2項規定，範圍如下：

1. 行政院、立法院或監察院關注之個資外洩案件。
2. 經媒體顯著披露之個資外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。



行政檢查-受稽查方之協力義務

- 消費者向主管機關檢舉某電腦公司違法個資法蒐集其個資，主管機關是否能強制電腦公司提供相關資料並說明之？
- 法律字第10703511710號函釋
 - 政府機關如為調查公司涉及違反個人資料保護法案件，得依行政程序法第40條規定要求公司提供必要之文書、資料或物品，若其拒絕提供，而機關認有必要或有違反個資法規定之虞，個資法第22條第1項及第2項規定進入檢查並為相關保存證據之處分，如該公司無正當理由規避、妨礙或拒絕者，得裁處新臺幣2萬元以上20萬元以下罰鍰（個資法第22條第4項及第49條參照）



行政責任裁罰案例

● 行政裁罰案例：A網路書局（3/3）

1. 行為一：違反個資法第48條第2款

- ○○○公司是否已踐行個資法第12條通知義務

2. 行為二：違反個資法第48條第4款前段（107年5月29日迄今）

- 個人資料保護與管理政策暨程序書與相關制度是否完備
- 就白名單管理與防毒軟體布署是否落實
- 是否建立個資外洩之危機處理措施程序
- 是否提出落實適當安全措施之紀錄與證據
- 是否安排資安合約採購作業與提供執行弱點掃描、滲透測試與白箱原碼檢測輸出等成果文件，以佐證已改善或排除弱點

3. 個資法第50條

- 代表人是否已善盡防止義務



行政責任裁罰案例

●行政裁罰案例：A網路書局

解除分期付款案件統計(107-108)

107.5.2
不通過
限期改善

- ☒ 未落實個資保護管理程序。
- ☒ 未落實白名單管理及進行log分析。
- ☒ 未落實個資外洩危機處理措施程序。
- ☒ 建立員工電腦與公司系統連線管控
- ☒ 提升使用者密碼強度及變更密碼機制
- ☒ 風險評鑑資訊清查
- ☒ 辦理員工資安教育訓練

107.9.12
不通過
限期改善

- ☒ 未落實個資保護管理程序。
- ☒ 未落實白名單管理及進行log分析。
- ☒ 未落實個資外洩危機處理措施程序。
- ☒ 建立員工電腦與公司系統連線管控
- ☒ 提升使用者密碼強度及變更密碼機制
- ☒ 風險評鑑資訊清查
- ☒ 提供員工教育訓練

108.3.13
不通過
限期改善

- ☒ 未落實個資保護管理程序。
- ☒ 未落實白名單管理及進行log分析。
- ☒ 未落實個資外洩危機處理措施程序。
- ☒ 建立員工電腦與公司系統連線管控
- ☒ 提升使用者密碼強度及變更密碼機制
- ☒ 風險評鑑資訊清查

108.7.23
不通過
限期改善

- ☒ 未落實個資保護管理程序。
- ☒ 未落實白名單管理及進行log分析。
- ☒ 未落實個資外洩危機處理措施程序。



NCC裁罰案例

業者	日期	事由	法令依據	結果
○○電信股份有限公司	108.9.25	於蒐集、處理及利用個人資料未經當事人同意，與加盟門市人員於個人手機及雲端帳戶儲存客戶個人資料	§§19 I、27 I、47 ②及第 48 II	處罰鍰新臺幣 5 萬元，並應限期改正
○○○○○電信股份有限公司	107.8.15	○○○○○電信股份有限公司未依規定於本案當事人離職後停止其個人資料之處理或利用	§§11 III、48 II	限期於1個月內改正並提報改善計畫到會，屆期未改正者，按次處予罰鍰
○○○○○股份有限公司	106.10.11	○○○○○○股份有限公司發行某軟體，利用號碼可攜集中式資料庫(NP資料庫)資料，涉揭露民眾使用電話號碼所屬電信業者別，或變更檢視結果為「網內/網外」，均不足以直接或間接識別該等電話號碼之個人身分。	§§1、20 I	不予裁罰



自評表

17	公司清楚瞭解違反個資法將有可能遭到民事損害賠償的請求，及刑事或行政處分的處罰(個資法第28、41、42及47~第50條)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.員工教育訓練
----	--	--	-------------------------------------



