

# 輔導人力供應業者 強化個資防護措施研習

李怡親 法律研究員  
資策會科技法律研究所  
2023.09.04



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



# 簡報 大綱

01

## 個資法遵重點提示

何謂個人資料

個人資料保護法重點條文介紹

個人資料生命週期核心義務

當事人權利保護行使因應之道

02

## 個資保護實務教戰指引

行政檢查重點提示

第三方驗證制度介紹



01

# 個資法遵重點提示



# 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         |



# 哪類個資外洩狀況最嚴重？

- 依據Gogolook 2022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）。

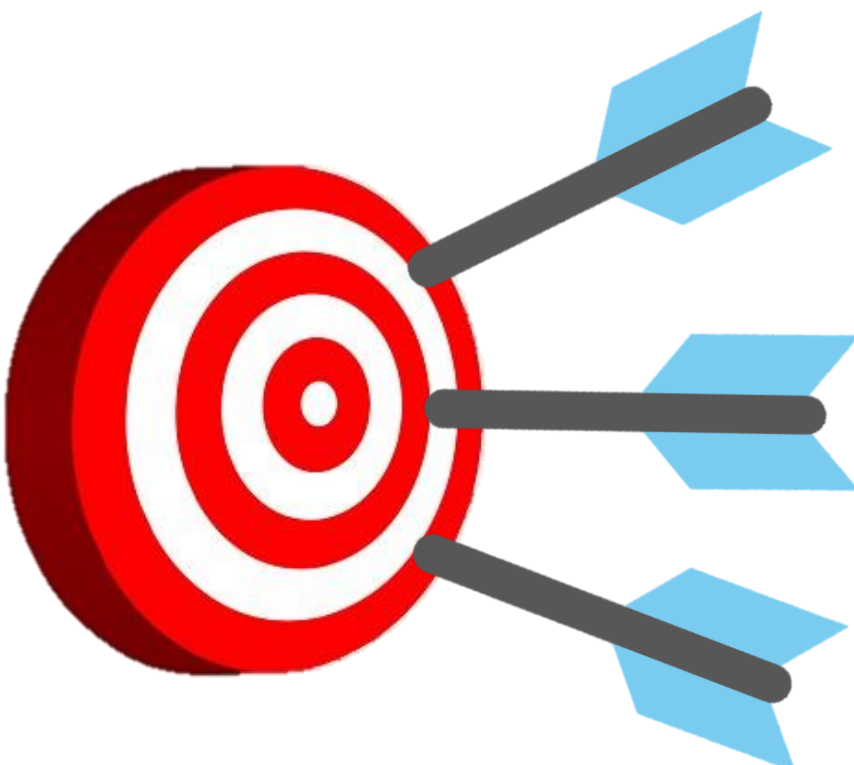


# 隱私權 ( J603 )

- 維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為**保障個人生活私密領域免於他人侵擾及個人資料之自主控制**，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障 (本院釋字第五八五號解釋參照)。
- 資訊隱私權的權利內涵，包含保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人**揭露的決定權**；並保障人民對其個人資料之使用有**知悉與控制權**及**資料記載錯誤**之更正權。



# 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員會
- 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



# PDCA方法論





# 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





# 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  | 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、電視、訂戶數達三千戶以上之直播衛星廣播電視服務事業、經營國內新聞台或購物頻道事業、電信消費爭議處理機構及其他公告通傳事業等八類 | 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   |                                                                                                                    | 56 |



# 訂定安全維護計畫

- 適用對象（本辦法§2）

- 本辦法適用對象，為行業統計分類規定之人力供應業。

- 人力供應業（本辦法§3）

- 人力供應業者為落實個人資料檔案之安全維護及管理，應訂定個人資料檔案安全維護計畫（以下簡稱本計畫）。
- 本計畫內容，應包括下列事項：
  - 個人資料保護規劃
  - 個人資料管理程序
  - 個人資料管理措施
  - 業務終止後個人資料處理方法
  - 紀錄機制
- 人力供應業者訂定前項計畫時，其內容應具體明確，並定期檢視及配合相關法令修正本計畫。



# 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



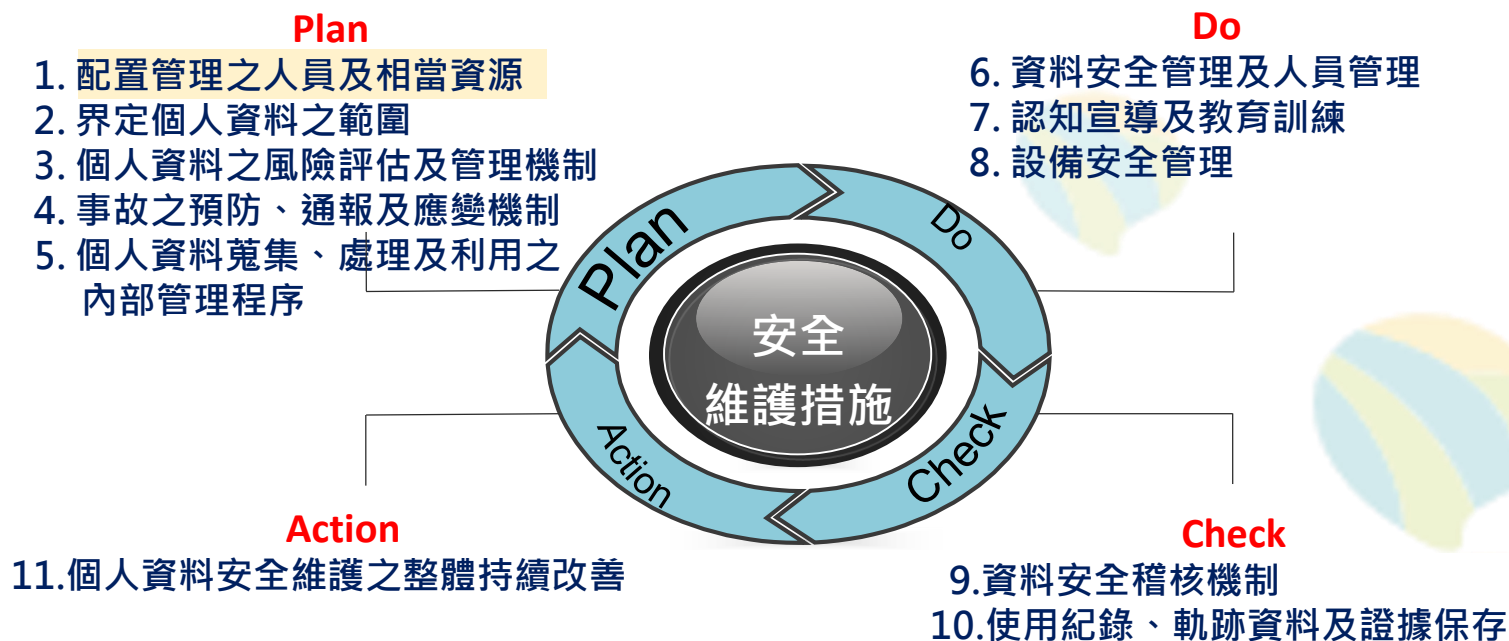
stli



# 訂定安全維護計畫

## • 配置資源 ( 本辦法§4 )

- 人力供應業者就個人資料檔案安全維護管理，應指定專人或建立專責組織負責，並配置相當資源。
- 前項專人或專責組織之任務如下：
  - 規劃、訂定、修正及執行本計畫
  - 訂定個人資料保護管理原則，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項公告，使其所屬人員瞭解



