民宿業個資教育訓練

李怡親 法律研究員
資策會科技法律研究所
2023.12.21

ichinlee@iii.org.tw
www.iii.org.tw

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

2023 © 資訊工業策進會 Institute for Information Industry

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
個資事故及法律責任
何謂行政檢查

02 個資保護實務教戰指引

制定個資安全維護計畫
個資盤點表
風險評鑑表
教育訓練
事故通報
紀錄機制

2023 © 資訊工業策進會 Institute for Information Industry

01 個資法遵重點提示

2023 © 資訊工業策進會 Institute for Information Industry

在我們上課前，先來考考大家

情境一、約翰第一次前往澎湖旅遊，興高彩烈的前往在訂房網預定的民宿，一抵達民宿業者要求登記並列印身分證，但最近詐騙案許多，約翰對此感到些許不安...

- Q1：訂房網訂定房間後，收到支付訂金的要求，如何確認非詐騙?
- Q2：住宿業者可否要求登記、影印旅客的身分證資料嗎？
- Q3：住宿業者可否依民眾提供的基本資料，發送廣告信嗎？
- Q4：住宿業者可否依照民眾訂房資料，分析旅客的住宿喜好嗎？
- Q5：若旅客在訂房網下訂不久後，接到詐騙電話而有財損，經查是因訂房網個資外洩所致，而非住宿業者自身網站出現問題，可否因此不用負責?



2023 © 資訊工業策進會 Institute for Information Industry

再來，我們來看兩個案例

- **案例一**、2021年7月起國軍英雄館訂房系統遭駭客入侵，住客個人資料被詐欺集團掌握，多位民眾遭歹徒假冒國軍英雄館人員以「VIP升等會員享優惠」、「系統作業錯誤」、**「至ATM操作解除分期付款」等話術詐騙而匯款至人頭帳戶，甚至有民眾被詐騙高達60萬台幣**。
- **案例二**、2023年初至今，**Booking.com遭鎖定成「詐騙工具」 今年民眾通報疑似個資外洩案件已破百**，如用戶看到自己關注的日本飯店便宜了1萬元，便按照指示下訂、填信用卡號等資訊，慘被盜刷約新台幣1.2萬；今年8月，另有一名用戶收到自己在Booking.com上預訂的飯店信件，並要求驗證信用卡，但點進去後會導入新頁面，且幣別顯示為歐元，該名用戶立刻聯繫Booking客服，業者及飯店均回應此為詐騙。
- 根據刑事局165防騙網統計今年初至今，旅遊網站遭詐騙通報以及諮詢件數，Booking.com已超過百件，Agoda也有30件、Trivago20件、雄獅20件。
- 經過調查，**Booking.com發現近期攻擊為網路犯罪者通過網路釣魚電子郵件，入侵Booking.com合作夥伴的帳戶**；他們也鄭重澄清，Booking.com 並沒有受到任何駭客入侵的情形。

2023 © 資訊工業策進會 Institute for Information Industry

2022年常見詐騙手法統計

假網拍排第一 內政部公布111年詐騙手法

發布日期：112-01-13 09:30 | 單位：警政署

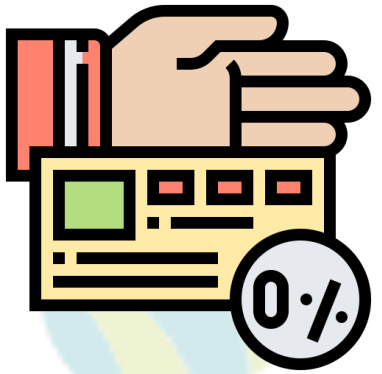
內政部公布111年詐騙手法前3名，分別為「假網路拍賣」、「假投資」及「解除分期付款」，提醒國人遇有任何可疑狀況，或是面對不熟悉的投資模式應謹慎判別，再三考量切勿急躁，並立即撥打110或165反詐騙諮詢專線主動求證。



假網拍



假投資



解除分期付款

2023 © 資訊工業策進會 Institute for Information Industry

多間旅宿業者系統疑似遭駭

小心+886來電 訂房系統疑被入侵竊個資



民視新聞網

更新時間： 2023年6月6日

民視新聞／許家程、張家維 南投報導

有民眾接到自稱來自南投清境民宿業者來電，指稱，自己訂了6間房間，民眾覺得可能接到詐騙電話，因此回過頭向民宿業者查證，業者解釋，訂房系統遭到駭客入侵，導致客人的資料外洩。對此，民宿業者不願回應，只說已經在官網公告，要旅客小心防範。

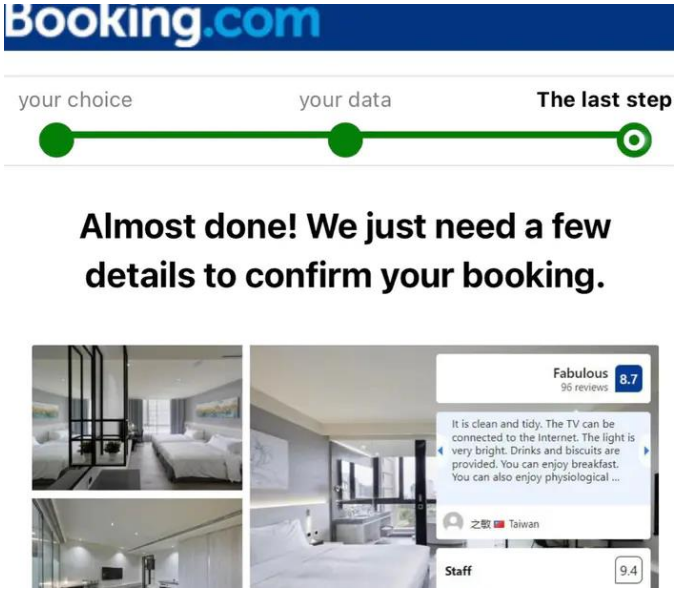
2023 © 資訊工業策進會 Institute for Information Industry

最新詐騙招數分享

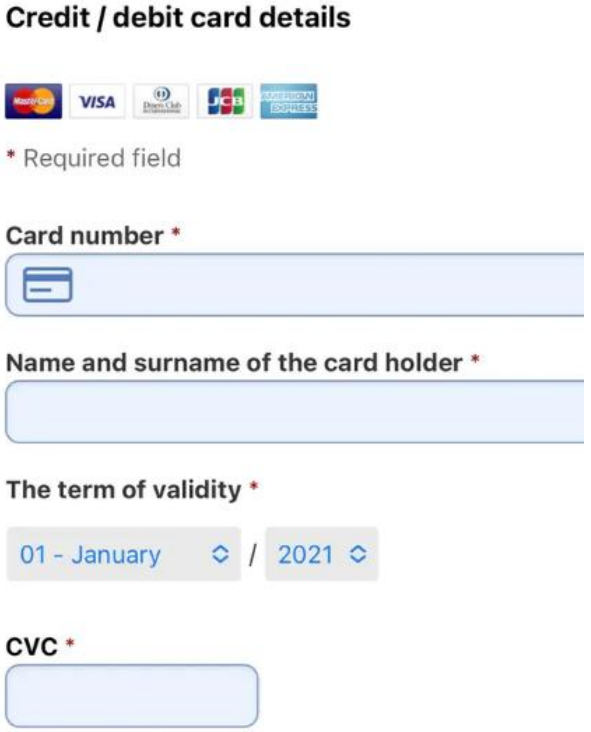


使用App

傳送QRCODE



導引到假網站



付款

2023 © 資訊工業策進會 Institute for Information Industry

消費者如何辨別真偽網站

- Q1：訂房網訂定房間後，收到支付訂金的要求，如何確認非詐騙?

booking.com

Domain Information

Domain:	booking.com
Registrar:	MarkMonitor Inc.
Registered On:	1998-04-17
Expires On:	2025-04-16
Updated On:	2023-09-25

Administrative Contact

Organization:	Booking.com B.V.
Country:	NL

https://whois.domaintools.com/

Booking.com 確認函編號：

寄件者： **Tiffany Lee** <yichinleetiffany@gmail.com>
收件者： XXXX （透過 Booking.com 發送）"
<4177702911-mvuy.edhe.kksf.sve5@property.booking.com>
日期： 2023年11月29日 上午11:50
主旨： Re: 您有來自澎湖夏日南風民宿的訊息
寄件人： gmail.com

您好，房間需先支付訂金1000麻煩於24小時內匯款完成，告知帳號後五碼即可；若需變更日期、人數等，請於「入住日前14天」於民宿上班時間通知（9AM-20:30PM)訂金可全額退還。
逾期未付訂金，訂單將會取消，不再另行通知，敬請見諒，謝謝。

2023 © 資訊工業策進會 Institute for Information Industry

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	駭客資料勒贖
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	駭客勒贖、會員個資外洩
2023	故宮	數千件國寶約十萬張圖檔遭竊賤賣

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	駭客資料勒贖
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	陸駭客展開持續性滲透威脅（APT）行動

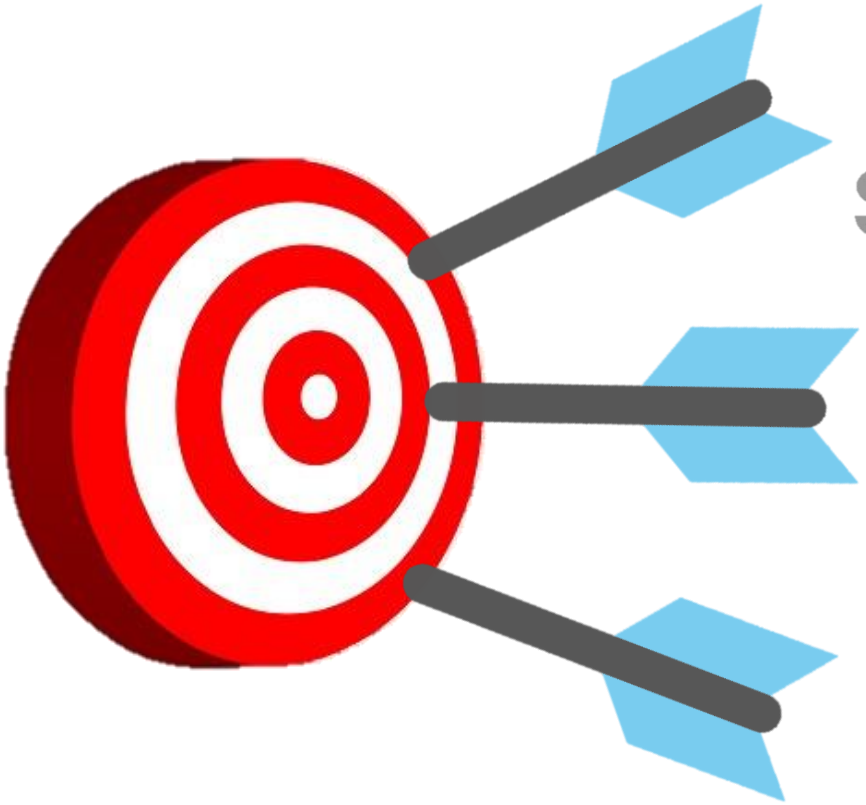
金融機構		
2016.7	第一銀行	東歐駭客入侵盜領8327萬元
2017.2	13家證券公司	首起集體遭駭客勒索
2017.1	遠東銀行	被盜轉6010萬美元
2021.11	7家證券、期貨商	駭客撞庫攻擊、客戶被異常下單

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
2023.05	微笑單車	透過境外IP位址嘗試取得YouBike的會員帳號、密碼

整理自聯合報系列報導：全民遇駭紀實

2023 © 資訊工業策進會 Institute for Information Industry

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
- 籌備處已成立12/5掛牌
- 具獨立性、專責性及機關性

提高個資法相關罰則

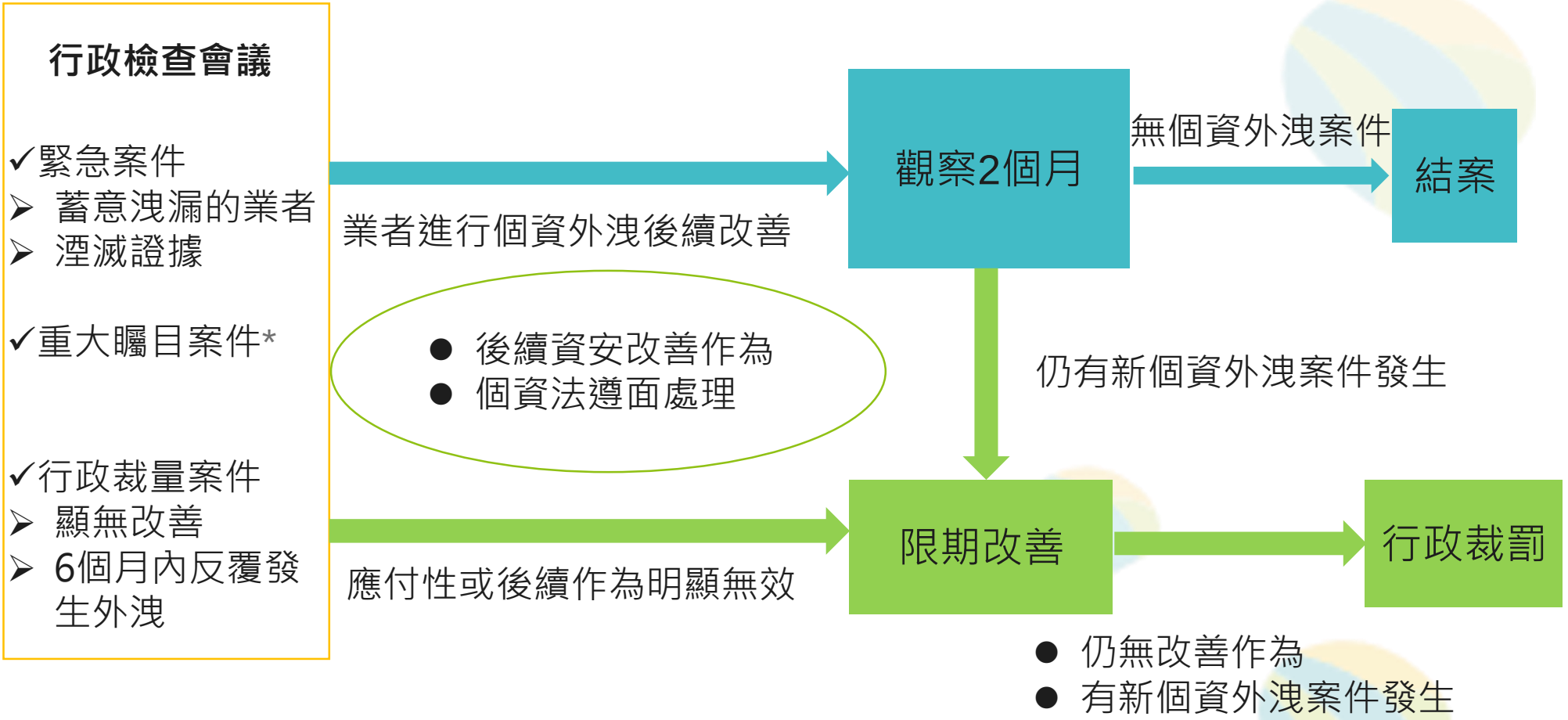
- 非公務機關未善盡個資管理義務，罰鍰提高到2萬元以上、200萬元以下；
- 非公務機關**未善盡適當之安全措施**或**未訂定個資檔案安全維護計畫或業務終止處理方法**，罰鍰提高到2萬元以上、200萬元以下，屆期未改按次處罰
- 對情節重大者，上修罰鍰為15萬元以上、1,500萬元以下

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

2023 © 資訊工業策進會 Institute for Information Industry

行政檢查



*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。

2023 © 資訊工業策進會 Institute for Information Industry

個資檔案安全維護規範現況-2023年

主管機關	業別	辦法數
數位部	數位經濟相關產業個人資料檔案安全維護管理辦法	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		