02

個資保護 實務教戰指引



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

個人資料盤點



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



個資盤點表（填表說明）（1/3）

TPIPAS教學用

盤點部門			人力處		盤點者		Kitty			盤點負責人				Chin						
檔案編號	作業流程名稱	個資行為態樣 1.蒐集 2.處理 3.利用 4.國際傳輸	個人資料			直接蒐集			間接蒐集			告知義務		委託或受託		保管儲存與刪除銷燬				數量
			檔案名稱	種類及類別	類型	方式	特定目的	法定情形	來源	特定目的	法定情形	告知與否	免告知之法定事由	有無	委託者或受託者	資料載體	儲放場所	保存期限	刪除銷燬	

- **作業流程名稱**：單位的部門職責內容、業務項目、日常作業流程等
- **個資行為態樣**：依照個資法對於個態樣的定義分別對應（可複選）
- **檔案名稱**：可供識別之個人資料檔案名稱
- **種類及類別**：依法務部公告「個人資料保護法之特定目的及個人資料之類別」（姓名、性別等）
- **檔案類型**：紙本 / 電子不同型態個資檔案應個別列出
 - 紙本：實體
 - 電子：電子檔、錄音（影）檔、圖片檔（含掃描檔）等
 - 資料庫：僅保存於資訊系統內，未另外列印成紙本或另存成電子檔案



個資盤點表（填表說明）（2/3）

TPIPAS教學用

盤點部門			人力處			盤點者			Kitty			盤點負責人				Chin				
檔案 編號	作業 流程 名稱	個資行為態樣 1.蒐集 2.處理 3.利用 4.國際 傳輸	個人資料			直接蒐集			間接蒐集			告知義務		委託或受託		保管儲存與 刪除銷燬				數量
			檔案 名稱	種類 及類別	類型	方式	特定 目的	法定 情形	來源	特定 目的	法定 情形	告知 與否	免告知 之法定 事由	有無	委託者 或 受託者	資料 載體	儲放 場所	保存 期限	刪除 銷燬	

- **蒐集方式或來源**：該個人資料檔案取得管道或建立之方法
- **特定目的**：依法務部公告「個人資料保護法之特定目的及個人資料之類別」（人事管理）
- **法定情形**：是否有法定保有依據或契約或機關自定之保有依據
- **告知與否**：判斷是否需依個資法第8條及第9條規定
 - 蒐集、處理或利用個人資料時應明確履行告知義務
 - 需告知，填Y；得免為告知，填N
- **免告知之法定事由**：判斷是否符合個資法第8條及第9條規定個別列出之
- **委託者或受託者**：委託之服務與個資檔案之蒐集、處理及利用流程有關，或為受委託方接觸到委託方客戶個資內容之委外機（構）或人員



個資盤點表（填表說明）（3/3）

TPIPAS教學用

盤點部門			人力處			盤點者			Kitty			盤點負責人				Chin				
檔案 編號	作業 流程 名稱	個資行為態樣 1.蒐集 2.處理 3.利用 4.國際 傳輸	個人資料			直接蒐集			間接蒐集			告知義務		委託或受託		保管儲存與 刪除銷燬				數量
			檔案 名稱	種類 及類別	類型	方式	特定 目的	法定 情形	來源	特定 目的	法定 情形	告知 與否	免告知 之法定 事由	有無	委託者 或 受託者	資料 載體	儲放 場所	保存 期限	刪除 銷燬	

- **資料載體**：紙本 / 電子不同型態個資檔案應個別列出
 - 紙本：實體
 - 電子：電子檔、錄音（影）檔、圖片檔（含掃描檔）等
 - 資料庫：僅保存於資訊系統內，未另外列印成紙本或另存成電子檔案
- **儲放場所**：個資檔案保管方式（如：檔案櫃上鎖、存於承辦人電腦並加密、資料庫主機...）
- **保存期限**：個資檔案按照法定或自訂的保存期限
 - 法定保存期限：該個人資料檔案依據檔案法等相關法律規定之保存期限（如：3年、5年...）並請說明法定依據
 - 自訂保存期限：該個人資料檔案依據本機關自訂之保存期限（如：3年、5年...）
- **刪除銷燬**：該個人資料檔案之銷毀方式（如：由總務單位統一辦理銷毀作業...）
- **數量**：概數即可