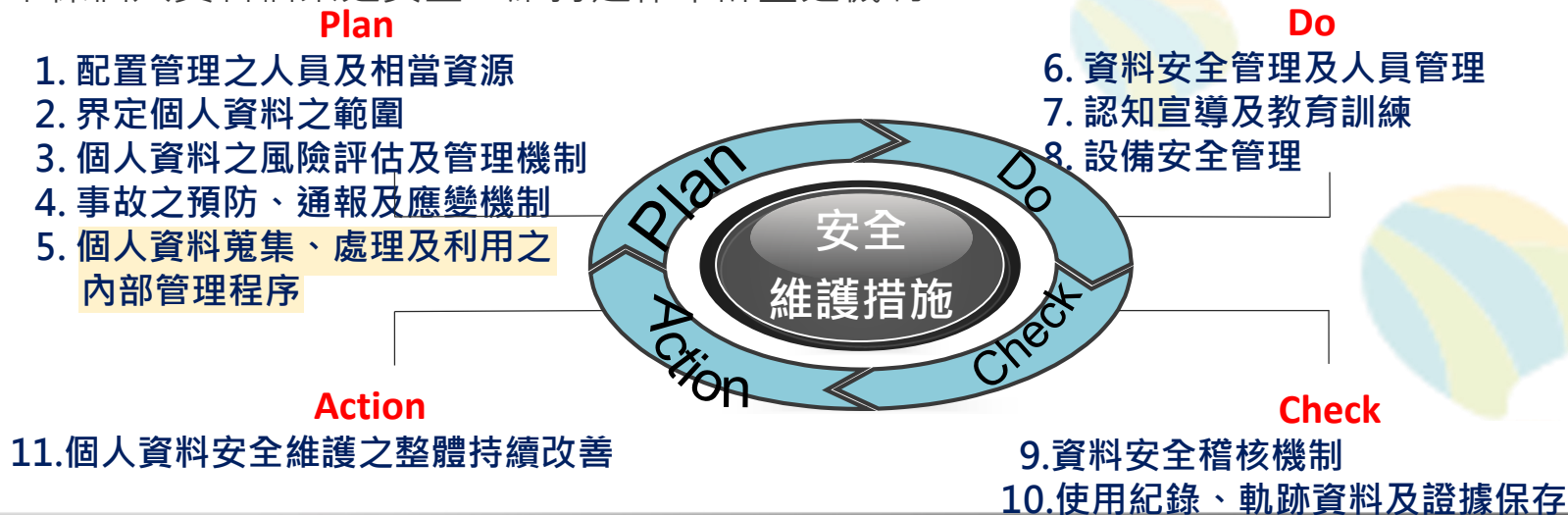


# 訂定安全維護計畫

## 訂定個人資料保護管理原則（本辦法§5）

— 人力供應業者訂定前條第二項第二款之個人資料保護管理原則，應包括下列事項：

- 個人資料保護相關法令規定之遵守
- 於特定目的範圍內，蒐集、處理及利用個人資料之合理安全方法
- 保護所蒐集、處理、利用之個人資料檔案之合理安全水準技術
- 供當事人行使個人資料之相關權利、提出相關申訴及諮詢之聯絡窗口
- 處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故之緊急應變程序
- 委託蒐集、處理及利用個人資料者，監督受託者之機制
- 確保個人資料檔案之安全，維持運作本計畫之機制

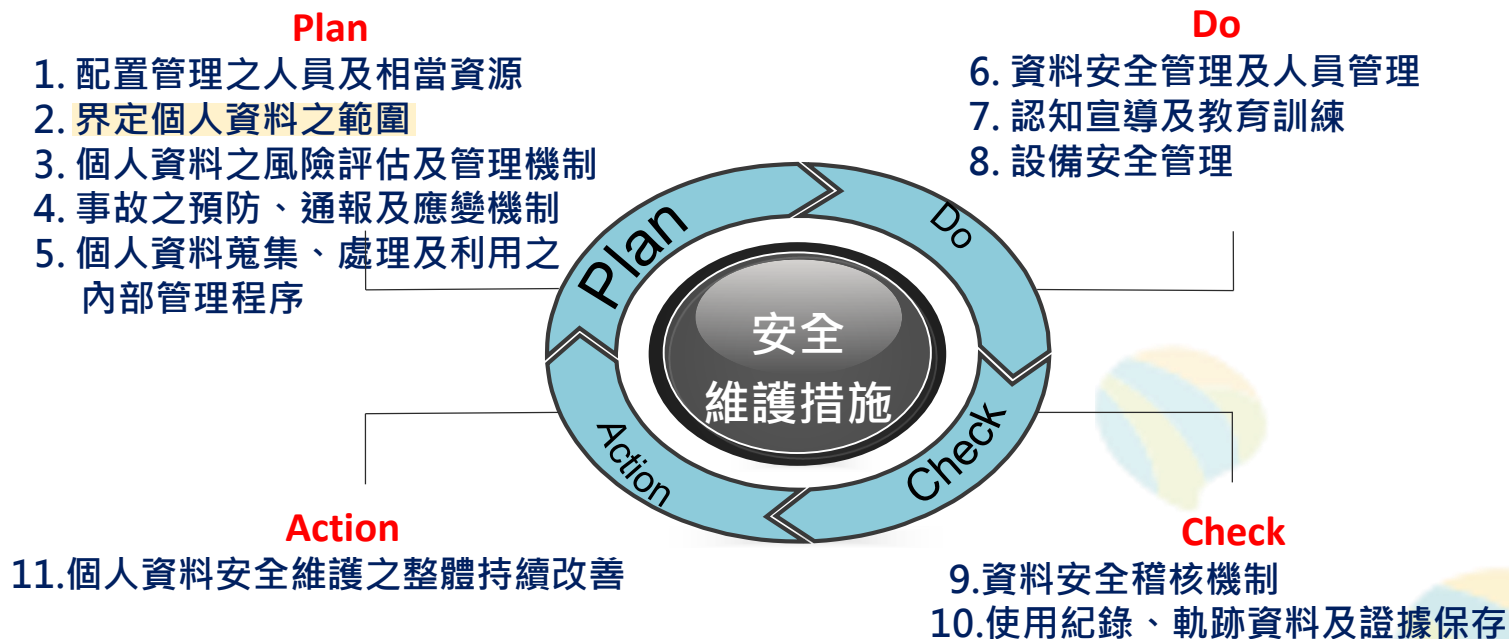




# 訂定安全維護計畫

- 個資盤點 ( 本辦法§6 )