2023 © 資訊工業策進會 Institute for Information Industry

交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法

- **適用範圍（本辦法§3）**
  - 本辦法所稱非公務機關包括下列各款：
    - 觀光旅館業
    - 旅遊業
    - 民宿
    - 旅行業
    - 觀光遊樂業
- **應訂定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（本辦法§4）**
  - 非公務機關保有消費者個人資料**達八千筆者**，應於2023/10/1完成訂定計畫及處理方法

2023 © 資訊工業策進會 Institute for Information Industry

個人資料檔案安全維護計畫及處理辦法

適當安全維護管理措施（本辦法§5）

（一）配置管理之人員及相當資源。
（二）界定蒐集、處理及利用個人資料之範圍。
（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）設備安全管理、資料安全管理及人員管理措施。
（七）認知宣導及教育訓練。
（八）個人資料安全維護稽核機制。
（九）使用紀錄、軌跡資料及證據保存。
（十）個人資料安全維護之整體持續改善。
（十一）業務終止後之個人資料處理方法。

個資法第27條1項
適當安全維護措施



個資法施行細則第
12條2項11款

2023 © 資訊工業策進會 Institute for Information Industry

PDCA方法論



Plan	Do	Check	Act
個人資料保護與管理制度之**規劃**	個人資料保護與管理制度之**實施**	個人資料保護與管理制度之**有效性評估**	持續**監督**與**改善**

2023 © 資訊工業策進會 Institute for Information Industry

個資法施行細則§12-適當安全維護措施

Plan

1. 配置管理之人員及相當資源
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

Do

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



Action

11.個人資料安全維護之整體持續改善

Check

9.資料安全稽核機制
10.使用紀錄、軌跡資料及證據保存

2023 © 資訊工業策進會 Institute for Information Industry

觀光產業個人資料檔案安全維護自主檢查表（自評表）

公司名稱：
經營業別：
保有個人資料筆數：
是否具對外電子商務服務系統：

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
1	消費者個人資料檔案安全維護計畫	訂定「消費者個人資料檔案安全維護計畫」	是□ 否□	• 個資檔案安全維護計畫 • 各管理措施SOP

2023 © 資訊工業策進會 Institute for Information Industry

臺灣個人資料保護與管理制度

Taiwan Personal Information Protection and Administration Systems

個資保護規劃

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

2023 © 資訊工業策進會 Institute for Information Industry

最容易踩紅線的個資法相關規定說明

個資法規	說明
§12	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。
細則§22	中央目的事業主管機關為執行資料檔案安全維護，認有必要或有違反本法規定之虞時，得請相關人員為必要之說明、配合措施或提供相關證明資料。
§27 I	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。
細則§12 I I	前項措施，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。

2023 © 資訊工業策進會 Institute for Information Industry

交通部指定觀光產業類
非公務機關個人資料檔案安全維護計畫及處理辦法

配置資源（本辦法§6）

- 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，建立個人資料檔案安全維護管理組織，配置相當人員及資源，負責規劃、訂定、修正與執行本計畫及處理方法等相關事項（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，應經非公務機關代表人或經其授權之人員核定署。
- 個人資料檔案安全維護管理組織，應定期就執行任務情形向非公務機關代表人或經其授權之人員提出書面報告。
- 非公務機關應將訂定之安全維護計畫留存營業所在地備查；主管機關得派員檢查。

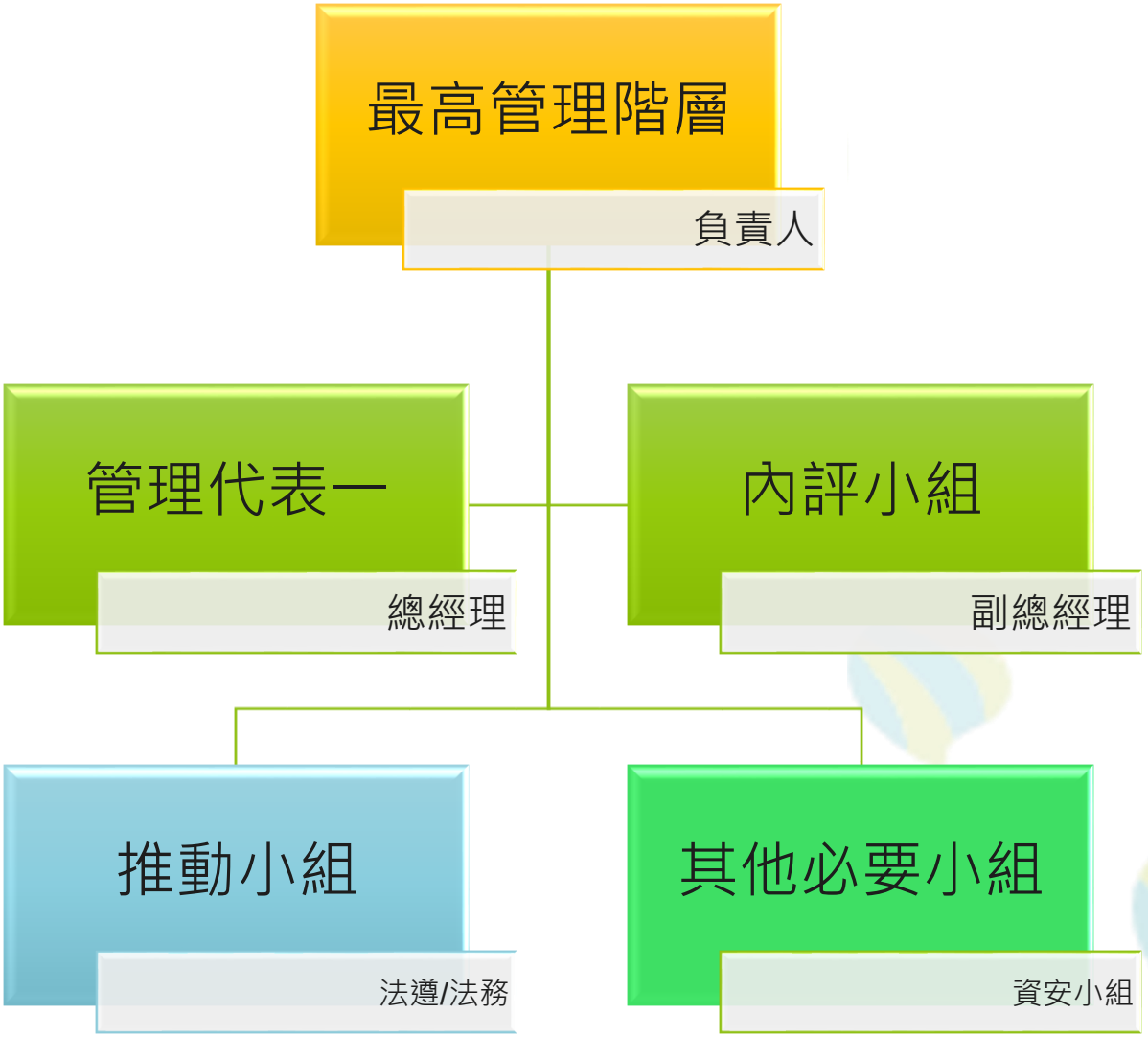
2023 © 資訊工業策進會 Institute for Information Industry

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

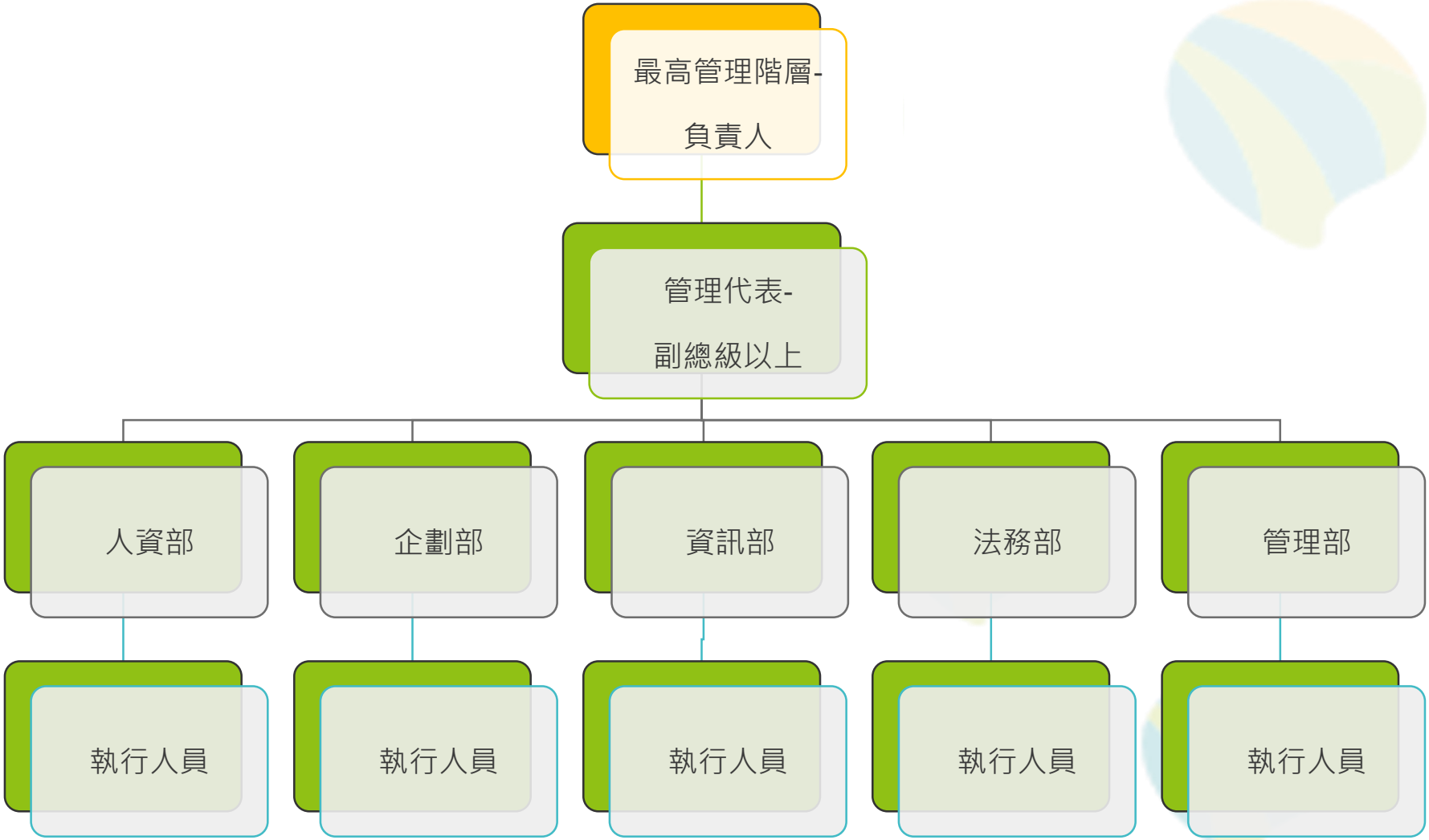
2023 © 資訊工業策進會 Institute for Information Industry

參考架構-任務型



2023 © 資訊工業策進會 Institute for Information Industry

參考架構-組織型



2023 © 資訊工業策進會 Institute for Information Industry

自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
2	公司組織及運管理情形	指定專人或建立專責組織負責管理	是□ 否□	• 個資檔案安全維護計畫 • 各管理措施SOP
3	專責人員或專責組織任務	• 規劃、訂定、修正與執行所訂計畫 • 定期向管理人報告 • 依稽核人員評核結果檢討改進，並向管理人與稽核人員提出書面報告 • 訂定個人資料保護管理政策 • 定期對所屬人員進行宣導或專業教育	是□ 否□	• 佐證資料如：企業組織圖，得以看出個資專責人員配置；政策文件；教育訓練計劃書等

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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」

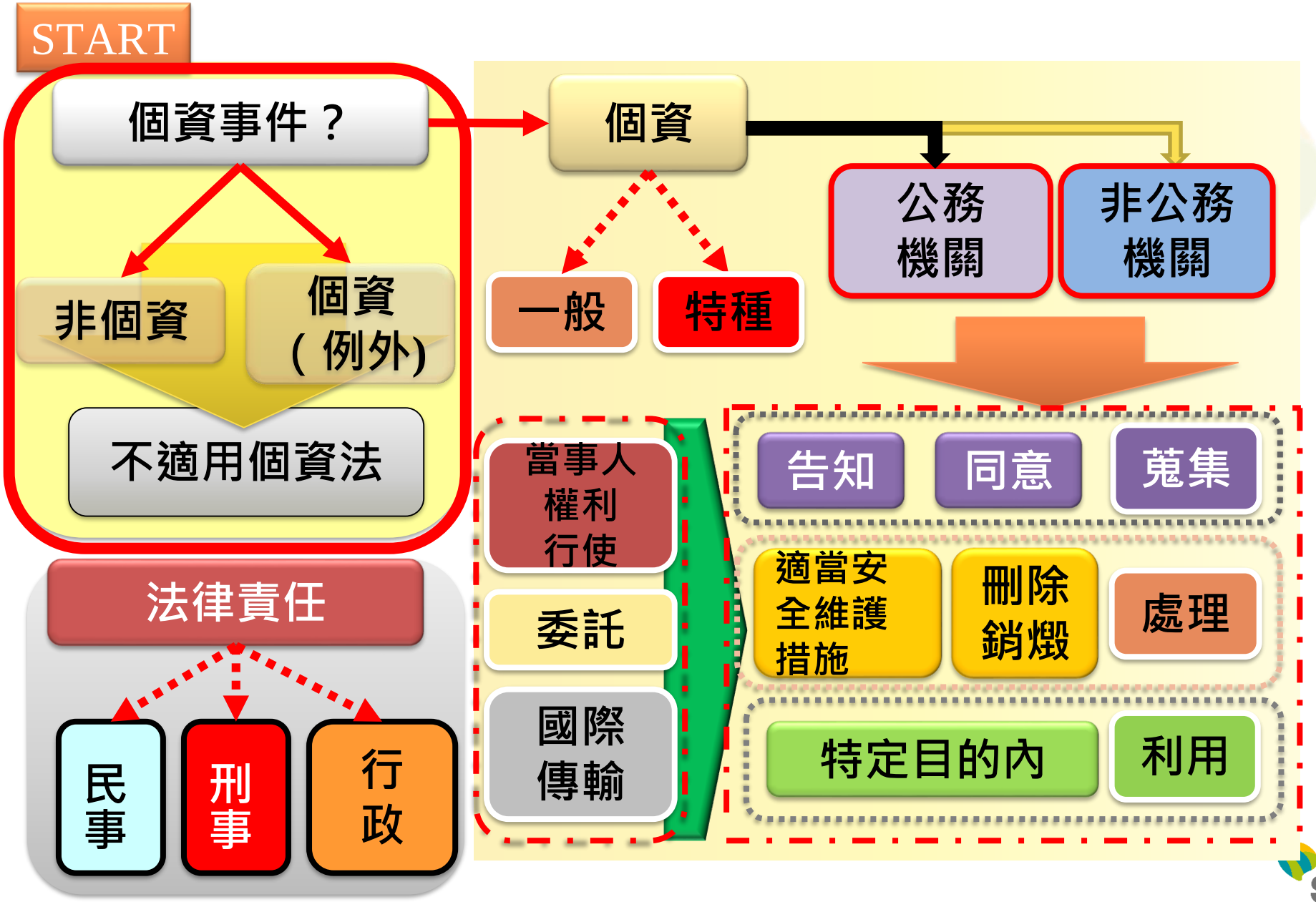
行為規範
增、修訂免告知事由&法定情形

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

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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？