客訴管理流程個資盤點表範例

檔案編號	作業流程名稱	個資行為態樣 (可複選) 1.蒐集 2.處理 3.利用 4.國際傳輸	個人資料			直接蒐集			間接蒐集			告知義務		委託或受託		保管儲存與刪除銷燬				數量 (概數)
			檔案名稱	種類及類別	類型 1.紙本 2.電子檔 3.資料庫 4.其他	方式	特定目的	法定情形	來源	特定目的	法定情形	告知與否	免告知法定事由	有無	委託者或受託者	資料載體	儲存場所	保存期限 1.法定 2.自訂 3.其他	刪除銷燬	
1	客訴管理	1.2.3.	客服表單	姓名、電話、電子郵件、住址	電子檔 資料庫	網頁蒐集	客訴管理	契約				網頁告知		無		電子檔	資料庫	系統存續期間	期限後刪除銷毀	5000
2	客訴管理	1.2.3.	客服錄音檔	姓名、電話、電子郵件	電子檔 資料庫	語音蒐集	客訴管理	契約				語音告知		無		電子檔	資料庫	系統存續期間	期限後刪除銷毀	4000





自評表

16	公司是否有針對含有個人資料之業務進行個資盤點？ (個資法施行細則第12條第2項第2款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.每年度定期、不定期實施稽核作業 2.改善措施及紀錄
----	--	--	---