- 人力供應業者應依據個人資料保護相關法令，定期清查所保有之個人資料，納入本計畫之範圍及建立檔案，並隨時確認法令有無變動。

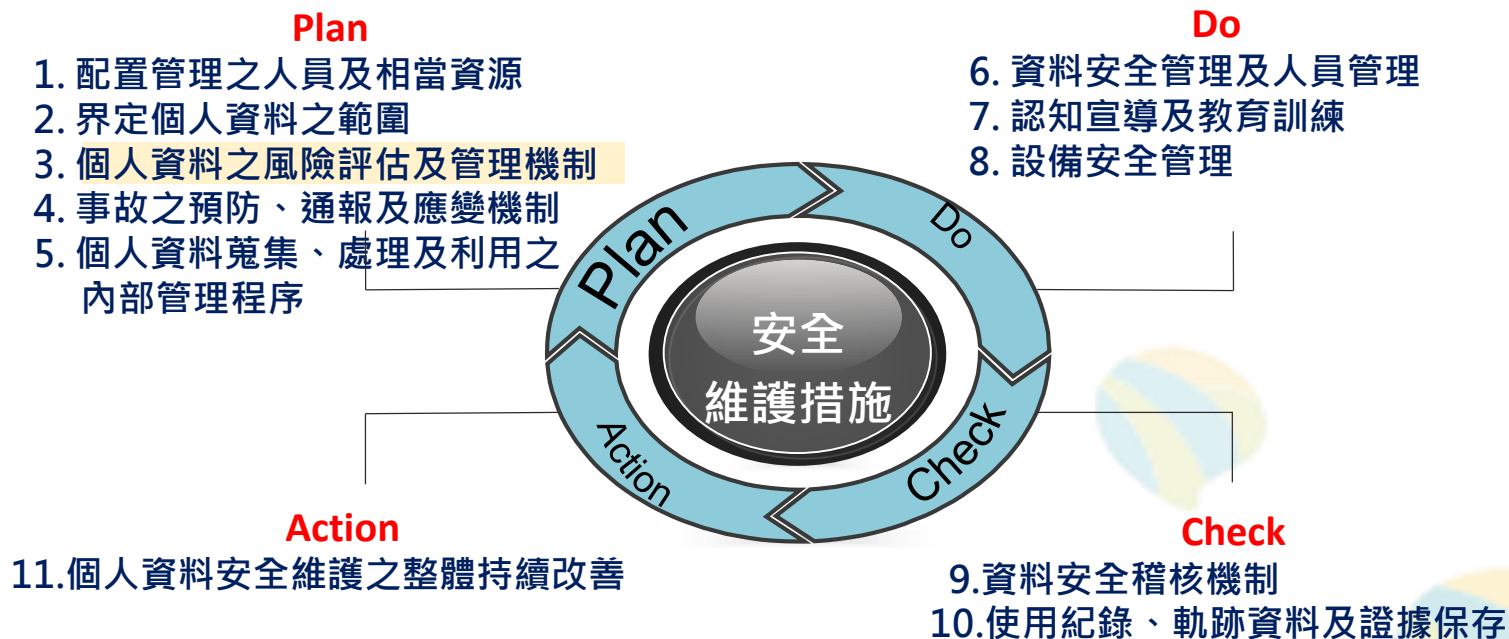




# 訂定安全維護計畫

## • 風險分析 ( 本辦法§7 )

- 人力供應業者應依據前條所界定之範圍，分析蒐集、處理及利用過程中可能產生之風險，並依據分析結果，訂定適當管控措施。

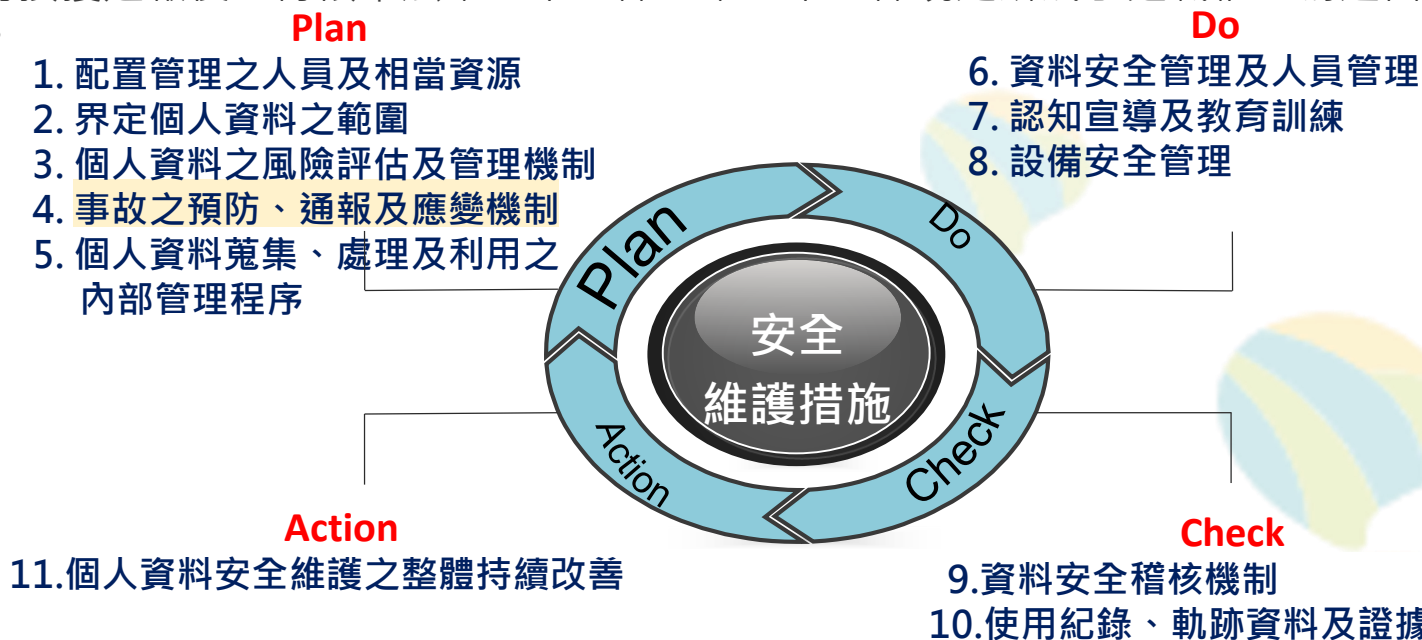




# 訂定安全維護計畫

## • 個人資料事故（本辦法§8）

- 人力供應業者為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應建立下列機制：
  - 採取適當應變措施，以控制事故對當事人之損害
  - 查明事故狀況，並以適當方式通知當事人相關事故事實、因應措施及諮詢服務專線等
  - 檢討預防機制，避免類似事故再次發生。
- 人力供應業者發現前項事故時，應於七十二小時內填具通報紀錄表（如附表），通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關；中央目的事業主管機關或直轄市、縣（市）政府接獲通報後，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。

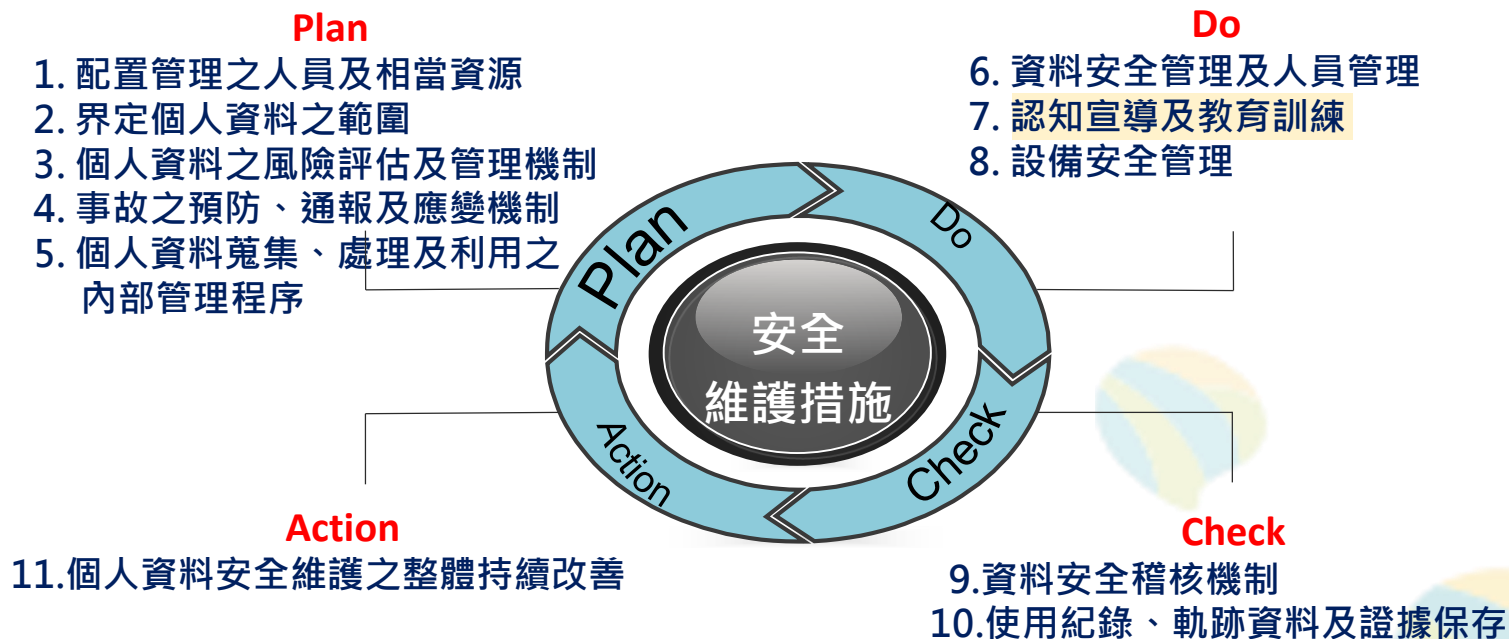




# 訂定安全維護計畫

## • 教育訓練 ( 本辦法§9 )

- 人力供應業者應定期對所屬人員施以基礎認知宣導或專業教育訓練，使其瞭解個人資料保護相關法令規定、責任範圍、管理措施或方法。





# 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

## 辦法第4條

I 人力供應業者就個人資料檔案安全維護管理，應指定專人或建立專責組織負責，並配置相當資源。

II 前項專人或專責組織之任務如下：

一、規劃、訂定、修正及執行本計畫。

二、訂定個人資料保護管理原則，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項公告，使其所屬人員瞭解。