2023 © 資訊工業策進會 Institute for Information Industry

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）

新聞連結

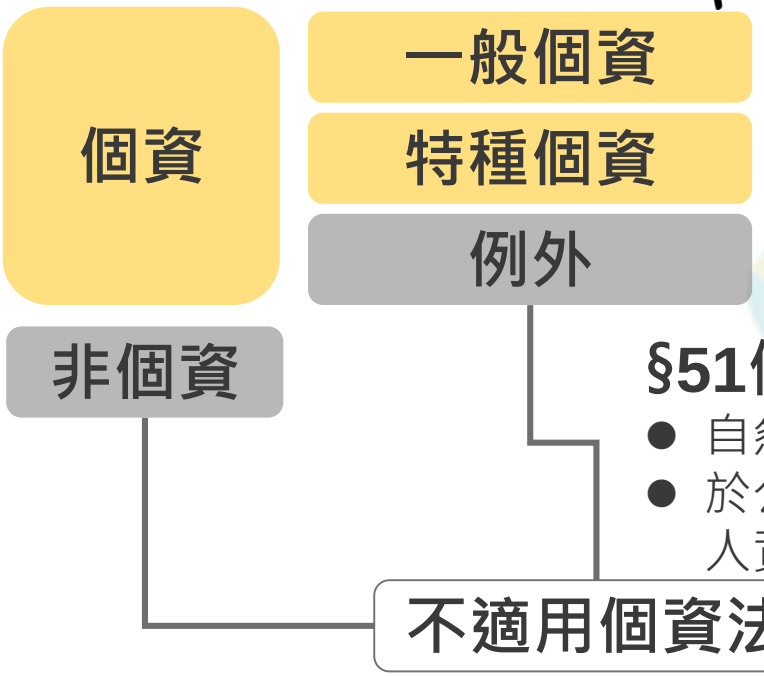
2023 © 資訊工業策進會 Institute for Information Industry

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

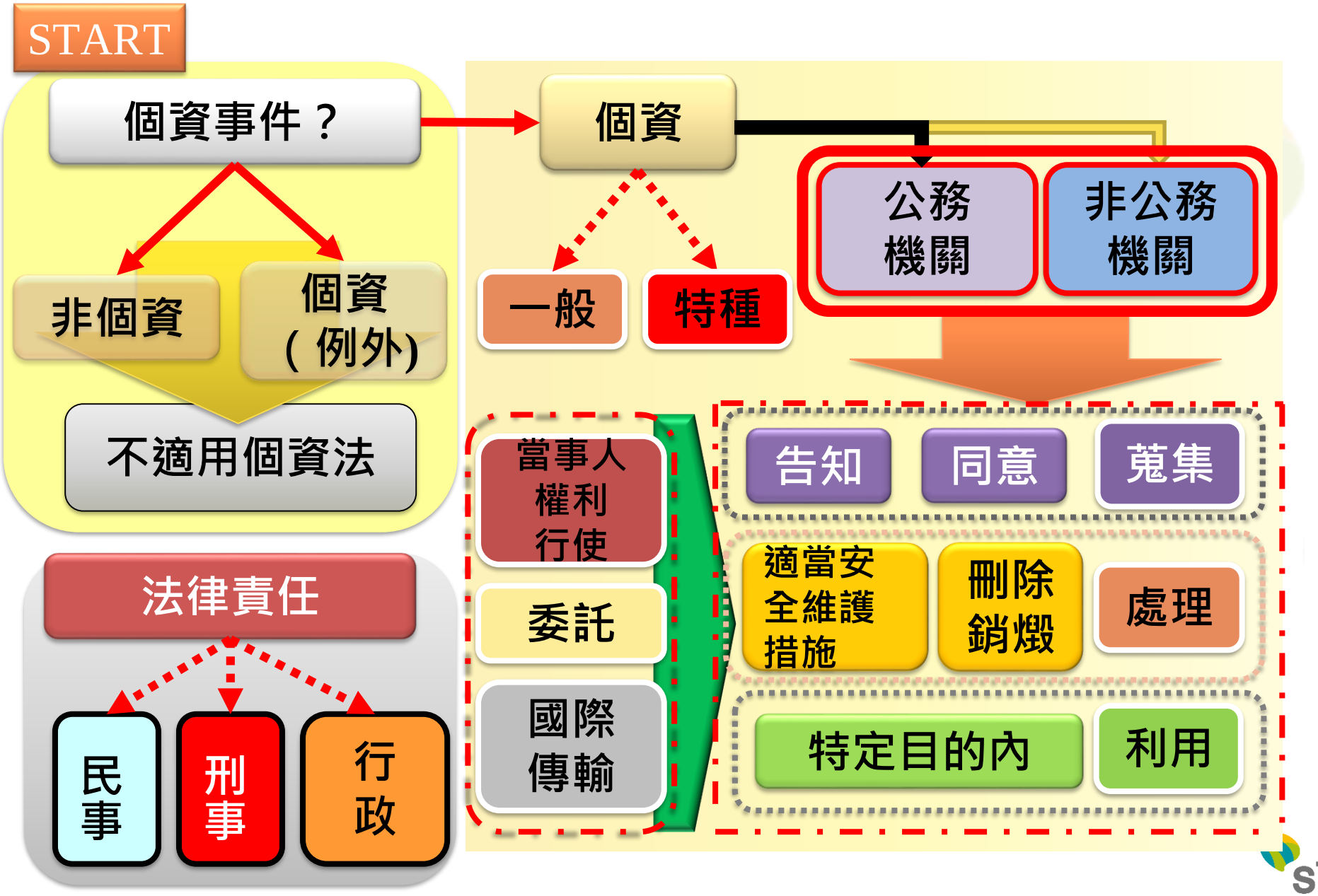
有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，原則上不得蒐集、處理或利用。

§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。

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

公務機關與非公務機關

- 區分實益

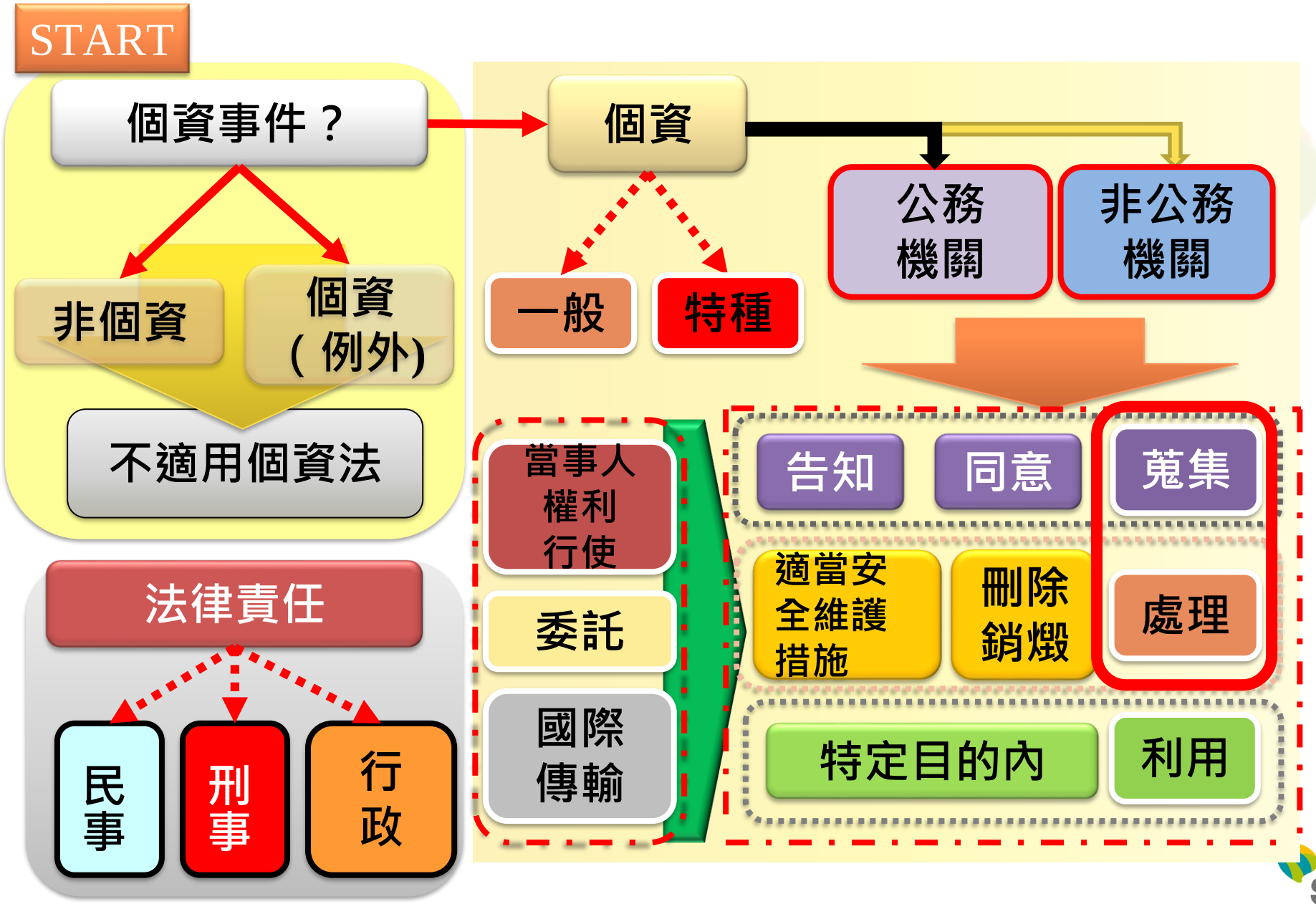
	公務機關	非公務機關
定義	指依法行使公權力之中央或地方機關或行政法人。	指公務機關以外之自然人、法人或其他團體。
蒐集、處理及利用	第二章（個資法第15 - 18條)	第三章（個資法第19 - 27條）
賠償責任的免除	不可抗力	無故意或過失
損害賠償責任依據	個資法+國賠法	個資法+民法

- 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

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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。

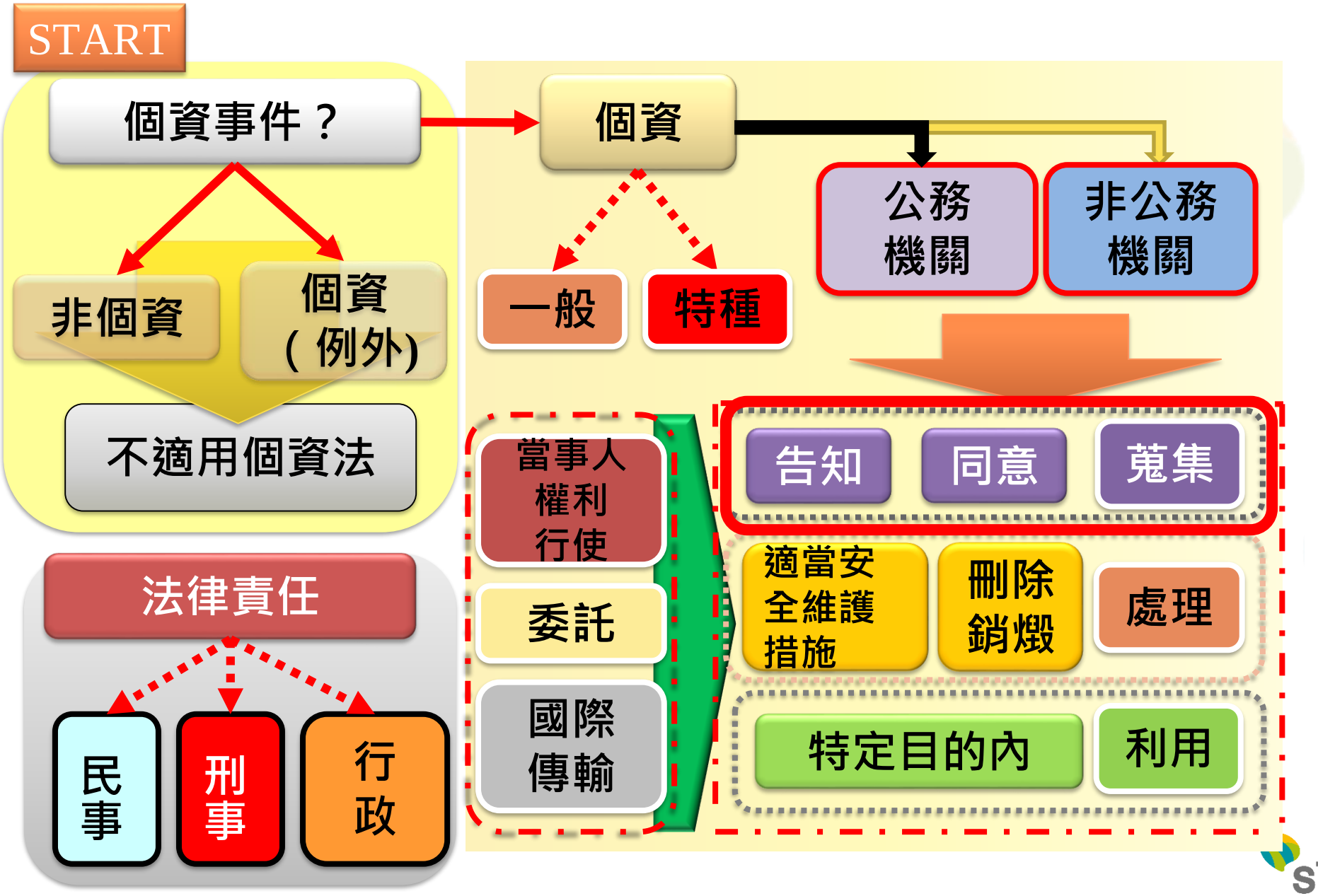
四. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

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。

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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 • 告知將妨害公共利益 • 當事人明知應告知之內容 • 蒐集非基於營利之目的且對當事人無不利影響	• 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

辦法**§11**

非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

2023 © 資訊工業策進會 Institute for Information Industry

告知義務例外要件試舉例

1. 法律規定得免告知

- 「保險法」第177條之1第3項

2. 係機關執行法定職務或履行法定義務所必要

- 稅務機關蒐集納稅人之所得資料，即屬公務機關執行法定職務所必要

3. 告知將妨害法定職務執行

- 法院執行扣押個人的財產，若將蒐集個人資料的狀況告知，該個人可能因而脫產，影響扣押的執行

4. 告知將妨害公共利益

- 線人資料來源

5. 當事人明知應告知之內容

- 個人的郵局金融卡遺失，向郵局申辦新的金融卡，其提供個人資料時，已知應告知的事項，所以郵局不需要再為告知

6. 蒐集非基於營利之目的且對當事人無不利影響

- 為提供員工免費通勤接駁車

2023 © 資訊工業策進會 Institute for Information Industry

個人資料蒐集告知聲明
以中華電信股份有限公司行動寬頻服務為例

(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/電信加值網路業務
● 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

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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		

2023 © 資訊工業策進會 Institute for Information Industry

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、市場或使用者調查、其他更適合您的電信及加值服務方案等。
  - 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)。

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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. 您若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

2023 © 資訊工業策進會 Institute for Information Industry

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**。

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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。**

2023 © 資訊工業策進會 Institute for Information Industry

同意之方式與內涵-兒童個資？

問題：蒐集兒童個資時的告知與同意取得？

國家發展委員會民國 108 年 03 月 12 日發法字第1082000384號函

教材業者欲基於當事人同意，蒐集未成年學童之個人資料，除應注意**業者以贈品誘使學童提供個人資料，是否已違反個資法第5條之誠實信用原則**外，業者另**應踐行個資法第8條第1項相關法定應告知事項**，徵諸上開立法理由，應使當事人得以充分瞭解後審慎為之，是業者之告知方式**應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使該學童得以充分瞭解其個人資料之後續利用**。倘教材業者未完整踐行告知，或其告知對象無法充分瞭解其個人資料之後續利用，則未能符合個資法第7條第1項之規定。另蒐集者就當事人同意合法要件之事實，應負舉證責任（同法第7條第4項規定參照），併予敘明。

2023 © 資訊工業策進會 Institute for Information Industry

案例分享-恐怖娃娃



KAGAMUSHA

★☆☆☆☆ **"Questions like what are you wearing**

Reviewed in the United States on December 30, 2015

Verified Purchase

This doll is a PEDOPHILE'S DREAM!! We gave the doll to our granddaughter for her Christmas Present, it was the 27th because we had to travel. She played with it all day,but by that evening a pervert hacker had hacked her WiFi connection!! "Questions like what are you wearing?" Statements like, "I'm not wearing anything! you shouldn't wear anything too!" At that point, my daughter disconnected the doll from the WiFi!!!