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

風險評估



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



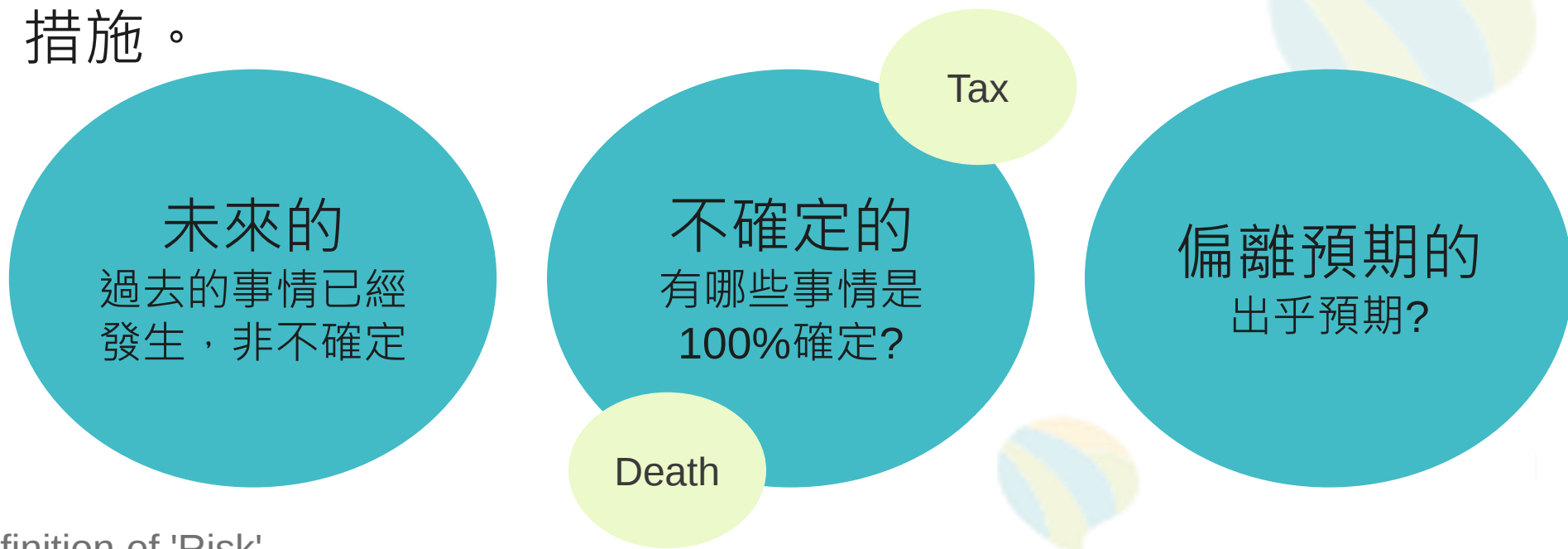
因應風險之規劃

- 組織應建立與維持個人資料相關之風險分析與評估程序，風險分析與評估程序應包含以下事項：
 - 建立與維護個人資料風險準則，包括風險接受準則與實施個人資料風險分析與評估的準則
 - 確保重複之個人資料風險分析與評估產生一致、有效及可比較之結果
 - 識別個人資料風險與風險擁有者
 - 分析個人資料風險，包括風險實現時可能導致之潛在後果、風險發生之實際可能性與決定風險等級
 - 評估個人資料風險，包括比較風險分析結果與訂定已分析風險之風險處理優先次序
 - 所識別風險應包含組織與當事人的影響



風險的定義

- 組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨的風險，視需求訂定管控措施。



Definition of 'Risk'

Definition: Risk implies future **uncertainty** about **deviation from expected earnings or expected outcome**. Risk measures the uncertainty that an investor is willing to take to realize a gain from an investment.



風險分析的方法與目標

- 個資作業流程圖 + 個資盤點清冊比對
- 目標：
 - 資源分配
 - 管控措施挑選

企業實作參考

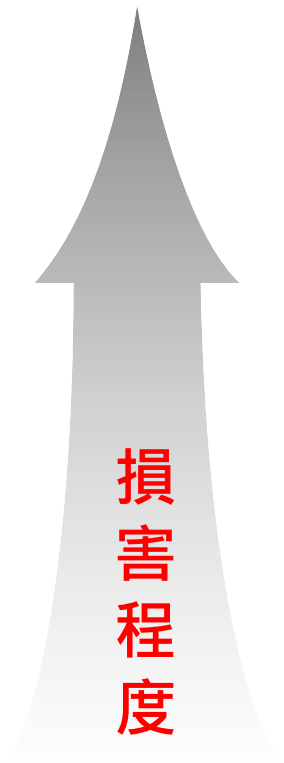
如某公司個資風險之分析進行方式包含：

1. 確定權責單位
2. 確定個資價值衝擊判定等級、威脅或弱點判定等級表、威脅弱點風險組合
3. 確定可接受風險值之基準值
4. 確定風險安控計畫格式、內容、負責部門及完成期限
5. 確定風險評鑑清冊更新週期（半年或一年）



風險管控措施

例：個資保險



損害程度



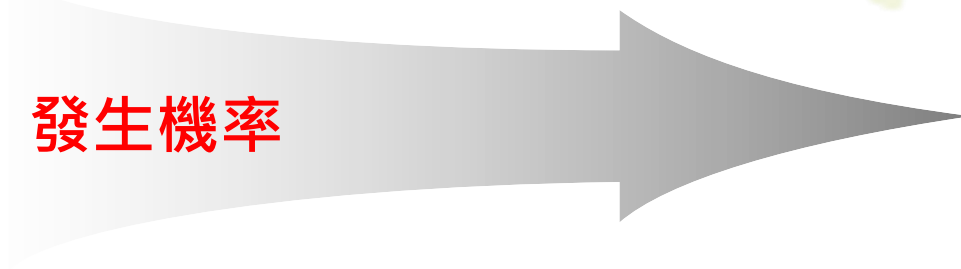
例：目的外利用



例：蒐集程序



發生機率





個資流程作業風險評估表填寫說明

TPIPAS教學用

欄位	填寫說明
主要業務、職掌	依個資流程衝擊分析表之「主要業務、職掌」欄位填寫。
細部作業名稱	依個資流程衝擊分析表之「細部作業名稱」欄位填寫。
風險大分類	依「細部作業名稱」囊括之個人資料檔案形態填入，詳細內容請參考風險情境表。 若「細部作業名稱」囊括之個人資料檔案含委外作業，則需加入委外作業類。
風險子分類	依前欄之風險大分類展開風險子分類逐一填入，詳細內容請參考風險情境表。
個資檔案控管措施(風險情境)	依前欄之風險子分類展開該類別風險情境，詳細內容請參考風險情境表。
衝擊值	從個人資料衝擊分析表將衝擊值填入。
個資侵害風險發生可能性評估	以「個資侵害風險發生可能性」欄位所述級距進行評估。 於受評估之個資作業流程中，該風險情境不存在者，填「0」(不適用)。
風險值	個資作業流程衝擊值×風險發生可能性。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。