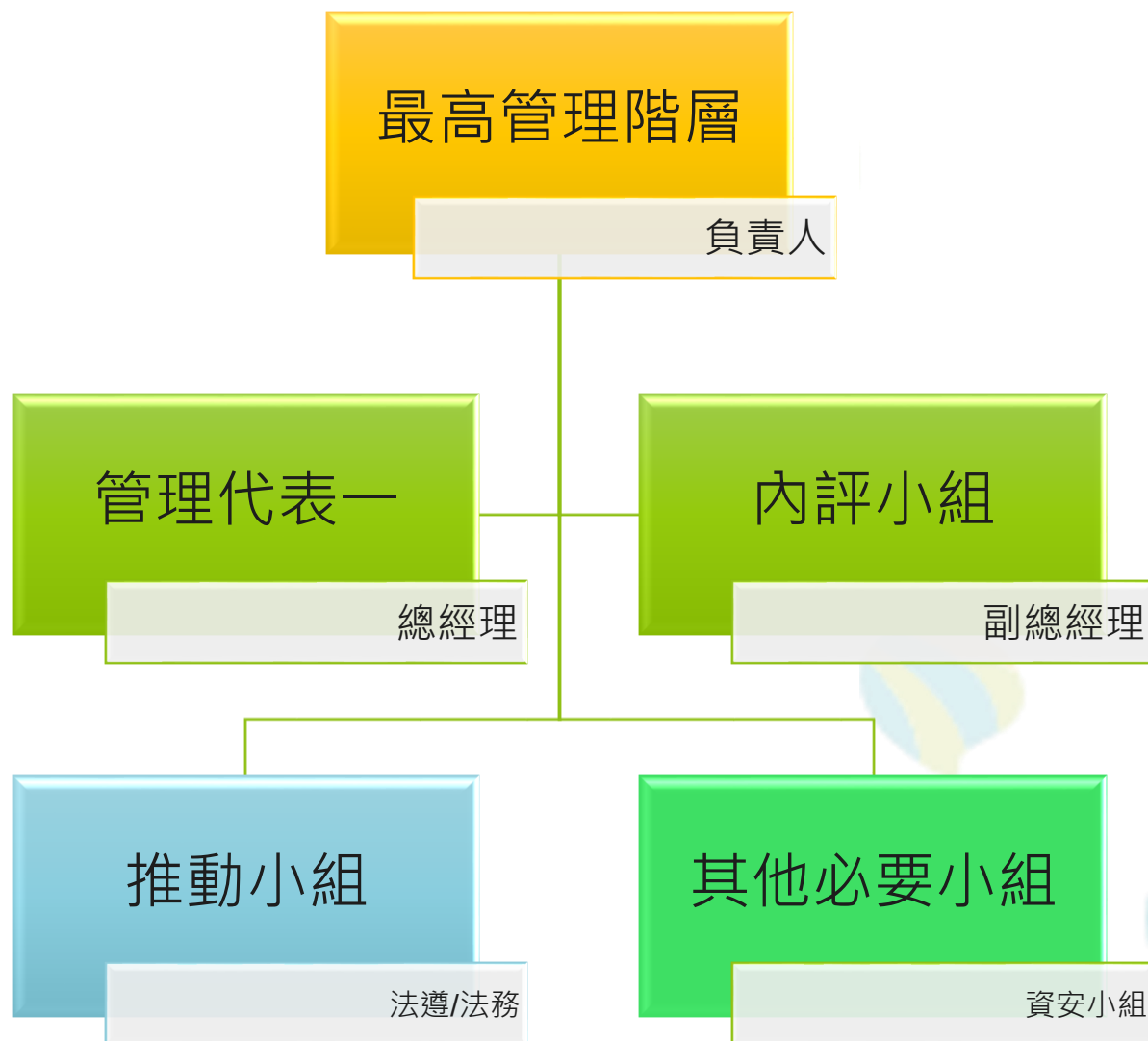


# 最高管理階層

- 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。

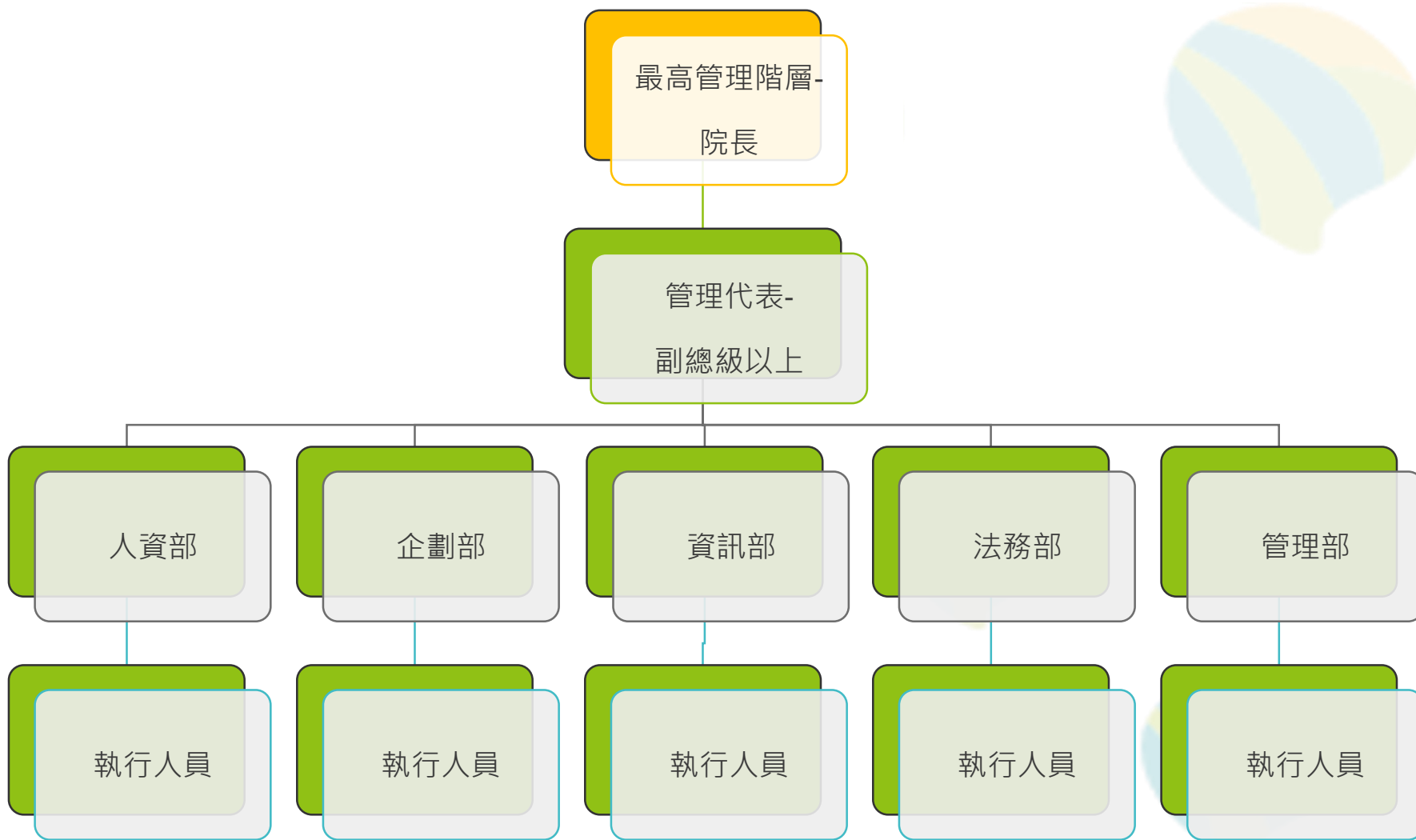


# 參考架構-任務型





# 參考架構-組織型





# 自評表

| 查檢項目                                                          | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                                |
|---------------------------------------------------------------|------|------|-----|-----|--------------------------------------------------------|
|                                                               | 符合   | 部分符合 | 不符合 | 不適用 |                                                        |
| 1.個人資料保護規劃                                                    |      |      |     |     |                                                        |
| 1.1是否指定專人或專責單位，負責辦理個人資料保護管理政策之研議、認知宣導與教育訓練、資料與設備安全管理、稽核等工作事項？ |      |      |     |     | ( 佐證資料如：企業組織圖，得以看出個資專責人員配置、會議記錄、教育訓練規劃、資安管理程序文件、稽核計畫 ) |
| 1.2是否有個人資料管理人員組織配置？並依分工執行？                                    |      |      |     |     | ( 佐證資料如：個資成員分工表)                                       |
| 1.3是否有個人資料保護管理政策是否公告公司人員周知？                                   |      |      |     |     | ( 佐證資料如：政策文件等)                                         |