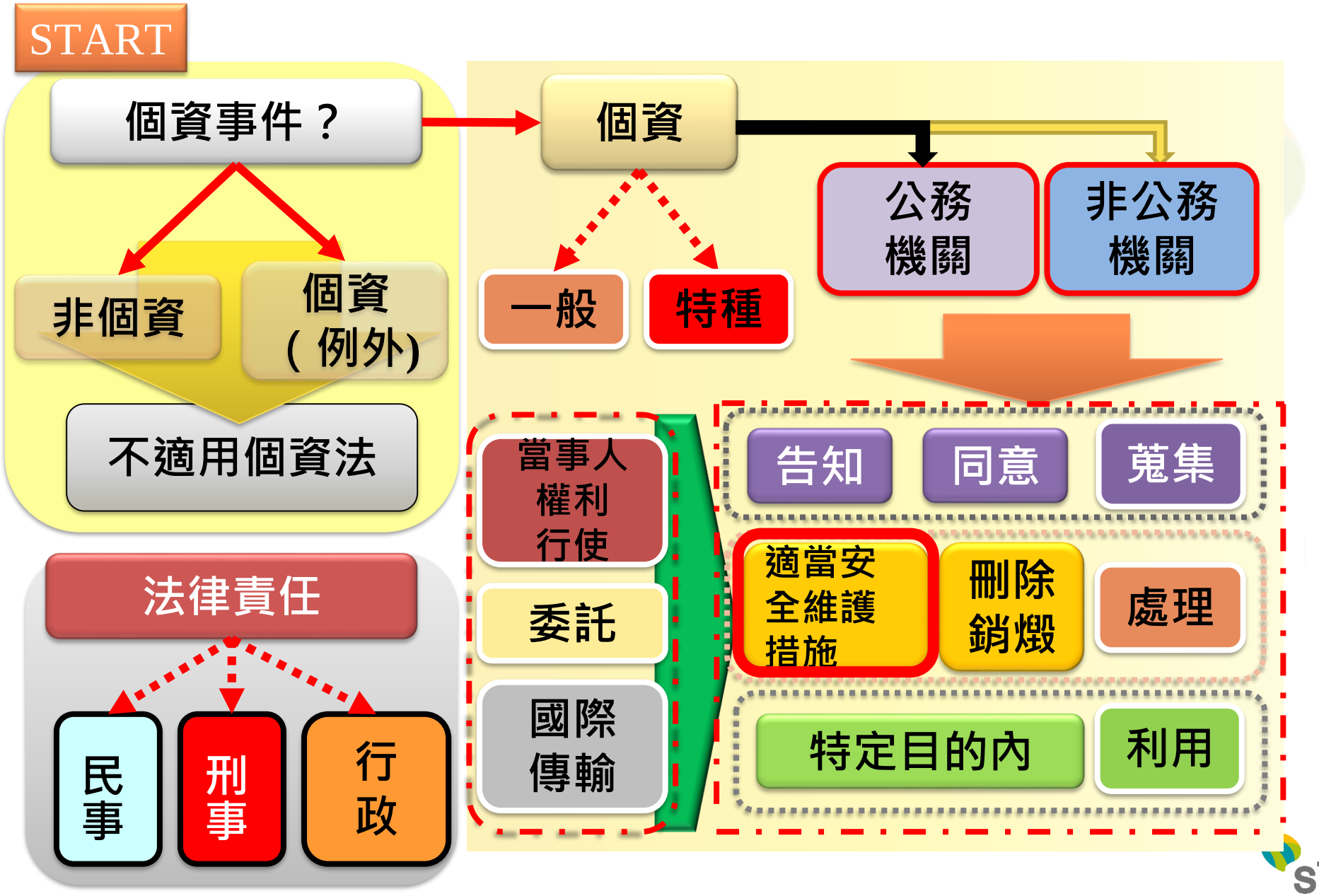
Of course, we will now return this doll for a refund.

Mattel needs to install some kind of encryption to it's Barbie system so little girls will NOT be subjected to what my granddaughter was...

SO, DO NOT BUY THIS DOLL! That is unless you want some damn pedophile hacking the line!!!

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



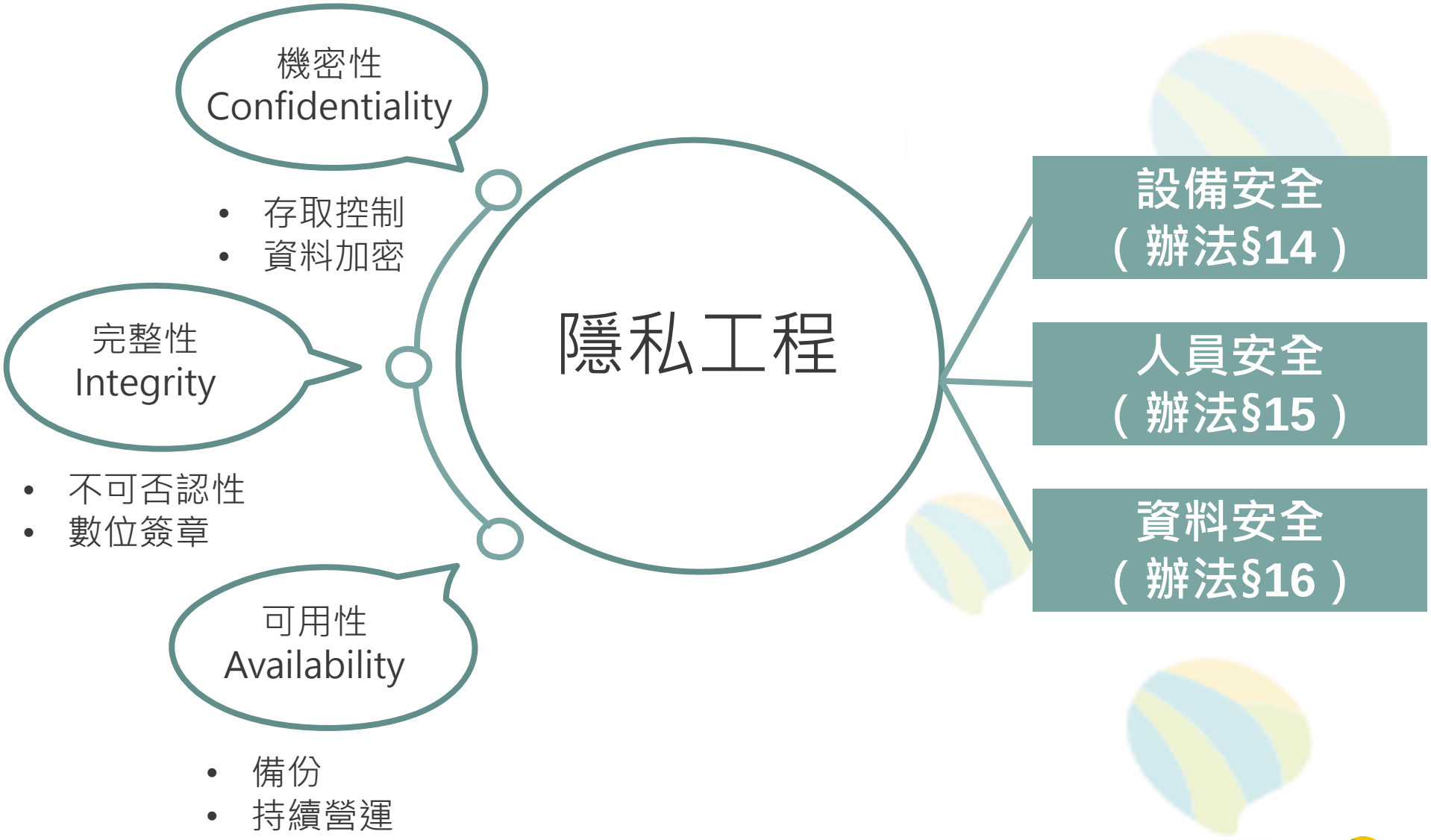
2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

安全管理目標



2023 © 資訊工業策進會 Institute for Information Industry

設備安全

- **辦法§14**

1. **紙本資料**檔案之安全保護設施
2. **電子資料檔案**存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制
3. **存有個人資料**之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，**應採取適當之銷毀或防範措施**，避免洩漏個人資料；**委託他人執行者**，非公務機關對受託者之監督依本法第二十條規定辦理

2023 © 資訊工業策進會 Institute for Information Industry

人員安全

- **辦法§15**

1. 依據業務需求，**適度設定所屬人員不同之權限**，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性
2. 檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員
3. 要求所屬人員妥善保管個人資料之**儲存媒介物**，並約定**保管及保密義務**
4. 所屬人員**異動或離職**時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂**保密切結書**

2023 © 資訊工業策進會 Institute for Information Industry

資料安全

- **辦法§16**

1. 使用者**身分確認**及保護機制
2. 個人資料顯示之**隱碼機制**
3. 網際網路傳輸之安全**加密機制**
4. 個人資料檔案與資料庫之**存取控制**及保護監控措施
5. 防止外部網路**入侵對策**
6. **非法或異常使用行為**之監控及因應機制

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施1

資通安全

- **存取控制**
  - 存取控制（存取控制清單）
  - 帳號管理（申請、開通、停用即刪除程序、登出時間設定等）
  - 職責分工（採用以Role-based access control機制）
  - 最小權限（管理角色應分開管理帳號，非全部使用最高權限）
  - 遠端存取（適當加密、自動監控）
  - 行動裝置存取（VPN、二（多）元驗證）
  - 資訊分享（個資不應儲存於共享資料夾）

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施2

資通安全

- **技術檢視**
  - 稽核事件（事件稽核日誌）
  - 稽核紀錄的檢視、分析（指派專人定期審視事件稽核日誌）

- **識別鑑別**
  - 使用者的識別與鑑別
    - 識別（Identification）:瞭解使用者為何
    - 鑑別（Authentication）:確認使用者身分為本人
      - Something you know（如：個人密碼）
      - Something you have（如：提款卡、憑證）
      - Something you are（如：指紋、聲音、虹膜）
  - 身分驗證管理（變更預設密碼）

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施3

資通安全

- **媒體安全**

- 媒體存取（授權特定人員）
- 媒體標記（書面文件等級標示於封面、封底或以浮水印呈現）
- 媒體儲存（實體管控措施、涉及個資應加密儲存）
- 媒體傳輸
  - 記錄儲存媒體識別資料(編號)、傳送人員簽名、時間、追蹤碼與目的地等紀錄
  - 若個資儲存媒體需委外傳送，應加強其包覆措施之強度，並留下相關紀錄
- 媒體汰除
  - 將重複使用之電子儲存媒體應採用多次亂數覆寫工具(data erasure)以抹除儲存資料，且應限制僅能提供機關內部人員使用；將報廢之電子儲存媒體則應採取消磁或實體破壞的方式銷毀
  - 非電子儲存媒體則應透過水銷或焚燒方式銷毀

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施4

資通安全

- **實體與環境安全**
  - 實體存取控制（存放個資場所採取適當安全措施、出入管制）
  - 實體存取監視（定期檢視有效性，並建立監視機制）
- **資訊傳輸**
  - 邊界保護（系統內外部建立適當監視與控制介面防護）
  - 傳輸機密性（傳輸時進行加密）

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施5

資通安全

- **系統與資訊完整性**
  - 安全性檢測（脆弱性識別、報告與修正；新系統測試，評估潛在結果及衝擊）
    - 系統更新事先測試
  - 稽核事件（規劃並測試稽核特定系統事件）
    - 僅限有權限之使用者
  - 惡意程式防護（針對脆弱點有效部屬惡意程式防護機制）
    - 出入端點、工作站、伺服器或可攜式媒體等設備，有效部署惡意程式防護機制
  - 資通系統監看（監視內外部通訊，及建立通報機制）
    - 資通訊監視內向與外向通識，發現有被入侵跡象，應通報特定人員

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施6

資通安全

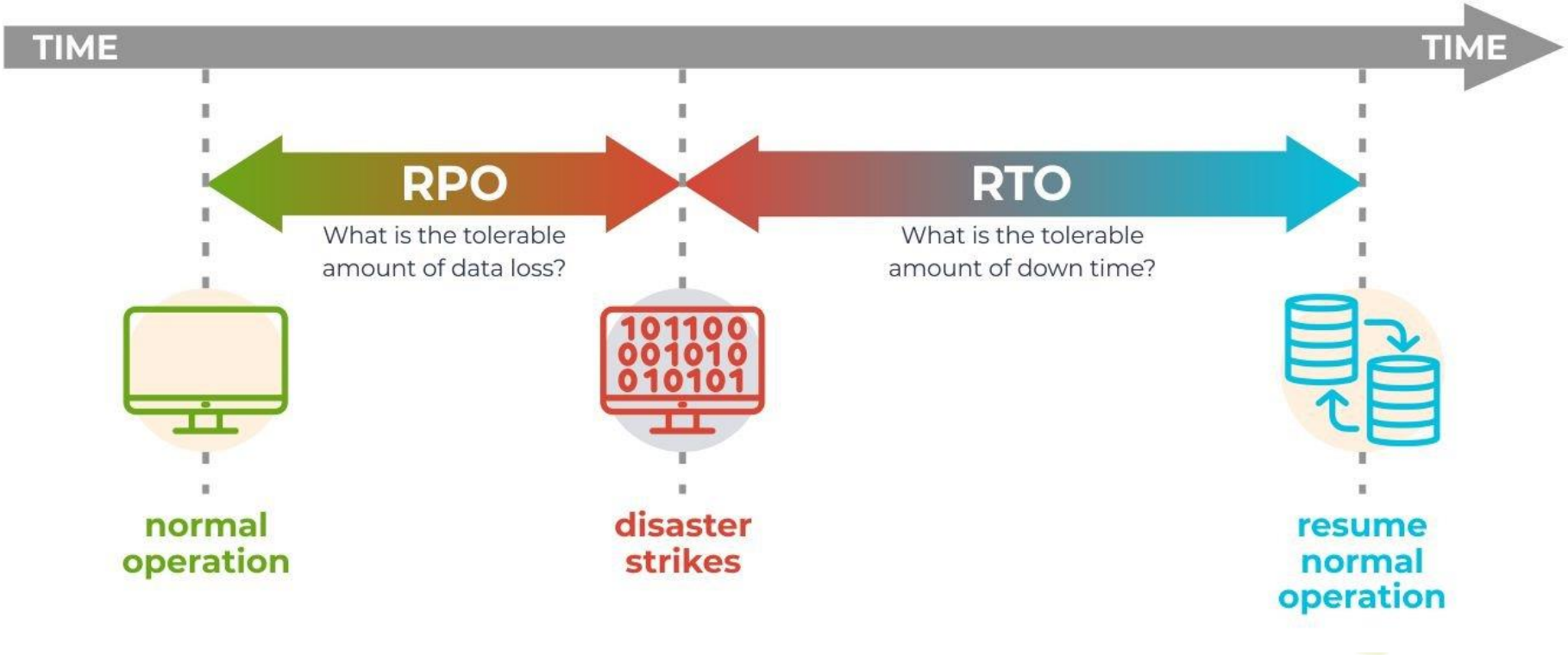
- **系統發展生命週期階段**
  - 系統規劃 (初步調查) ->系統規劃書
  - 系統(需求)分析 ->系統需求書
  - 系統設計 ->系統規格書
  - 系統建置與測試 / 系統開發 ->程式、 測試計畫及報告
  - 系統上線與維護 / 系統實施與評估 -> 釋出計畫、使用者手冊
- **系統發展生命週期委外階段**
  - 依等級將安全需求納入委外契約
- **獲得程序與系統文件**
  - 避免使用真實個資做為系統之測試資料
  - 若有使用真實個資之必要，應透過申請並將許可並留下紀錄