風險評鑑表範例(1/5)

個人資料衝擊分析表								
作業流程名稱		衝擊分析項目				衝擊值	備註	單位名稱
主要業務、職掌	細部作業名稱	個資數量	個資敏感度	損害組織信譽	個資當事人隱私衝擊			
		5:每年產生大於1000筆	5:包含姓名、身分證號、私人連絡方式(電話+地址)、財務情況、指紋、特種個資	5:若作業發生個資外洩事故，將導致組織形象信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾集結遊行抗爭或上級機關關切等情形。	5:洩漏資訊，對個資當事人造成重大影響如：勒索、綁架。			
		3:每年產生100~1000筆	3:包含姓名、身分證號、護照、私人聯絡方式(電話及地址)、其他非特種特資欄位	3:若作業發生個資外洩事故，將導致組織形象信譽受到嚴重損害，如：導致3家以上媒體報導負面新聞或造成民眾至機關抗議或陳情等情形。	3:洩漏資訊，對個資當事人有部分影響，如：遭受不明騷擾、詐騙。	衝擊值係以衝擊構面之評分加總		
		1:每年產生小於100筆	1:僅含姓名、聯絡方式(電話)	1:若該作業發生個資外洩事故，將導致組織形象、信譽受到輕微損害，如：導致部份媒體報導負面新聞、造成多位民眾電話抱怨等情形。	1:洩漏資訊，對個資當事人產生些微影響			
○○○業務之規劃、推動與輔導	○○活動報名作業	5	3	1	3	12		○○單位



風險評鑑表範例(5/5)

作業流程名稱		風險控管分類			衝擊值I	個資侵害風險發生可能性P (弱點與威脅分析)	風險值	備註	單位
主要 業務職掌	細部 作業名稱	風險 大分類	風險 子分類	個資檔案 控管措施	從個人資 料衝擊分 析表將衝 擊值帶入	5：控管嚴謹度低、經常被 忽略、現行個資檔案控管方 式沒有詳細規範。	I×P		
						3：控管嚴謹度中等、偶發 性被忽略、現行個資檔案控 管方式僅有部分規範。			
						1：控管嚴謹度高、充分落 實，現行個資檔案控管方式 已有詳細規範。			
						0：不適用			
○○○業 務之規劃、 推動與輔 導	○○活動 報名作業	1.紙本類	1.1處理	1.1.1紙本 文件於內 部處理過 程中，長 時間不使 用或下班 時收存於 辦公室上 鎖之資料 櫃。	12	1	12		○○單位



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

教育訓練



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



相關實務案例

行員向保全洩露客戶個資 金管會要台新銀 落實3件事

本文共591字

要求台新銀落實法遵
加強員工教育訓練
積極和個案當事人溝通



2022/01/27 18:21:27

中央社 記者謝方媛台北27日電  讚 1

近日台新銀行板南分行行員向保全洩露客戶個資，引起外界譁然，台新銀已開除行員並向金管會通報重大偶發事件。金管會指出，將要求台新銀落實法遵、加強員工教育訓練、積極和個案當事人溝通。

一名網友近日在網路社群平台Dcard發文控訴，日前去新北市板橋區台新銀行板南分行辦理開戶，沒想到保全覺得該名網友漂亮、想認識，行員就將開戶資料中的電話號碼抄給保全，因此網友離開後遭保全用電話號碼加LINE傳訊息。



相關實務案例

臺灣高等法院107年度上易字第188號民事判決

當事人

1. 某中華郵政員工透過公司內部電腦系統，擅自查詢當事人的個人資料，並洩漏給第三人。
2. 請求中華郵政公司連帶賠償當事人每人各12萬元。

公司

1. 已安排個人資料法相關教育訓練課程。
2. 留有查詢帳戶資料記錄以供查核。
3. 中華郵政公司已善盡監督義務。

法院

1. 每違法查詢一次客戶資料以1萬元計算，最高判賠新台幣8萬元。
2. 企業除適時法令宣導與教育訓練外，應建置**內部查核機制**，隨時查考從業人員有無落實該項法令及防弊措施。
3. 企業主不能僅以安排教育訓練即卸免監督之責。