| 1.4就個人資料之蒐集、處理及利用是否有相關程序規定？是否公告公司人員周知？                        |      |      |     |     | ( 佐證資料如：個人資料之蒐集、處理及利用是否有相關程序或個人資料檔案安全維護計畫、佈達證據等 )      |
| 1.5是否進行個人資料盤點並備有清冊？盤點之方式為何？結果之正確性？                            |      |      |     |     | ( 佐證資料如：個資盤點清冊、稽核紀錄等)                                  |



# 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



# 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.





# 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





# 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

# 法令主管機關移由國家發展委員會主政

行政院公報

第 025 卷 第 010 期 20190115 外交國防法務篇

法 務 部  
國家發展委員會公告  
中華民國 108 年 1 月 10 日  
法律字第 10803500010 號  
發法字第 1080080004A 號

主 旨：為配合一百零七年十二月十二日修正發布之法務部處務規程第八條及第十八條修正條文，公告個人資料保護法及個人資料保護法施行細則相關條文涉及原管轄機關為法務部者，變更為國家發展委員會。

依 據：行政程序法第十一條第二項規定。

公告事項：「個人資料保護法及個人資料保護法施行細則管轄變更法律及法規命令條文表」。

個人資料保護法及個人資料保護法施行細則管轄變更法律及法規命令條文表

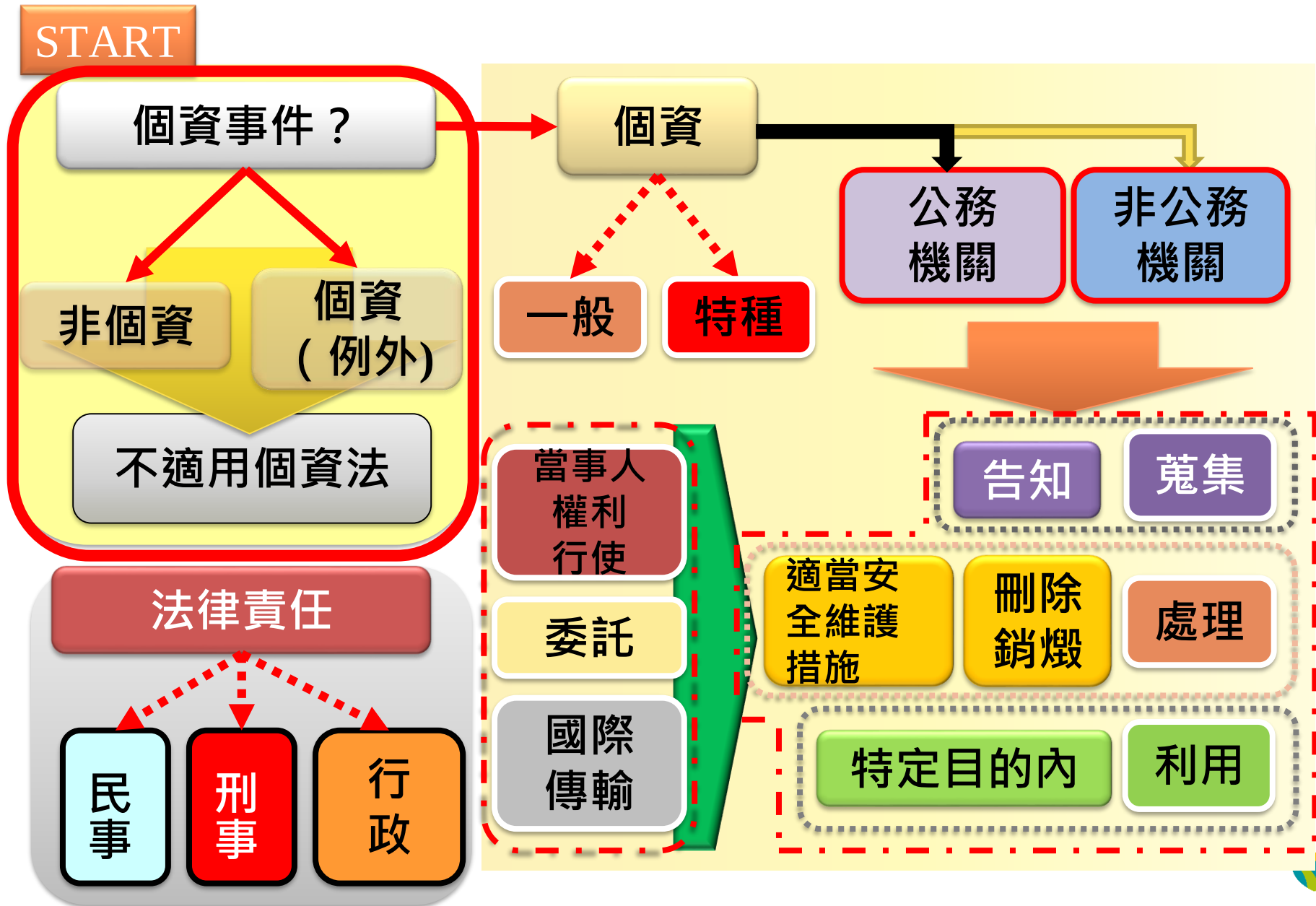
| 序號 | 法律名稱        | 條項款目    | 管轄事項變更情形                            |
|----|-------------|---------|-------------------------------------|
| 1  | 個人資料保護法     | §53、§55 | 本法各該規定所列屬「法務部」之權責事項，改由「國家發展委員會」管轄。  |
| 2  | 個人資料保護法施行細則 | §33     | 本細則各該規定所列屬「法務部」之權責事項，改由「國家發展委員會」管轄。 |

註：為茲簡明，條項款目標中，各條、項、款、目等，分以下列方式表達：條→§（條號以阿拉伯數字表達）、項→I（羅馬符號）、款→(1)（括弧內置阿拉伯數字）、目→○1（圓圈內置阿拉伯數字），目以下則以「之○（阿拉伯數字）」表達。