2023 © 資訊工業策進會 Institute for Information Industry

安全管理措施7

資通安全

- 營運持續計畫



2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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。

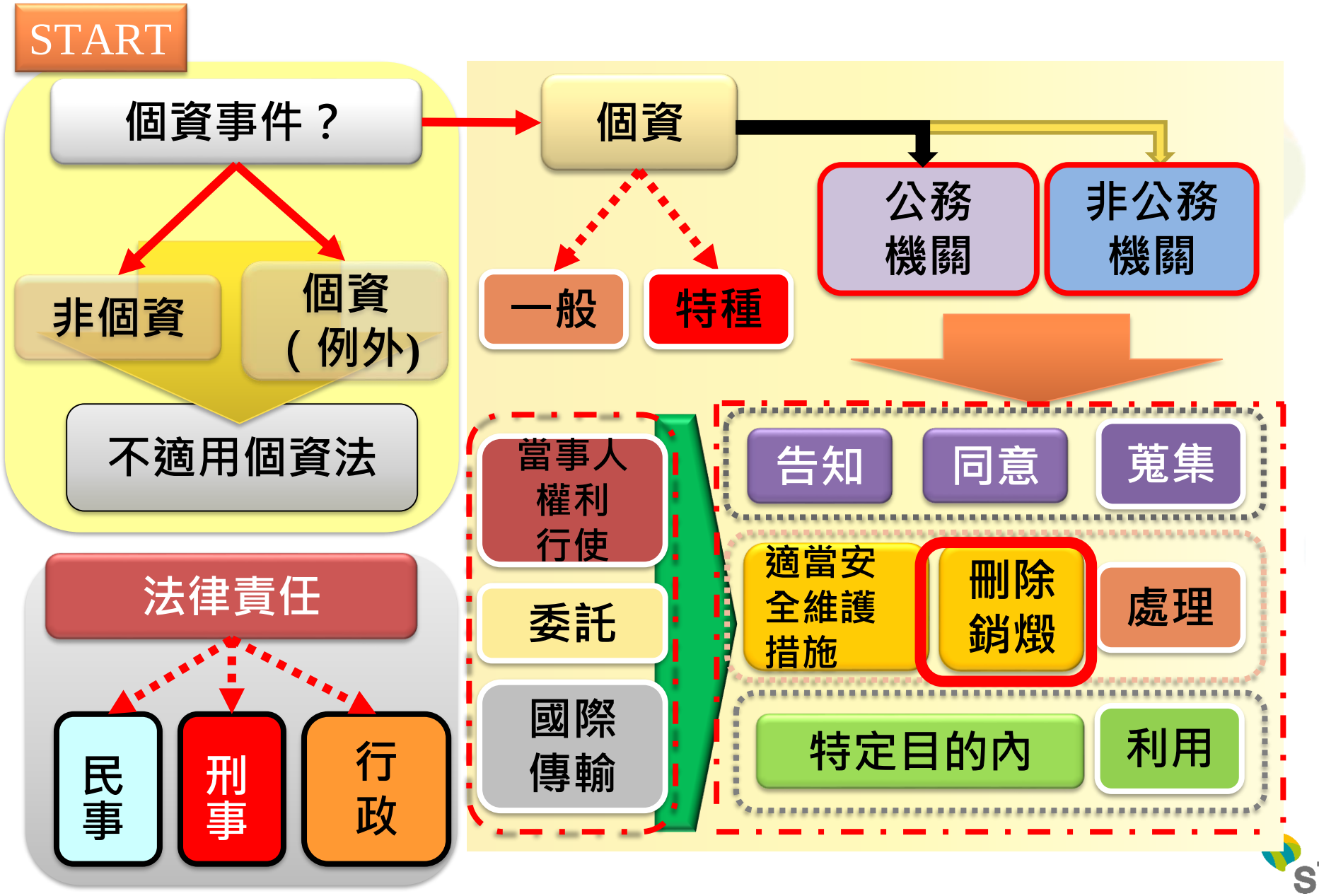
2023 © 資訊工業策進會 Institute for Information Industry

觀光產業個人資料檔案安全維護
自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
5	保有個資達8千筆，且具對外電子商務服務**系統之安全管理**	• 使用者身分確認及保護機制 • 個人資料顯示之隱碼機制 • 網際網路傳輸之安全加密機制 • 個人資料檔案及資料庫之存取控制與保護監控措施 • 防止外部網路入侵對策 • 非法或異常使用行為之監控與因應機制 • 定期演練及檢討改善	是□ 否□	佐證資料如： • 存取措施、存取權限管理、監控審核記錄等 • IP限制、使用VPN加密通道或雙因子認證 • 提供資料庫的結構和設計、針對個人資料的去識別化措施或資料加密截圖 • 留存登入紀錄、監控網站異常流量或異常活動等 • 演練及改善報告
6	環境管理措施	• 對個資存取媒介物及環境(如機房)，採取環境管理措施	是□ 否□	• 佐證資料如：人員進出登記簿定期評估環境溫度、濕度、設備安全等 • 內部評估或稽核記錄、內部制度文件等，應能呈現採取之安全管理措施項目等資訊
9	第三方資安檢測	• 系統弱點掃描 • 滲透測試 • 資安健診 • APP檢測	是□ 否□	• 佐證資料如：定期弱點掃描、滲透測試報告、資安檢測報告或取得第三方資安驗證

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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。

資料擷取自ithome: https://www.ithome.com.tw/news/148716

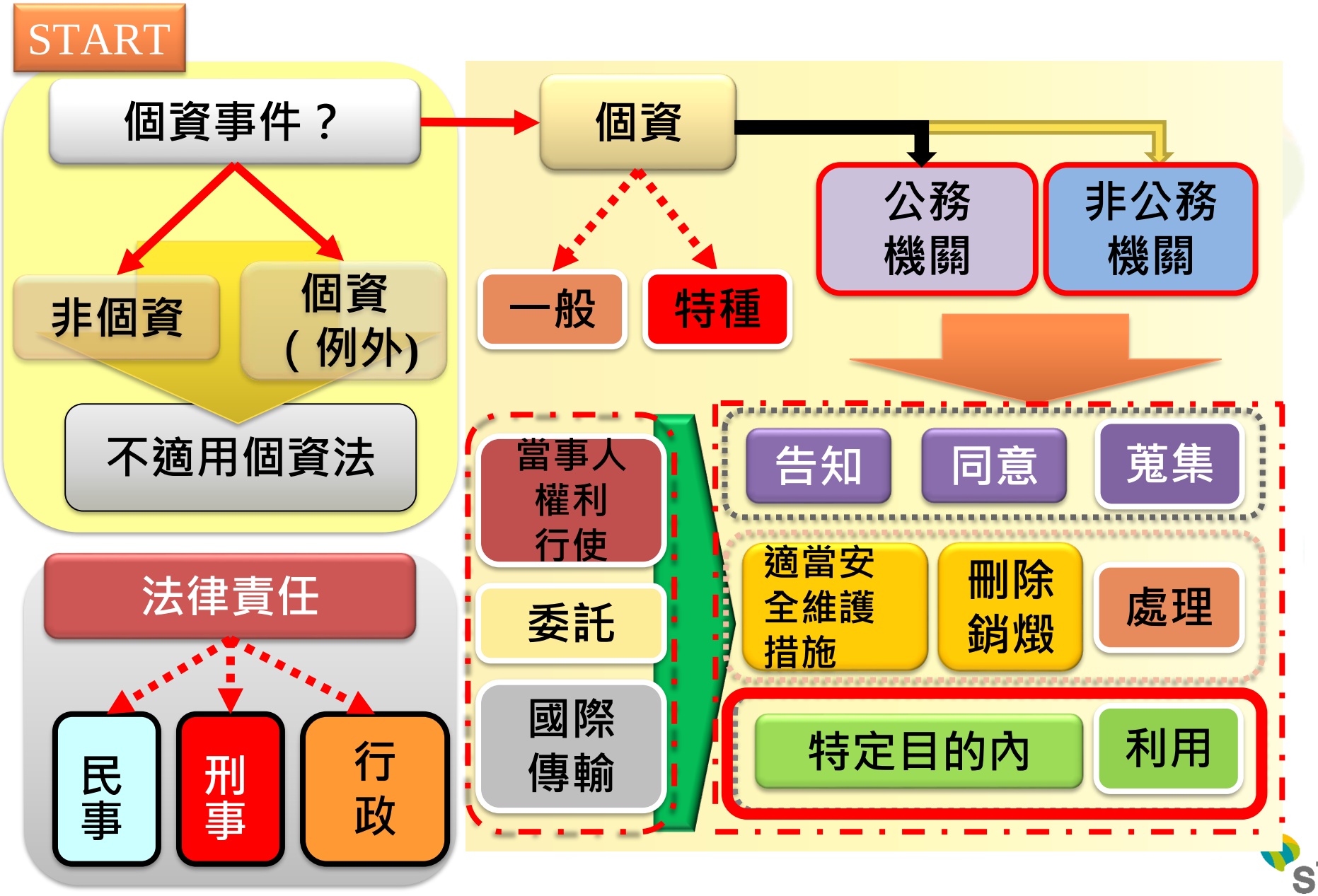
2023 © 資訊工業策進會 Institute for Information Industry

觀光產業個人資料檔案安全維護
自主檢查表（自評表）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
7	業務終止之個資管理	• 訂有業務終止之個資處置措施個人資料顯示之隱碼機制 • 留存相關紀錄保存至少五年以上	是□ 否□	佐證資料如： • 提供資料庫的結構和設計、針對個人資料的去識別化措施或資料加密截圖 • 紙本部分：存取及利用紀錄調閱紀錄、軌跡資料、銷毀紀錄；或是相關日誌(LOG)留存

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

利用之法定要件

個資法§20

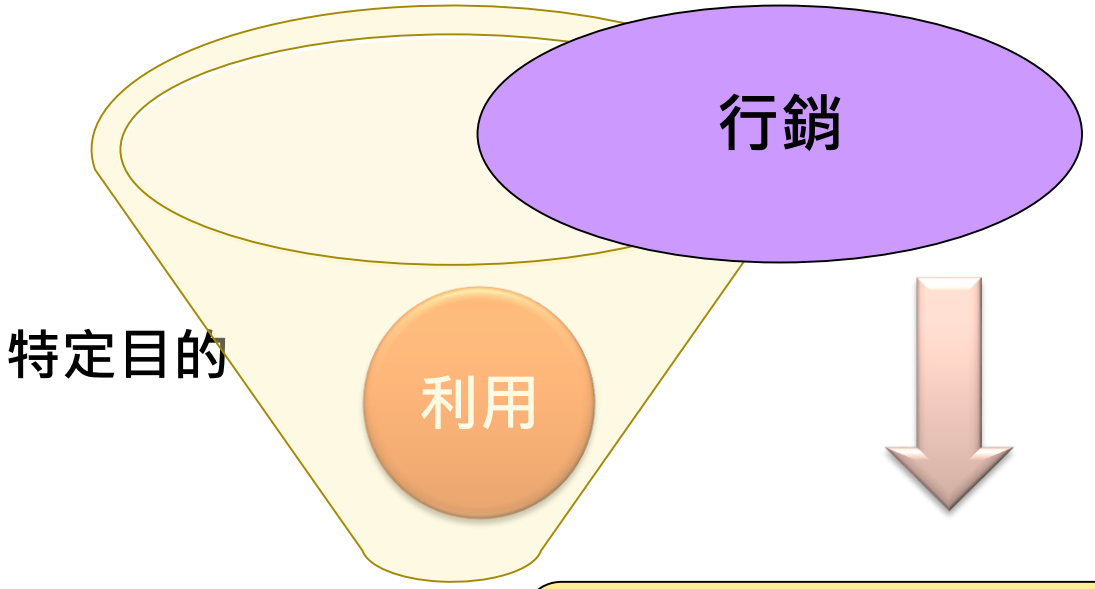
- **非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：**
  - 法律明文規定。
  - 為增進公共利益所必要。
  - 為免除當事人之生命、身體、自由或財產上之危險。
  - 為防止他人權益之重大危害。
  - 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
  - 經當事人同意。
  - 有利於當事人權益。
- **非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。**
- **非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。**

辦法§10

非公務機關所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。

2023 © 資訊工業策進會 Institute for Information Industry

利用（二）行銷（非公務機關）



- 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**。

2023 © 資訊工業策進會 Institute for Information Industry

國發會-拒絕行銷指引（1/3）

- **事前**

1. 非公務機關利用合法蒐集之個人資料對當事人進行商業行銷時，於首次及後續行銷時須主動表明其名稱。
2. 非公務機關於首次進行商業行銷時，應提供當事人免費、快速、容易表達之簡便方式以拒絕接受上開行銷，例如:免付費電話或簡訊、電子郵件地址、企業網站客戶服務網址、於應用程式(APP)內取消行銷資訊等。
3. 非公務機關首次利用合法蒐集之個人資料，對當事人依本法第二十條第三項規定進行商業行銷後，於其行使同條第二項規定之拒絕權利前，而非公務機關續行對當事人行銷時，仍宜以清楚易懂、置於醒目位置且容易取得之方式，持續揭示便利當事人拒絕接受商業行銷相關方式之資訊(例如:於企業網站公佈)。

2023 © 資訊工業策進會 Institute for Information Industry

國發會-拒絕行銷指引（2/3）

- 事中

1. 當事人對非公務機關利用其個人資料為商業行銷時，有權不附理由，隨時、任意地表示拒絕，且不以該機關為首次商業行銷時為限。
2. 非公務機關應尊重當事人拒絕商業行銷之意思，按其拒絕行銷之意願及範圍停止行銷；其後非經當事人再為通知或更改其意願前，不得再為行銷。
3. 本法第二十條第三項雖規範非公務機關須提供當事人拒絕接受行銷之方式，惟未限制當事人僅得以上開方式行使拒絕權，非公務機關不得以當事人未依所提供之方式為由，拒絕停止對當事人商業行銷。

2023 © 資訊工業策進會 Institute for Information Industry

國發會-拒絕行銷指引（3/3）

- **事後**

1. 非公務機關應記錄、更新及彙整當事人拒絕商業行銷之意思表示，並回覆當事人已收到其拒絕行銷之通知；另依本法第二十七條第一項及同法施行細則第十二條規定，採行適當之安全措施。
2. 非公務機關應儘速周知所屬人員或受委託者，依本法第二十條第二項意旨，停止對該當事人進行商業行銷。

- **其他注意事項**

如非公務機關委託他人向當事人進行商業行銷，應採取適當之監 督措施（例如於雙方契約中納入對應約款），確保受託者履行該 非公務機關所適用之本法第二十條第二項及第三項規定(另參照 本法施行細則第七條及第八條)，以處理當事人拒絕商業行銷之 相關事宜。

2023 © 資訊工業策進會 Institute for Information Industry

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**。

2023 © 資訊工業策進會 Institute for Information Industry

綑綁式行銷?