自評表

19	定期針對新進人員及內部員工施以個資保護與管理相關教育訓練，以培養其個資保護之意識與能力？(個資法施行細則第12條第2項第7款)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.各年度辦理的情形 2.內控稽核及個管人員規劃
----	---	--	--



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

紀錄機制



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



紀錄管理重點

管理重點

結合內部管理

因應法規要求

協助訴訟舉證

使用紀錄、軌跡資料及證據保存可作為內部安全管理措施之一環，如軌跡資料包含相關log紀錄，可判別資料存取人員、時間、設備等，搭配內部控制作為或規範，倘發生有異常狀況，即可適時處理。

配合個資法第7條修正，蒐集者對當事人同意之事實負有舉證責任，如有相關使用紀錄、軌跡資料及證據保存，亦可協助訴訟程序之舉證。



自評表

15	公司是否訂定管理程序以保存個資管理紀錄、軌跡資料或證據？(相關規定：施行細則第12條第2項第10款、辦法第6條)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.SOP
----	--	--	----------------------------------



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

事故緊急應變



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



個資事故之通知（1/2）

- **個資法第12條**

- 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。

- **通知的方式（個資法施行細則第22條第1項）**

- 即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。
- 但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

- **通知的內容（個資法施行細則第22條第2項）**

- 依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。



指定非公務機關個人資料檔案安全維護辦法

• 事故通報（本辦法§ 4）

- 非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制：
 - 事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。
 - 事故發生後應受通報之對象及其通報方式。
 - 事故發生後，其改善措施之研議機制。
- 非公務機關遇有重大個人資料事故者，應於知悉後一小時內通報本會，並於七十二小時內依附表格式，續行通報本會。但非公務機關接獲本會或有關機關通報發生事故時，應於四十八小時內，依附表格式通報本會。
- 前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，並有下列情形之一者：
 - 危及非公務機關正常營運之虞。
 - 造成當事人權益重大損失之虞。
 - 達本會裁處通訊傳播事業違反個人資料保護法罰鍰案件處理要點第二點之評量表第（一）項第（13）小項所定很嚴重等級以上。
- 第一項第三款所研議之改善機制，應經取得相關認證資格之機構，進行整體診斷及檢視。
- 本會接獲非公務機關依第二項通報後，得依本法第二十二條至第二十五條等規定，為適當之監督管理措施。



個人資料侵害事故通報及紀錄表

公司名稱：	通報時間： 分 年 月 日 時	
姓名：	通報人： 職稱：	簽章
	電話：	
	電子郵件：	
	地址：	
事件發生時間		
事件發生種類	☐ 竊取 ☐ 洩漏 ☐ 竄改 ☐ 毀損 ☐ 滅失 ☐ 其他侵害 事故	個資侵害之總筆數 (大約) _____ 筆
		☐ 一般個資 _____ 筆 ☐ 特種個資 _____ 筆
發生原因及事件摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後 72 小時內通報	☐ 是 ☐ 否，理由	



通報方式（電子郵件）



國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法第四條之通報方式(電子郵件)

📅 111/07/01

通訊傳播事業(本辦法指定非公務機關)通報方式(電子郵件)

通訊傳播事業(本辦法指定非公務機關)通報方式 電子郵件：notify@ncc.gov.tw





思考-是否符合個資事故通知要求？



和雲行動服務

【和雲行動服務聲明稿】

2023 年 2 月 1 日

近日新聞媒體提及本公司 iRent 資料庫部分資料存在外洩風險，經內部調查後，為紀錄應用程式 Log 檔之「暫存資料庫」發生防護性缺口，倘外部專業資訊人員使用特定工具及技巧，可能得以進入該資料庫內查詢近三個月的會員異動資料。

本公司在 1/28(六)接獲通報 1 個小時內，已將該資料庫之缺失防堵，並加強、提高安全防護等級，致力防免資安事件。

經過本公司初步評估，可能受影響會員資料約有 14 萬筆，包括會員姓名、電話、地址、經遮蔽保護的部分信用卡資訊。本公司將儘速針對可能受影響之用戶寄發通知與補償，提醒用戶留意潛在詐騙風險。