行政院公報第25卷10期2763頁「法務部、國家發展委員會公告：為配合107年12月12日修正發布之「法務部處務規程」第8條及第18條修正條文，公告「個人資料保護法」及「個人資料保護法施行細則」相關條文涉及原管轄機關為法務部者，變更為「國家發展委員會」。



# 個資法規範架構暨個資全生命週期



# 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。



# 路人入鏡，是否有個資法適用？

- 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？



# 案例-神搜OL波多野 路人入鏡挨酸怒告

- 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

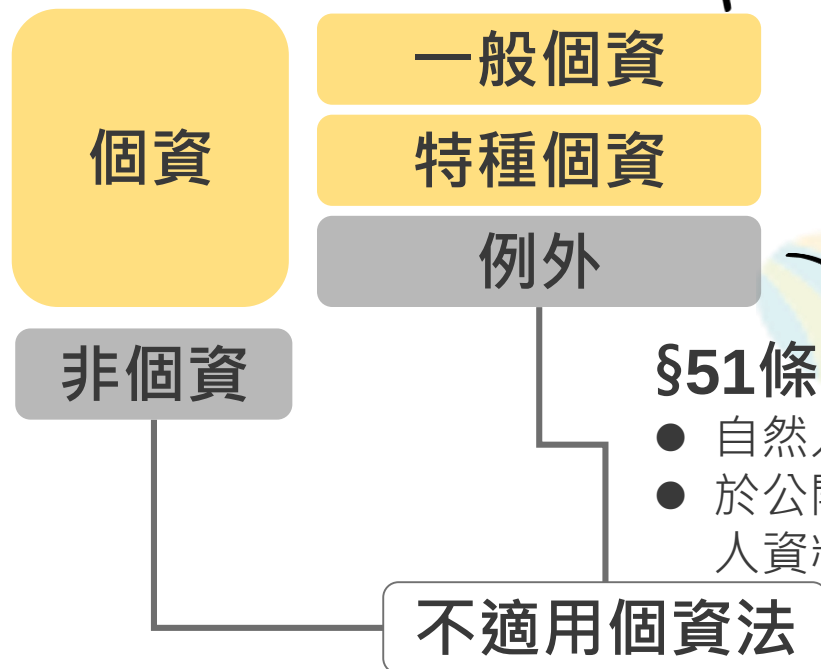
亡者資料？

## §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。



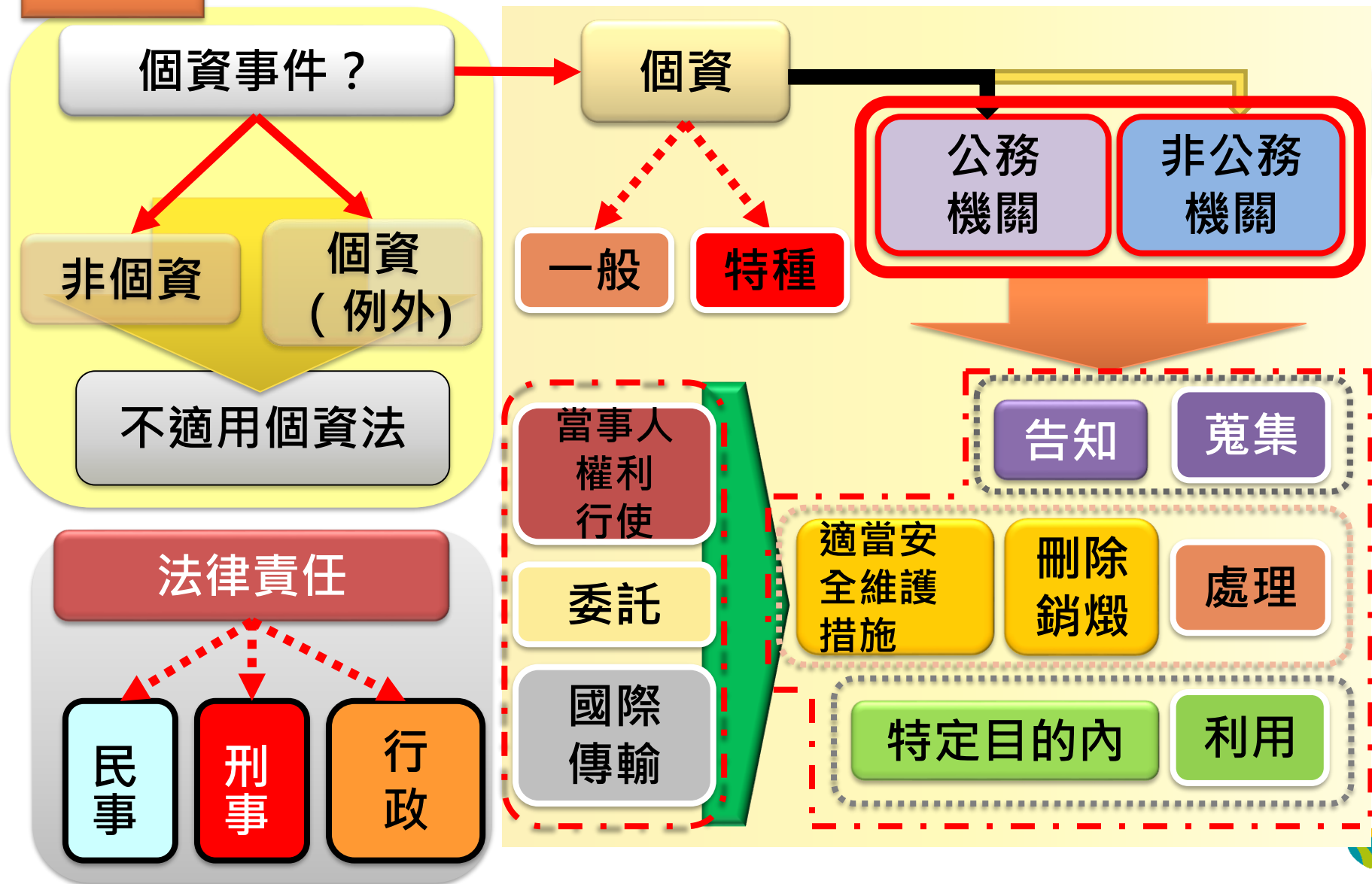
## §51條

- 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

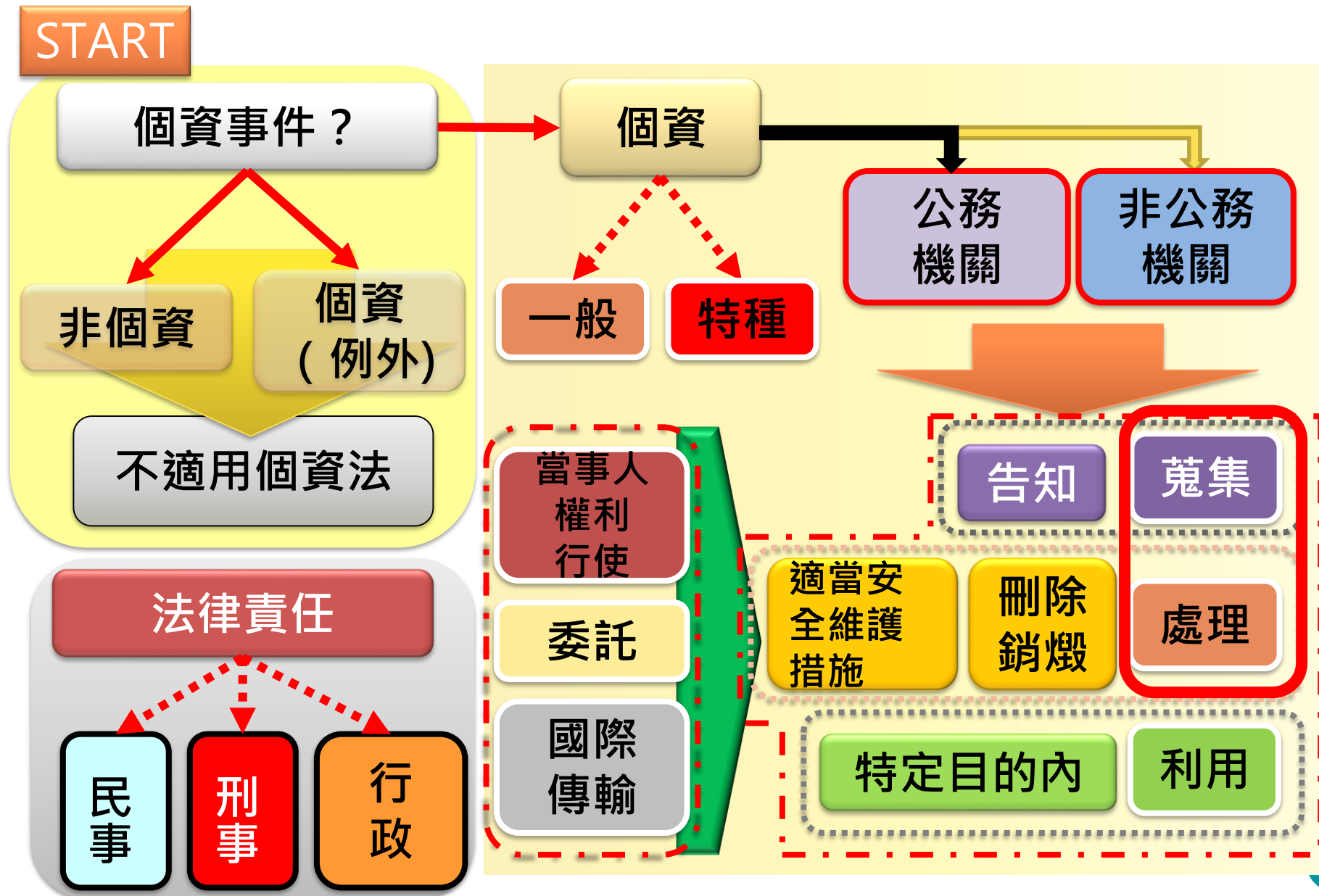
|          | 公務機關                   | 非公務機關                |
|----------|------------------------|----------------------|
| 定義       | 指依法行使公權力之中央或地方機關或行政法人。 | 指公務機關以外之自然人、法人或其他團體。 |
| 蒐集、處理及利用 | 第二章 ( 個資法第15 - 18條)    | 第三章 ( 個資法第19 - 27條 ) |
| 賠償責任的免除  | 不可抗力                   | 無故意或過失            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

### 辦法§12

- ◆ 人力供應業者對個人資料之蒐集、處理或利用，除本法第六條第一項所定之資料外，應建立下列作業程序：
  - 確認蒐集、處理個人資料符合特定目的及法定要件。
  - 確認利用個人資料符合特定目的必要範圍；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外之利用要件。



# 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

### 辦法§12

人力供應業者對個人資料之蒐集、處理或利用，除本法第六條第一項所定之資料外，應建立下列作業程序：

- 確認蒐集、處理個人資料符合特定目的及法定要件。
- 確認利用個人資料符合特定目的必要範圍；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外之利用要件。