為何老是接到行銷電話？立委揭產險公司「綑綁式同意」放送個資

潘維庭 + 追蹤 2021-01-20 12:36 3151 人氣 贊助本文 簡 分享 4 LINE



2023 © 資訊工業策進會 Institute for Information Industry

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載本人資料轉送產、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。

2023 © 資訊工業策進會 Institute for Information Industry

問題回顧

- **Q2：住宿業者可否要求登記、影印旅客的身分證資料嗎？**
- A2：可以，依據「觀光旅館業管理規則§19」、「旅館業管理規則§23」以及「民宿管理辦法§28」中，均有規定住宿業者必須登記每日住宿旅客資料，且保存期間為六個月之規定。
- 為確保交易及旅客住宿安全，因此住宿業者確實可以要求登記、影印身分證資料，然而依照個人資料保護法§19 I法律要求的規定，但業者須基於**確保交易及旅客住宿安全的特定目的**

法規	內容
觀光旅館業管理規則§19	• **觀光旅館業**應登記每日住宿旅客資料；**其保存期間為半年**。 • 前項旅客登記資料之蒐集、處理及利用，並應符合個人資料保護法相關規定。
旅館業管理規則§23	• **旅館業**應將每日住宿旅客資料登記；**其保存期間為半**年。 • 前項旅客登記資料之蒐集、處理及利用，並應符合個人資料保護法相關規定。
民宿管理辦法§28	• **民宿經營者**應將每日住宿旅客資料登記；**其保存期間為六個月**。 • 前項旅客登記資料之蒐集、處理及利用，並應符合個人資料保護法相關規定。

2023 © 資訊工業策進會 Institute for Information Industry

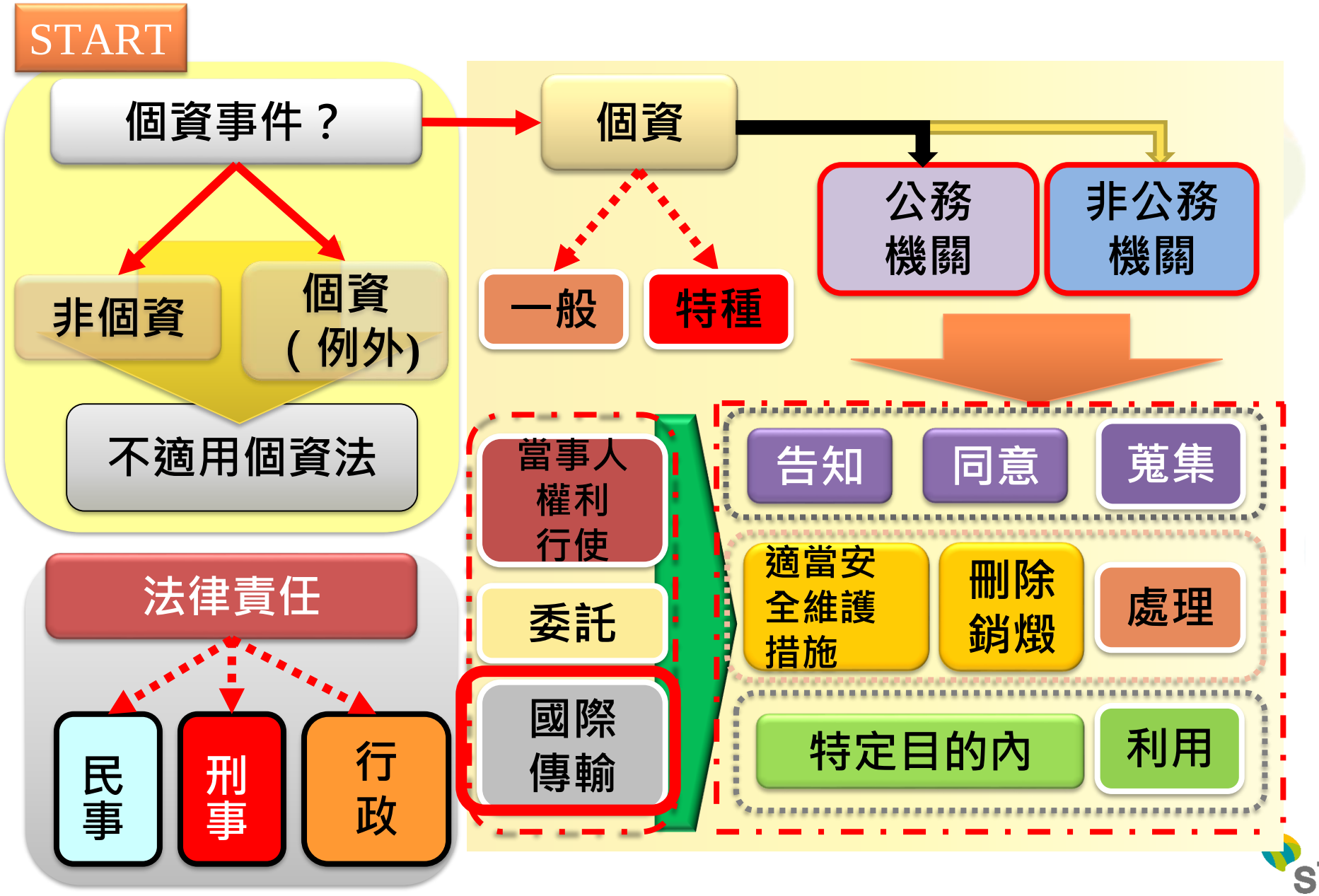
問題回顧

- **Q3：住宿業者可否依民眾提供的基本資料，發送廣告信嗎？**
- A3： 利用民眾未辦理住宿而留下的基本資料，基於個資法19條規定，只能在此特定目的外利用；若在蒐集資料時，如有另外詢問是否勾選寄送電子報，而獲得同意，始可發送廣告信，並應注意給予簡單取消訂閱的方式。

- **Q4：住宿業者可否依照民眾訂房資料，分析旅客的住宿喜好嗎？**
- A4：承上題，除了要符合個資法20條，關於利用的規定外，尚須明確單獨取得當事人的同意，始可進行特定目的外的利用。

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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

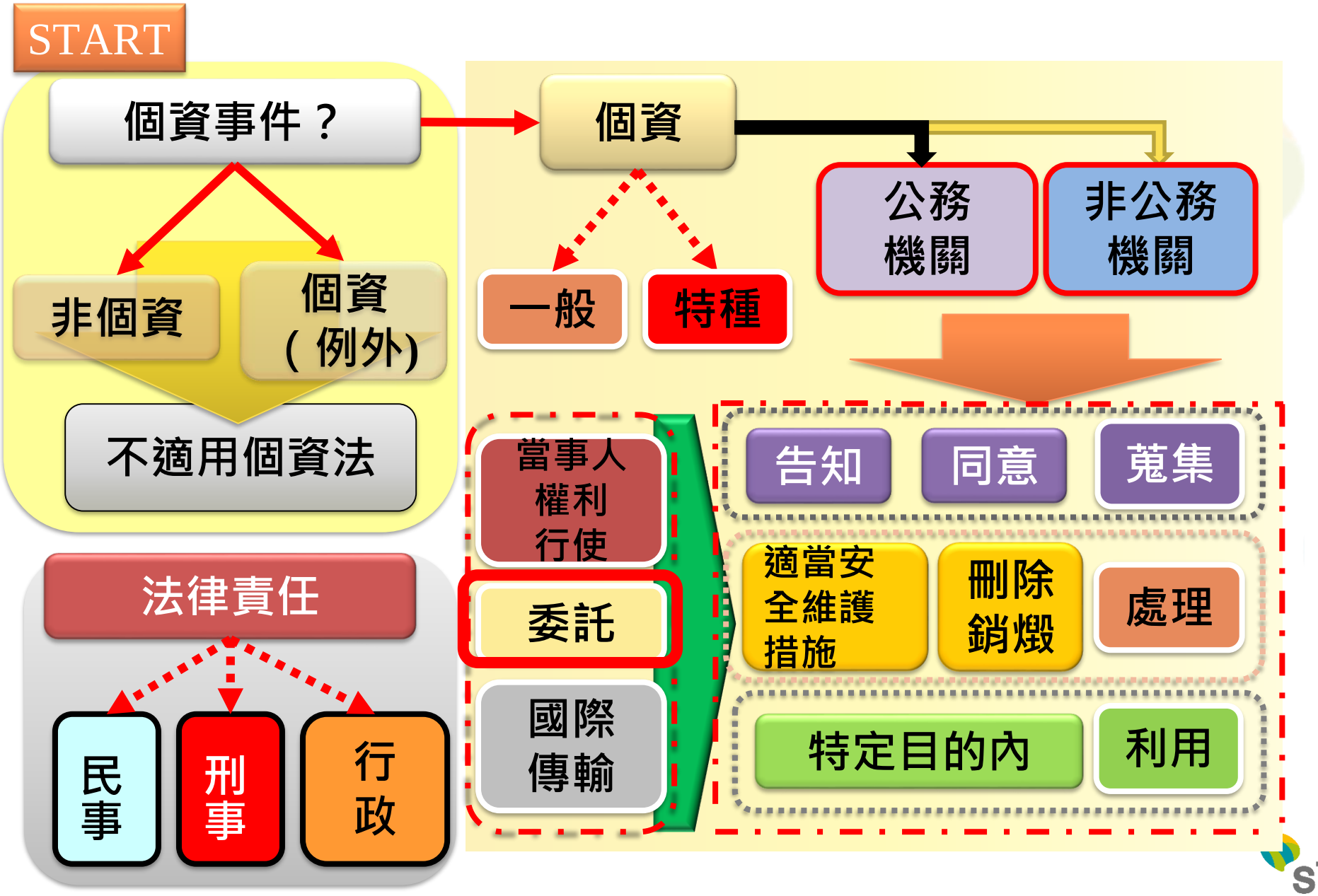
2023 © 資訊工業策進會 Institute for Information Industry

國際傳輸 - 對旅宿/住宿業規定

- **辦法§12**
- 中央主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。
- 非公務機關將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：
  - 預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。
  - 當事人行使本法第三條所定權利之相關事項。

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

委託 - 對旅宿/住宿業規定

- **辦法§21**
- 非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定為適當監督。
- 非公務機關為執行前項監督，應與受託者明確約定相關監督事項及方式

2023 © 資訊工業策進會 Institute for Information Industry

個資行為委託注意事項

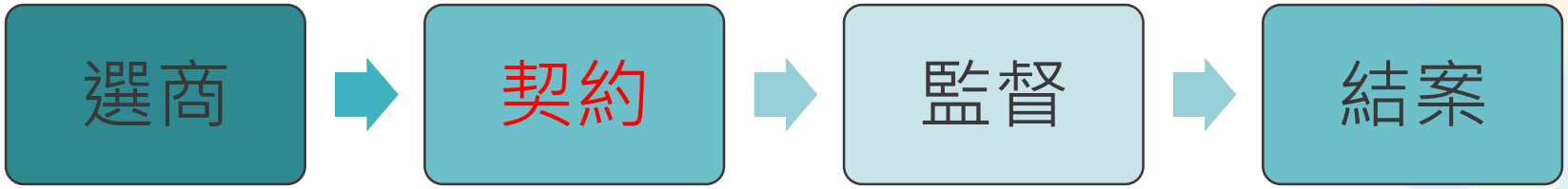
選商 → 契約 → 監督 → 結案

- **Step1：確認委託行為性質**
  - 所委託工作是否涉及個資蒐集、處理、利用行為？（屬於本身業務？）
- **Step2：選任委外廠商（受託者）之標準**
  - 選任受託者辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證（T8.9.）。
  - 可在**選商標準**（招標文件）列明：廠商個資管理措施、個資認證、近年有無發生個資事故，並要求廠商聲明



2023 © 資訊工業策進會 Institute for Information Industry

個資行為委託注意事項



- 常見問題：受託者表示合作契約已有「保密條款」、「保密聲明」即可。此論述是否正確？
- 說明
  - 恐無法符合個資法「適當監督」要求（施§8I、II）。→不僅限於保密
  - 契約效果：接受監督（避免反以個資法為藉口不配合）、違約責任。
- 常見問題：可否直接載明應遵循機關「個資保護管理制度」、政策即可？
- 說明
  - 建議機關至少應將「個資保護管理制度」、「個資管理程序書」作為契約附件，以發生契約拘束力。

2023 © 資訊工業策進會 Institute for Information Industry

受託者之選擇-自評表

管理重點

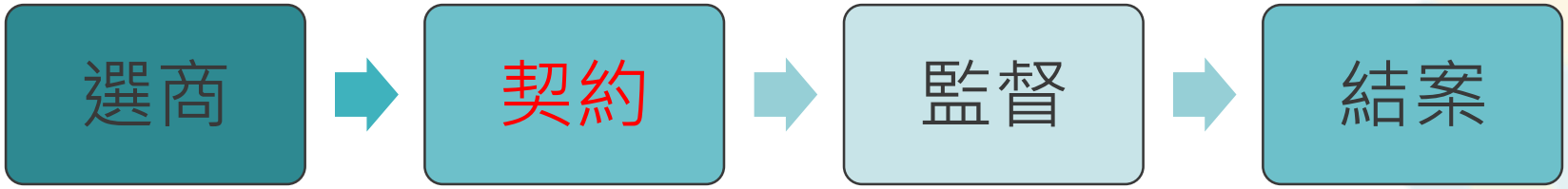
判斷個資有無委外處理等 → 選擇委外監督方式，簽約或實地查核 → 後續處置及內部管理機制

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	

2023 © 資訊工業策進會 Institute for Information Industry

個資行為委託注意事項

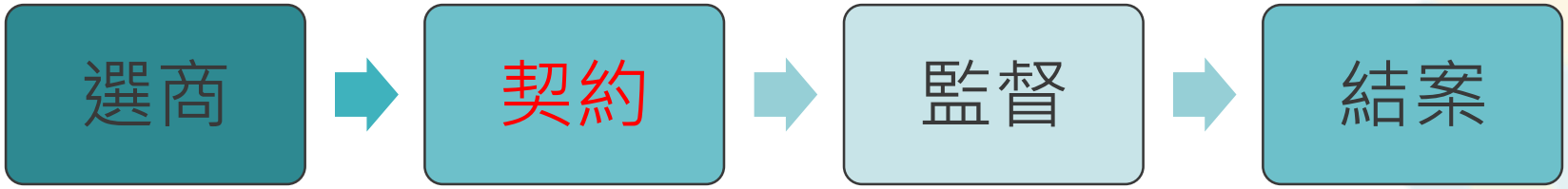


- **建議明訂於契約中之項目：**

	事項	遵守
1	委託人及受託人之權利義務。	
2	委託蒐集、處理或利用個資之範圍、類別、特定目的及其期間。	
3	受託人對個人資料之安全管理措施。	
4	發生事故時向委託人即時報告及採行之補救措施等事項。	
5	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。	
6	Plus：向委託人報告關於個人資料處理狀況之內容及報告週期。	
7	如有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。	
8	如有保留指示，委託人對受託人保留指示之事項。	

2023 © 資訊工業策進會 Institute for Information Industry

個資行為委託注意事項



- **複委託危機**
  - **複委託之禁止？監督？**
  - **民法§537：受任人應自己處理委任事務。但經委任人之同意或另有習慣或有不得已之事由者，得使第三人代為處理。**
  - **日本尼崎市政府將疫情補助發放工作委託B公司執行，B公司再將業務外包給A公司，A公司又外包給C公司。C公司員工發生個資外洩。**
  - **如果在台灣，從個資法角度誰要相關負責？**
    - 有無事前的契約監督約定及監督執行？
    - **問題**：委託人可否直接對於**複委託之受託人**進行查核？

2023 © 資訊工業策進會 Institute for Information Industry

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。

就在本月21日，該外包商派出一名40多歲職員處理一筆資料，該名職員手上握有存有46萬人個資的USB。不過報導指出，按照處理流程，職員在處理完資料後，就要把USB內的檔案消除，但當時該名職員並沒有完成消除檔案的作業。