本公司除再次針對主機系統做弱點及滲透掃描外，亦將對 iRent App 進行源碼掃描，確保客戶交易過程全程採用 SSL 安全加密，同時全面盤查 iRent 現有各項對外服務資源，進行資安驗證。本公司已申請導入 ISO 27701 隱私資訊管理系統，亦委請外部第三方專業資安廠商針對現行服務，再次全面進行資安健檢與加強防護。



自評表

編號	查核項目(相關規定)	建置(執行)情形	具體措施(含佐證資料)及補充說明 (參考依據或說明)
3	公司因應個資之竊取、竄改毀損、滅失或洩漏等安全事故，是否訂定應變、通報及改善機制？(相關規定：個資法第27條第1項、施行細則第12條第2項第4、11款、辦法第4條)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.如於稽核作業時，是否包括模擬實務演練？ 2.改善措施SOP



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

績效評估 / 改善



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE



stli



有效性量測

- 組織應針對個人資料管理制度之實施，建立分析量測機制，藉由使用各項方式，使管理代表能判定個人資料管理制度內所建立之程序與機制是否有效，將所進行之分析量測作成紀錄，以確保制度之持續有效運作與改善。



內部評量

- 組織每年應依其特性規劃執行內部評量，以瞭解個人資料管理制度是否符合下列要求：
 - 符合法規及本制度之要求。
 - 符合個人資料保護管理政策、手冊及相關具體規則之要求。
- 組織應規劃內部評量方式及流程，以決定內部評量之準則、範圍、頻率及方法。
- 組織應將內部評量之規劃、執行、報告、改善、追蹤等事項製作書面之內部評量報告。



自評表

編號	查核項目(相關規定)	建置(執行)情形	具體措施(含佐證資料)及補充說明 (參考依據或說明)
2	公司保有用戶個資達五千筆以上者，是否訂有個資安全稽核機制並定期(內稽及外稽)執行？或未達者，是否訂有內部稽核機制及定期執行？(相關規定：個資法第27條第1項、施行細則第12條第2項第3、5、6、9款、辦法第3條第3項)	是 ☐ 否 ☐	(參考本會107~109年委託案所擬檢查文件) 1.內、外部稽核報告(含改善情形) 2.稽核週期



臺灣個人資料保護與管理制度

Taiwan Personal Information
Protection and Administration Systems

投入個資保護效益



stli

科技法律研究所
SCIENCE & TECHNOLOGY
LAW INSTITUTE

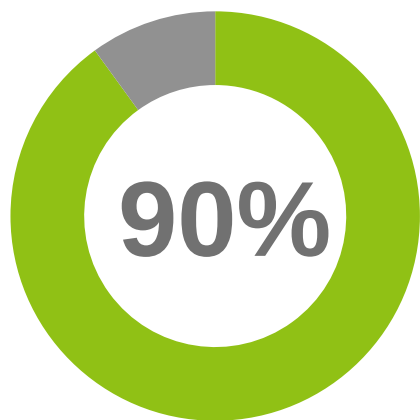


stli



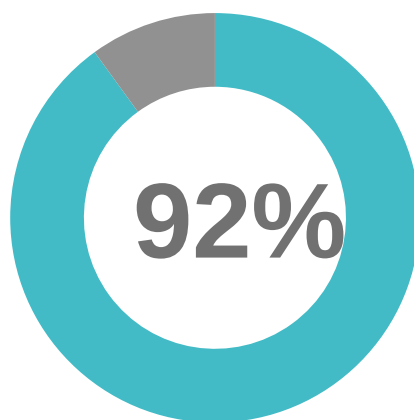
投資隱私的整體價值

個資管理能力為
爭取消費者信賴關鍵



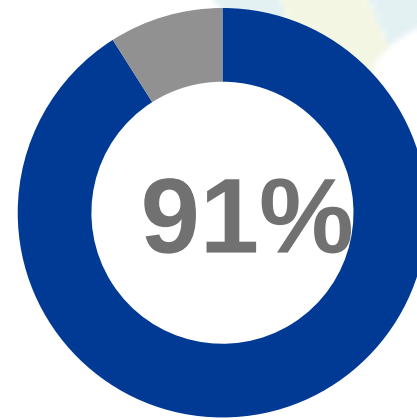
90%消費者認為，若無法信賴企業具有妥善管理個資的能力，即無意願購買其商品或服務。