# 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。



# 個資的蒐集或處理要件彙整

| 公務機關 15    | 非公務機關 19                 | 特種資料 6                                                                |
|------------|--------------------------|-----------------------------------------------------------------------|
| 執行法定職務必要範圍 | 法律明文規定                   | 法律明文規定<br>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<br>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所必要 |
| 經當事人同意     | 經當事人同意                   | 經當事人書面同意                                                              |
| 對當事人權益無侵害  | 對當事人權益無侵害。               |                                                                       |
|            | 當事人自行公開或其他已合法公開之個人資料     | 當事人自行公開或其他已合法公開之個人資料                                                  |
|            | 學術研究機構基於公共利益為統計或學術研究而有必要 | 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                               |
|            | 與當事人有契約或類似契約關係           |                                                                       |
|            | 為增進公共利益所必要               | 已採取適當之安全措施                                                            |
|            | 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。                                  |

事前或事後有適當安全維護措施



# 個人資料管理程序

## 辦法§10

- ◆ 人力供應業者就本法第六條第一項所定之個人資料，應於蒐集、處理或利用前，確認符合相關法令規定。

## 辦法§11

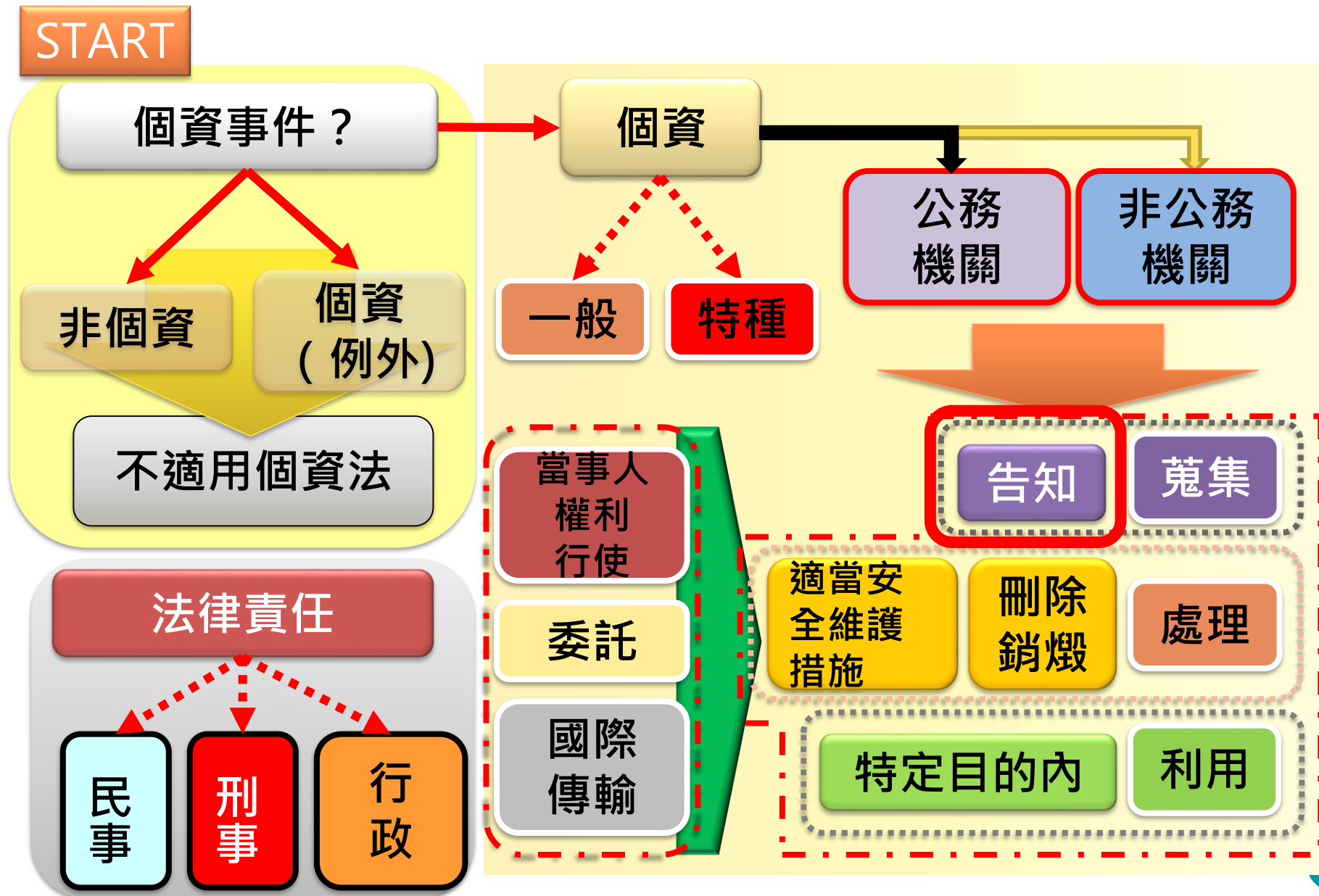
- ◆ 人力供應業者為履行本法第八條及第九條規定之告知義務，應建立下列作業程序：
  - 依據蒐集資料情況，採取適當之告知方式。
  - 確認符合免告知當事人之事由。