2023 © 資訊工業策進會 Institute for Information Industry

複委託的風險



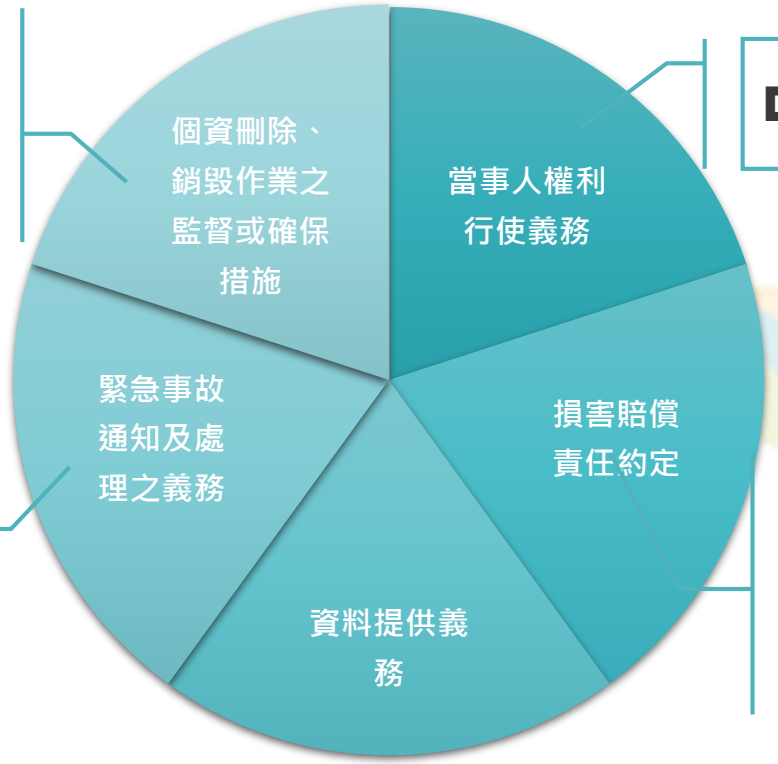
Amagasaki2022

2023 © 資訊工業策進會 Institute for Information Industry

個資行為委託注意事項

選商 → 契約 → 監督 → 結案

- 必要時得實地查訪之配合義務
- 未返還、刪除，或留存備份時之處罰方式



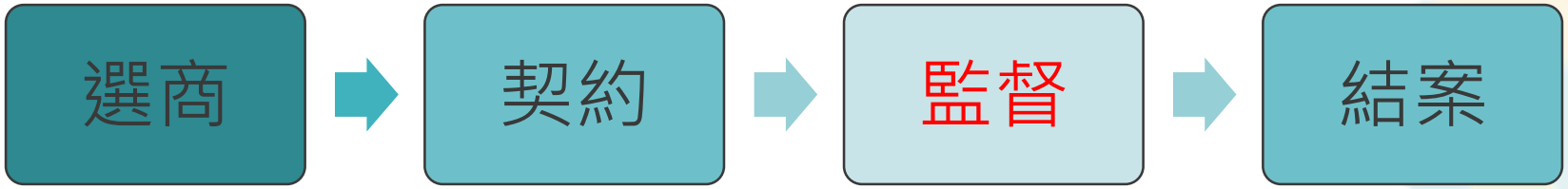
- 供備查 / 確認

- 通知並採取因應措施
- 經同意之補救措施

- 補正
- 賠償範圍
- 違約金 / 懲罰性違約金
- 協助答辯義務

2023 © 資訊工業策進會 Institute for Information Industry

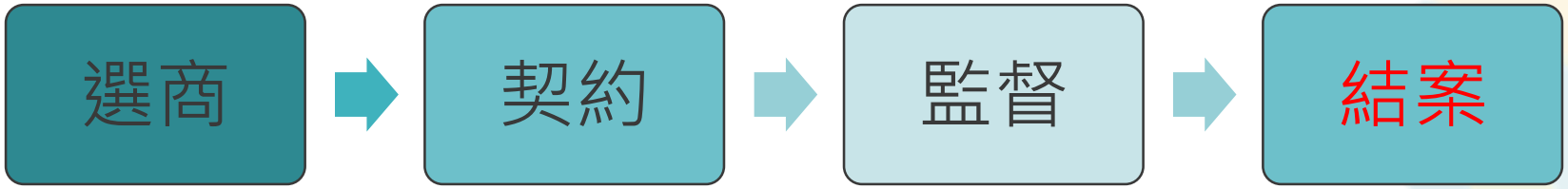
個資行為委託注意事項



- 規定：委託機關應定期確認（與審查）受託者執行之狀況，並將確認結果記錄之。
- 作法：
  - 受託者提交「個資管理自評表」
  - 受託者填寫及委託機關提供的自評表
  - 委託機關實際稽核受託者（best practice）
- 常見問題：受託人不接受監督、查核之處理？（例如，Google, Meta等服務提供者，以制式契約條件合作，事前無法補入監督條款，事中亦不提供查核）

2023 © 資訊工業策進會 Institute for Information Industry

個資行為委託注意事項



- 規定
  - 民法：委託（民§540：「受任人應將委任事務進行之狀況，報告委任人，委任關係終止時，應明確報告其顛末。」）
  - 個資法：委託關係終止或解除時，個資載體之返還，及儲存於受託人持有個人資料之刪除。
- 作法
  - 受託者提交出具已執行之紀錄或切結聲明
  - 個資事故發生之協助處理義務，不因合作結束後而解除
  - 若能搭配結案作業及尾款交付更佳

2023 © 資訊工業策進會 Institute for Information Industry

案例探討

● 案例：111年度沙簡字第3號

事實概要

- 原告等6人受雇於被告星月公司，被告將其相關會計事項，委由被告耘家公司「耘家會計師雲端管理系統」，作為線上檢視財務、稅務文件。
- 原告於網路瀏覽，赫然發現於搜尋引擎輸入姓名、扣憑關鍵字搜尋，竟出現載有原告姓名、國民身分證統一編號、地址及薪資所得等個人資料之各類所得扣繳暨免扣繳憑單。

判決要旨

- **原告依個資法第29條、民法第185條、第195條第1項規定，請求被告負連帶侵權責任，於原告請求，各於1萬元、1萬2千元、1萬2千元、1萬2千元、1萬5千元、1萬5千元。**
- 被告耘家公司受被告星月公司委託處理其財務、稅務相關會計事項，其蒐集、處理、利用原告之個人資料，自應遵守個資法第20、27條之規範，於合法範圍內為之、並有採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩露之義務。
- 被告耘家公司違反上開義務，亦無法定事由存在、違反個資法上開規範，致原告個人資料外洩公開，而各該資料除含個人身分相關辨識資料外，亦攸關個人財產狀況。
- **被告耘家公司應負個資法第29條損害賠償責任。**
- 被告星月公司，因委託被告耘家公司處理資料，依**個資法施行細則第8條規定，對受託者實有監督義務**，惟**被告未善盡對被告耘家公司之監督**，**致原告個人資料外洩**，亦侵害原告之隱私權，應與被告耘家公司共同就個資法第29條、民法第185條、第195條第1項規定，負連帶侵權責任。

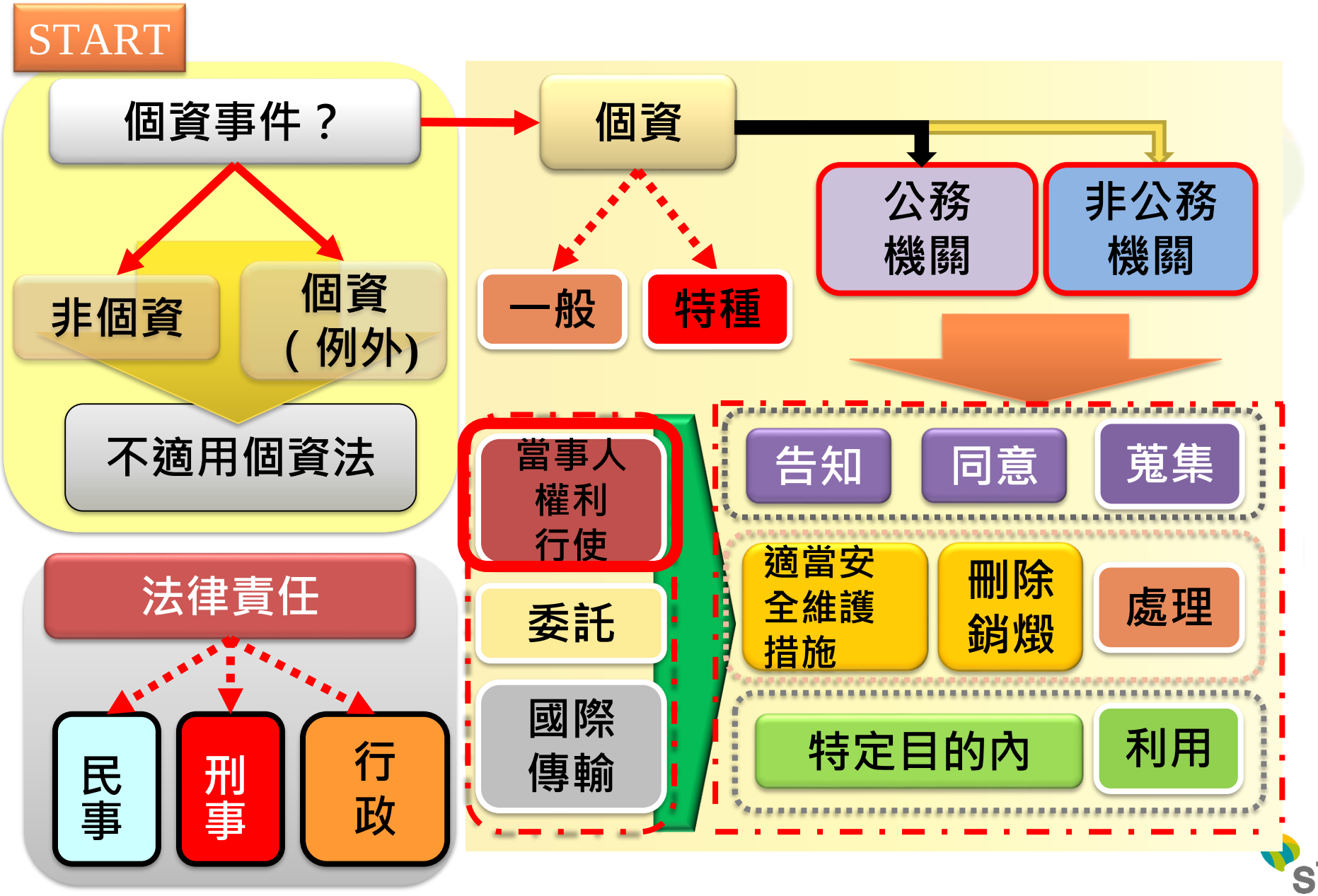
2023 © 資訊工業策進會 Institute for Information Industry

問題回顧

- **Q5：若旅客在訂房網下訂不久後，接到詐騙電話而有財損，經查是因訂房網個資外洩所致，而非住宿業者自身網站出現問題，可否因此不用負責?**
- A5： 不行！委託其他公司蒐集、處理、利用資料，依個資法施行細則第8條規定，應對受託者實有監督義務，若未善盡監督，致個人資料外洩，亦應與受託公司共同負責。

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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	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
請求製給複製本		
請求補充或更正	無爭議	30+30
請求停止蒐集、處理或利用	有爭議	
請求刪除		

- 正確性問題 *
- 特定目的消失/期限屆滿 *
- 違法蒐集處理利用

* 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

2023 © 資訊工業策進會 Institute for Information Industry

當事人權力行使 - 對旅宿/住宿業規定

- **辦法§13**
- 非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

1. 提供聯絡窗口及聯絡方式。
2. 確認為個人資料當事人本人，或經其委託者。
3. 認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。
4. 有收取必要成本費用者，應告知當事人收費基準。
5. 遵守本法第十三條有關處理期限之規定。

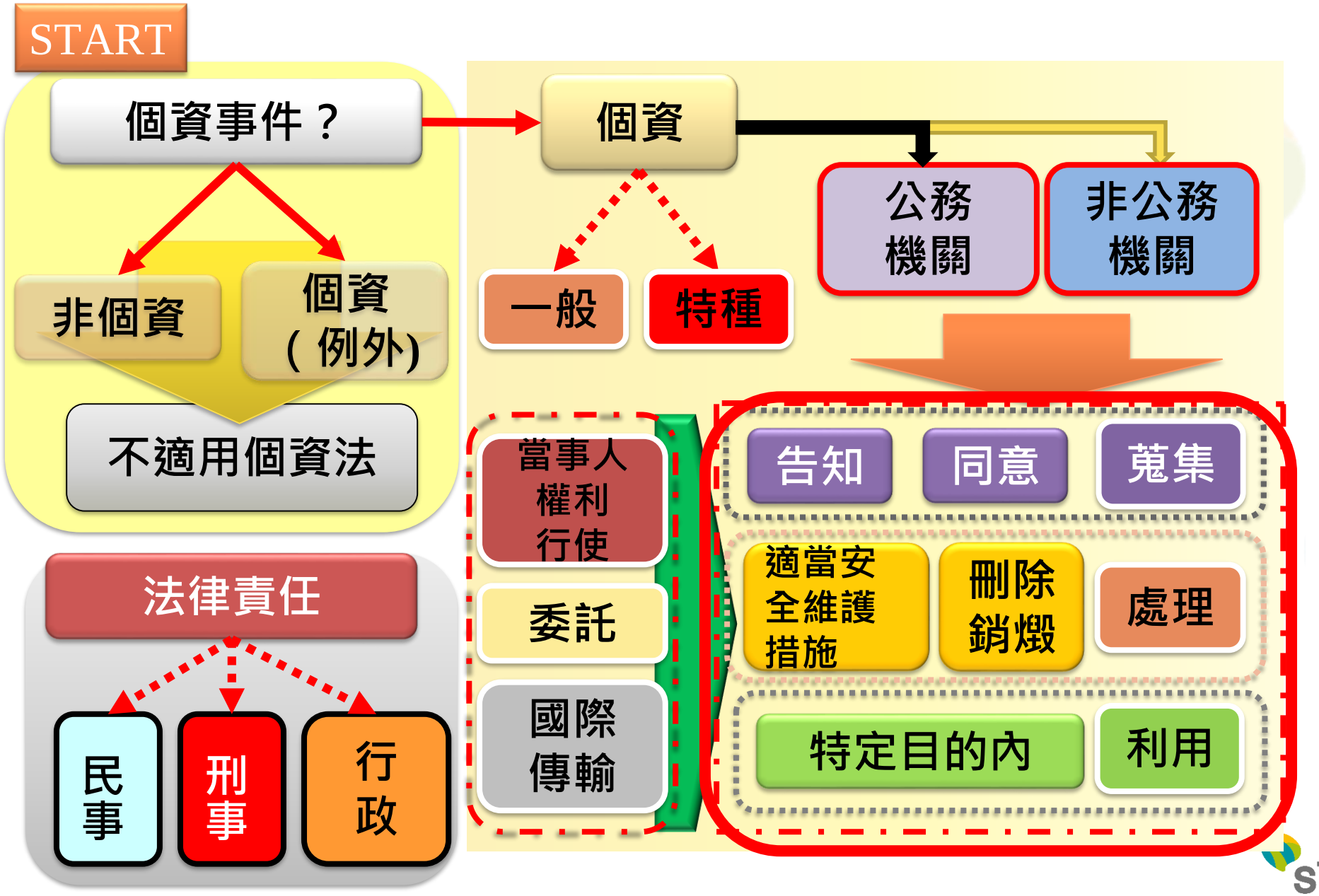
2023 © 資訊工業策進會 Institute for Information Industry