個資隱私保護意識
為不可或缺之組織文化



92%企業認為，隨著疫情升溫，個資保護議題的重要性亦逐年提高。

取得外部隱私認證
為個資隱私管理有力證明



91%企業認為，供應商是否取得個資隱私管理外部認證，為採購流程必要考慮之關鍵因素。

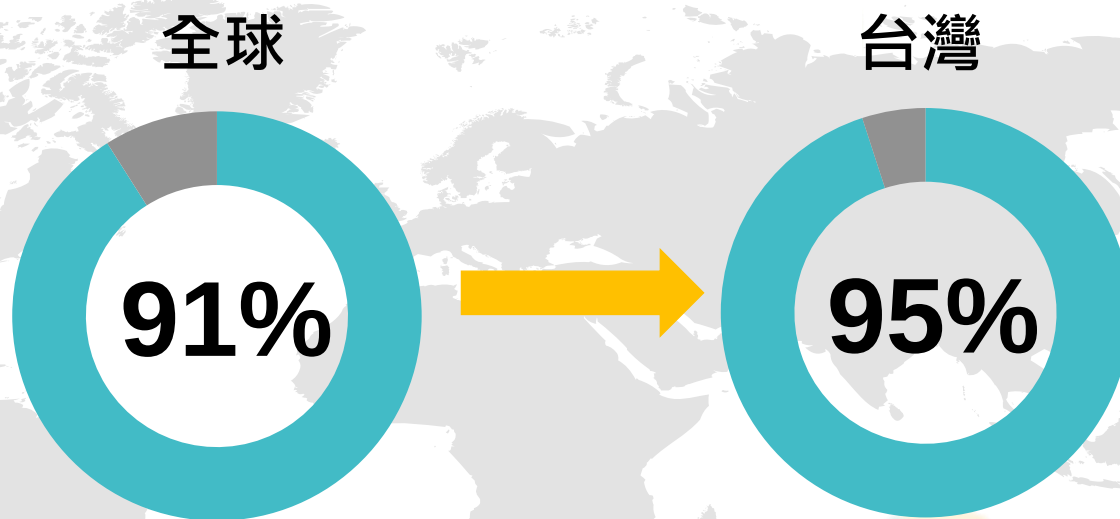
資料來源：

CISCO 2022年「資料隱私基準研究」報告



取得隱私標章的商業價值

隱私標章商業價值



對於世界各地的企業而言，隱私保護已成為真正的商業要素及獲得客戶信任的關鍵原因。**全球高達91%受訪者，將是否取得第三方隱私認證，作為其選擇產品或供應商重要關鍵；在台灣，此比例更是高達95%。**

資料來源：

CISCO 2020年「從隱私到利益：實現投資隱私的正報酬」報告、
CISCO 2021及2022年「資料隱私基準研究」報告

CBPR+TPIPAS最符合國內外個資法要求

制度	CBPR	TPIPAS	BS 10012	ISO 27001	ISO 27701
性質	國際隱私法遵標準	個人資訊管理系統 (PIMS)	個人資訊管理系統 (PIMS)	資訊安全管理系統 (ISMS)	擴充 27001 增加對資訊安全管理要求
主導單位	APEC	我國數位部	英國標準協會	國際標準組織	
特色	以國際要求銜接各國法遵規範，建立國際性一致性標準	● 唯一依照我國個人資料保護法為基礎設計 ● 銜接 APEC CBPR 國際要求	● 主要依循 GDPR設計	第一個全球資訊安全管理的國際標準	包括： ISO27001、 ISO27002、 ISO29100
所涉法令標準	國際法	我國個資法	GDPR	國際標準	國際標準





Thank you



臺灣個人資料保護與管理制度

- ◆ 服務專線：(02) 6631-1069
- ◆ 傳真專線：(02) 6631-1001
- ◆ 服務信箱：tpipas@iii.org.tw
- ◆ 聯絡地址：台北市大安區敦化南路2段216號22樓