案例思考-當事人權利行使

- 阿竹加入購物公司S會員，並有定期消費的習慣，試問阿竹跟S公司下列行為是否合宜？
  - 阿竹想要修改其會員資料，透過網站修改資料。
  - 阿竹想要刪除其個人資料，S公司要求其必須從台北親自至桃園S公司臨櫃辦理。
  - 阿竹想要申請某一筆購買證明的複本，S公司表示影印一份需支付500元的費用。
  - 對於阿竹刪除個資的聲請，S公司表示為了執行業務之必要，可能需等15年後才可刪除。

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

蒐集處理利用 - 對旅宿/住宿業規定

- **辦法§10**
- 非公務機關所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。

- **辦法§11**
- 非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理

2023 © 資訊工業策進會 Institute for Information Industry

觀光產業個人資料檔案安全維護
自主檢查表（自評表1）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
4	個人資料盤點、管理與紀錄	定期盤點所保有個人資料並確認應遵守之法令	是□ 否□	佐證資料如：資料盤點表、資料流程說明（圖）或其他內部制度文件等
		風險分析及管控措施	是□ 否□	風險評估表、風險識別與風險預估
		依資料屬性訂定管理程序	是□ 否□	適當之管控及因應措施、區分風險分級
		向當事人蒐集個資，或於利用非由當事人提供之個資前盡告知義務	是□ 否□	資料盤點表其他內部制度文件等
		檢視蒐集、處理個人資料是否符合個人資料保護法第十九條規定之目的及要件	是□ 否□	資料盤點表、資料流程說明（圖）或其他內部制度文件等
		委託他人進行資料蒐集、處理或利用，進行適當監督	是□ 否□	契約、查核記錄或其他內部制度文件等

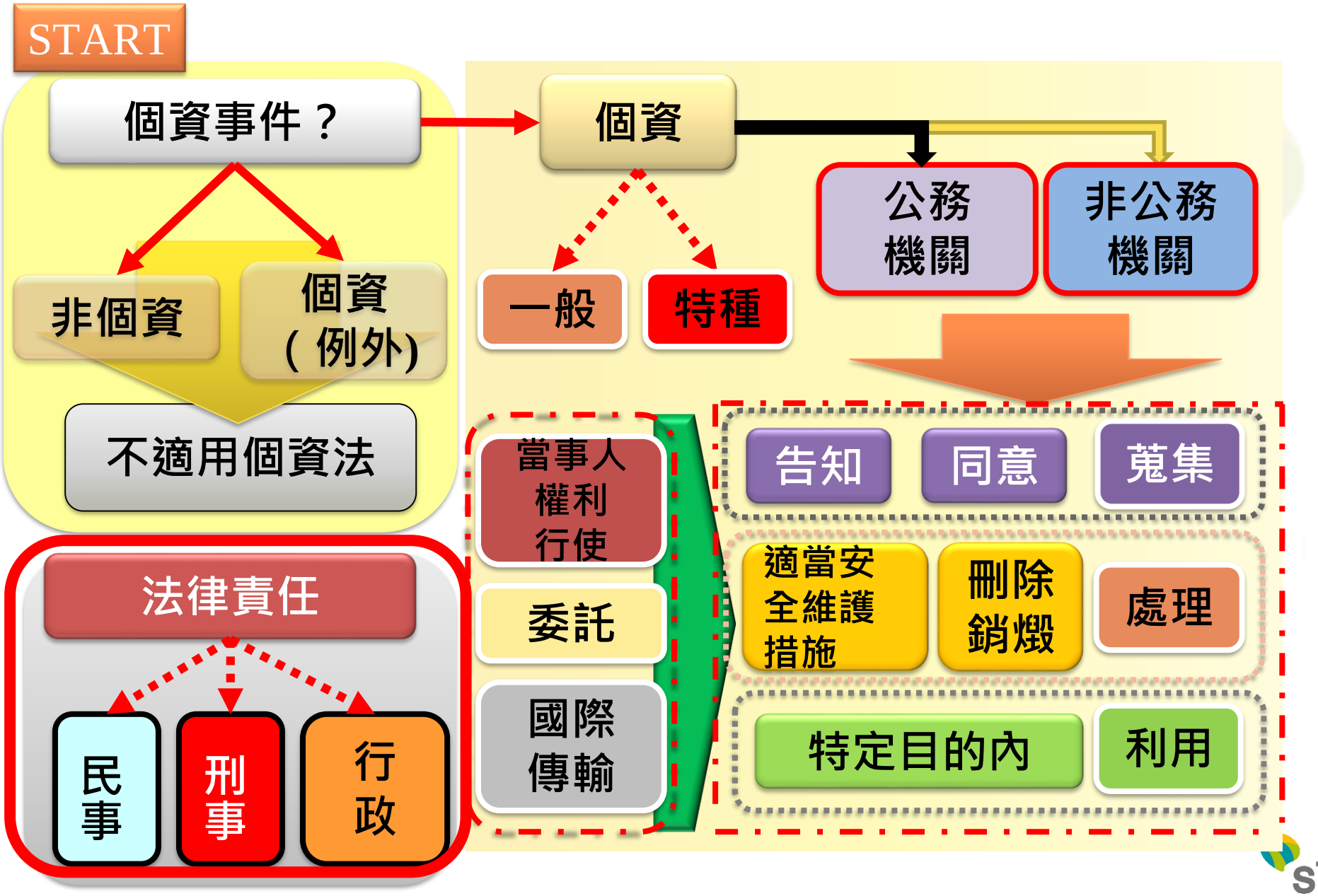
2023 © 資訊工業策進會 Institute for Information Industry

觀光產業個人資料檔案安全維護
自主檢查表（自評表2）

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
4	個人資料盤點、管理與紀錄	首次利用個資行銷之當事人確認作業	是□ 否□	佐證資料如：資料盤點表、資料流程說明（圖）或其他關於行銷內部制度文件等
		確認與維護保有個資之正確性	是□ 否□	風險評估表、風險識別與風險預估
		針對所屬人員設定不同管理權限，並要求負保密義務	是□ 否□	權責區分表、保密協議書
		對存有個資之系統設備、媒介物等採取安全管理措施	是□ 否□	內部評估或稽核記錄、內部制度文件等，應能呈現採取之安全管理措施項目等資訊
		存有個資之系統設備、媒介物報廢或轉作他用時，採取適當防護措施	是□ 否□	執行記錄、內部評估或稽核記錄、內部制度文件等，應能呈現有效處理之結果
		留存所有個資使用紀錄、機關設備軌跡紀錄、相關證據紀錄至少五年以上	是□ 否□	紙本部分：存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄； 資訊系統使用紀錄及軌跡資料紀錄、針對儲存個人資料資料庫的存取紀錄

2023 © 資訊工業策進會 Institute for Information Industry

個資法規範架構暨個資全生命週期



2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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。



2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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	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	受同一額度罰鍰之處罰 ->**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。

2023 © 資訊工業策進會 Institute for Information Industry

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用其個資，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）

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

02 個資保護實務教戰指引

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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

辦法§7：非公務機關應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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 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

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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

辦法§8：非公務機關應依前條界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管控機制。

2023 © 資訊工業策進會 Institute for Information Industry

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。

未來的
過去的事情已經發生，非不確定

不確定的
有哪些事情是100%確定?

偏離預期的
出乎預期?

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.

資料來源：The Economic Times

2023 © 資訊工業策進會 Institute for Information Industry

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

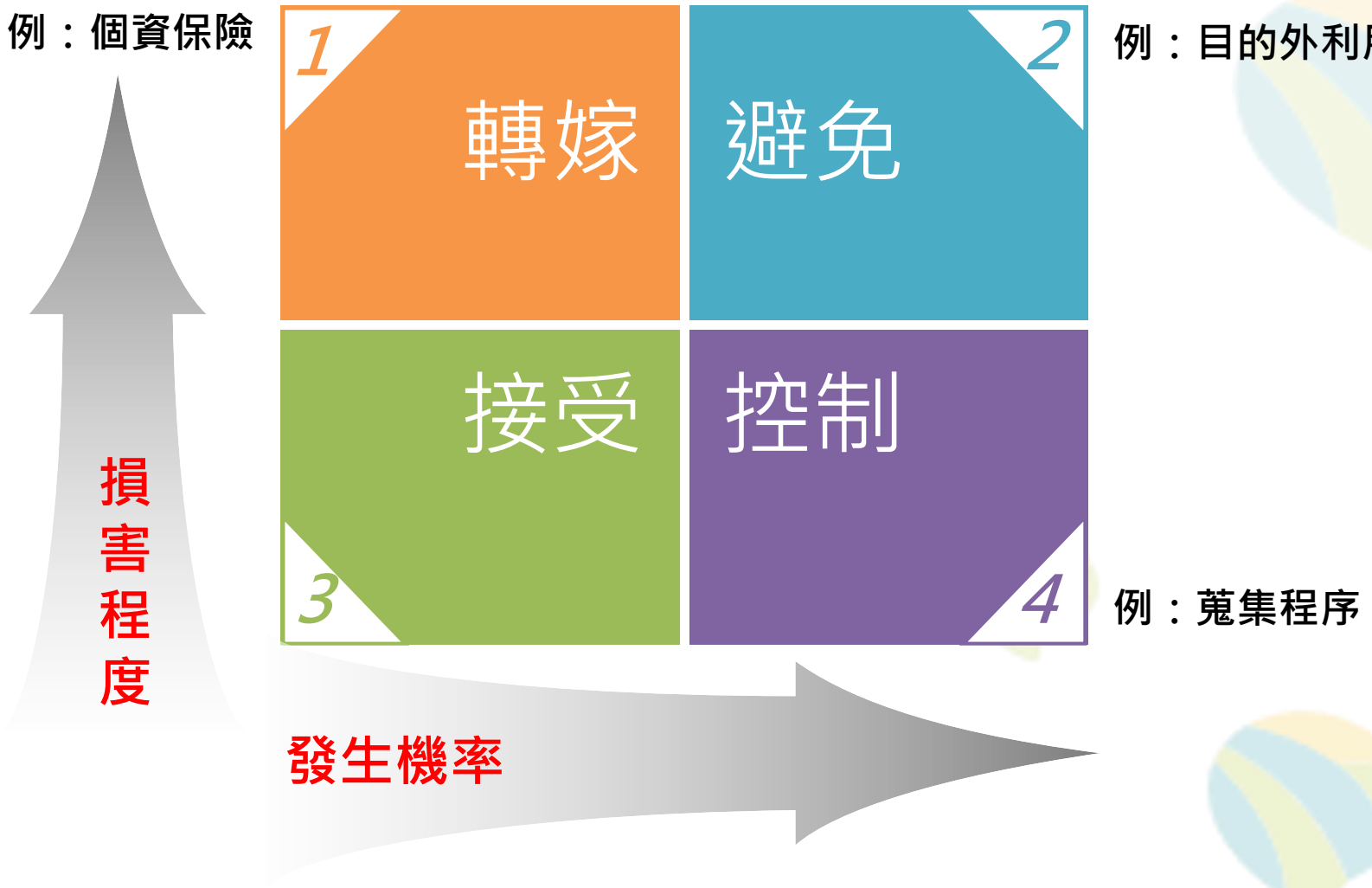
企業實作參考

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）

2023 © 資訊工業策進會 Institute for Information Industry

風險管控措施



2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

風險評鑑表範例(1/5)

TPIPAS教學用

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。	衝擊值係以衝擊構面之評分加總		
		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。			
		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

經濟部個人資料保護作業手冊

2023 © 資訊工業策進會 Institute for Information Industry

風險評鑑表範例(5/5)

TPIPAS教學用

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。 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	I×P		
○○○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

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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

00:00

2022/01/27 18:21:27

中央社 記者謝方婞台北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。

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

辦法§17：

非公務機關應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

紀錄管理重點

結合內部管理

因應法規要求

協助訴訟舉證

管理重點

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。

2023 © 資訊工業策進會 Institute for Information Industry

紀錄留存 - 對旅宿/住宿業規定

- **辦法§19**
- 非公務機關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，應記錄其個人資料使用情況，留存軌跡資料或相關證據。
- 非公務機關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，應留存下列紀錄：

1. 刪除、停止處理或利用之方法、時間或地點。
2. 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。

- 前二項之軌跡資料、相關證據及紀錄，**應至少留存五年**。但法令另有規定或契約另有約定者，不在此限。

2023 © 資訊工業策進會 Institute for Information Industry

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

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

2023 © 資訊工業策進會 Institute for Information Industry

個資事故之通知

- **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。

2023 © 資訊工業策進會 Institute for Information Industry

事故通報 - 對旅宿/住宿業規定

- **辦法§9**
- 非公務機關為因應消費者個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定下列應變、通報及預防機制：

1. 事故發生後應採取之應變措施，包括降低、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。
2. 事故發生後應受通報之對象及其通報方式。
3. 事故發生後研議其矯正預防措施之機制。

- 非公務機關遇有消費者個人資料外洩事故，將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內依附表格式通報其主管機關。如向地方主管機關通報，非公務機關並應副知中央主管機關。
- 無法於時限內通報或無法於當次提供前項所述事項之全部資訊者，應檢附延遲理由或分階段提供。
- 主管機關得知或接獲第二項通報後，得依本法第二十二條至第二十五條規定，為適當之監督管理措施。中央主管機關認有必要時，得督導地方主管機關對於非公務機關之相關機制改善情形。

2023 © 資訊工業策進會 Institute for Information Industry

監督通報紀錄表（電子郵件）

□警政署來函：____年____月___日____字_____號函
□非公務機關自行通報：日期____年____月___日
□其他，請敘明：

首次通報作業(註1)	
非公務機關名稱：_____ 通報機關：_____ 通知： 國家發展委員會 (傳真：02-25066223， Email：notify@ndc.gov.tw) 數位發展部**(重大矚目)** (電話： Email：待國發會確認後另行通知) 副知： □交通部次長室(資安長)FAX：2371-7990 □交通部郵電司　FAX：2381-3928 □交通部路政司　FAX：2389-9887 □交通部航政司　FAX：2381-1550 □交通部管理資訊中心　FAX：2382-0655	通報時間：　年　月　日　時　分 通報人：　　簽名(蓋章) 職稱： 電話： 傳真： Email： 地址：

2023 © 資訊工業策進會 Institute for Information Industry

個人資料侵害事故通報及紀錄表

公司名稱： 姓名：	通報時間：分　　年　　月　　日　　時 通報人：　職稱： 電話：　　簽章 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	

2023 © 資訊工業策進會 Institute for Information Industry

思考-是否符合個資事故通知要求？

和泰集團 | 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。

2023 © 資訊工業策進會 Institute for Information Industry

觀光產業個人資料檔案安全維護自主檢查表

編號	查核重點	查核內容	執行	具體措施(含佐證資料)及補充說明
8	事故通報與應變程序	制訂個資洩漏等事故發生或知悉起72小時內通報流程	是□ 否□	佐證資料如：通報應變程序文字、通報紀錄等
		對個資洩漏等事故採應變措施以控制損害	是□ 否□	說明所採應變措施
		於查明事故後以適當方式通知當事人並告知已採取因應措施	是□ 否□	通知書內容
		研議預防機制	是□ 否□	說明所採預防措施

2023 © 資訊工業策進會 Institute for Information Industry

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

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

內部評量 - 對旅宿/住宿業規定

- **辦法§18**
- 非公務機關為確保本計畫及處理方法之落實，應依其組織規模及特性，衡酌資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員每年至少進行一次本計畫及處理方法執行情形之檢查。
- 前項檢查結果應向代表人提出報告，並留存相關紀錄，其保存期限**至少五年**。
- 非公務機關依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。
- **辦法§20**
- 非公務機關應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規增修等因素，檢討所定本計畫及處理方法，必要時予以修正。

2023 © 資訊工業策進會 Institute for Information Industry

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。

2023 © 資訊工業策進會 Institute for Information Industry

有效性量測

- 課後測驗



2023 © 資訊工業策進會 Institute for Information Industry

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

dp.mark
資料隱私保護標章

2023 © 資訊工業策進會 Institute for Information Industry