## 辦法§12

- ◆ 人力供應業者對個人資料之蒐集、處理或利用，除本法第六條第一項所定之資料外，應建立下列作業程序：
  - 確認蒐集、處理個人資料符合特定目的及法定要件。
  - 確認利用個人資料符合特定目的必要範圍；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外之利用要件。



# 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 | <ul style="list-style-type: none"><li>• 法律規定得免告知</li><li>• 係機關執行法定職務或履行法定義務所必要</li><li>• 告知將妨害法定職務執行</li><li>• 告知將妨害公共利益</li><li>• 當事人明知應告知之內容</li><li>• 蒐集<u>非基於營利之目的</u>且對當事人<u>無不利影響</u></li></ul> | <ul style="list-style-type: none"><li>• 有左列情形</li><li>• 當事人自行公開或已合法公開之個資</li><li>• 不能向當事人或其法定代理人為告知</li><li>• 基於公共利益為統計或學術研究之目的而有必要等</li><li>• 大眾傳播業者基於新聞報導之公益目的而蒐集個資</li></ul> |

## 辦法§11

- ◆ 人力供應業者為履行本法第八條及第九條規定之告知義務，應建立下列作業程序：
  - 依據蒐集資料情況，採取適當之告知方式。
  - 確認符合免告知當事人之事由。



# 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。



# 書面同意vs.電子方式？

法務部102年03月21日法律字第10203502480號函

應考人於進行國家考試網路報名系統進行報名前，均經告知並需填具同意書，始得進行網路報名，則該同意書雖係以電子方式為之，倘足以確認當事人之意思表示，並有可為證明之方式（電子簽章法第4條第2項規定參照），即具有本法第7條第2項「書面同意」之效力（經濟部100年10月27日經商字第10000663080號函參照），從而戶役政機關及各級學校將應考人個人資料提供貴部查驗，即符合本法第16條第7款、第20條第1項第6款「經當事人書面同意」之情形，而得合法為個人資料之特定目的外利用。



# 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。



# 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？

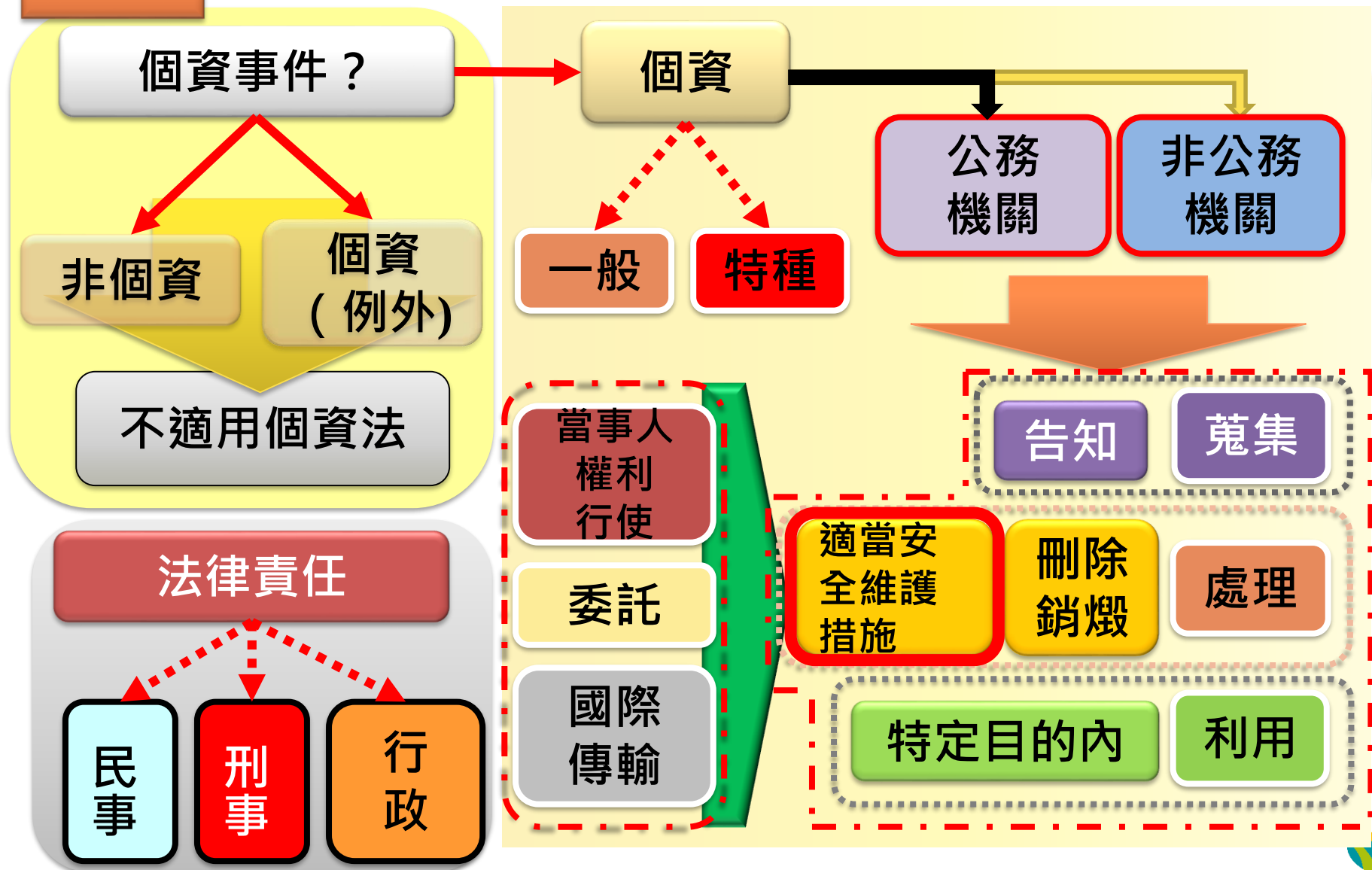
國家發展委員會民國 108 年 03 月 12 日發法字第1082000384號函

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。



# 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。



# 辦法所規定之個人資料管理措施

- 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。
- 必要且適當之安全管理措施應至少包括，但不限於下列措施：
  - 人員面安全管理措施
  - 資安面安全管理措施
  - 設備面安全管理措施
  - 技術面安全管理措施
- 組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。

辦法第19~22條

包含人員、資安、設備安全管理、技術管理。





# 人員安全管理措施

## 辦法§19

### ◆ 人力供應業者就人員管理，應採取下列措施：

- 確認蒐集、處理及利用個人資料之各相關業務流程之負責人員。
- 依據作業之需要，建立管理機制，設定所屬人員不同權限，並定期確認權限內容之適當及必要性。
- 與所屬人員約定保密義務。
- 所屬人員離職時取消其識別碼，並收繳其通行證（卡）及相關證件。
- 所屬人員持有個人資料者，於其離職時，應要求其返還個人資料之載體，並銷毀或刪除因執行業務儲存而持有之個人資料。



# 人員安全管理措施

## 人員之管理與監督

- 選任監督
  - 聘用適當人才（專業知識、證照）
- 保密契約
  - 在職期間及離職後一段時間仍適用
- 教育訓練
  - 制定教育訓練計畫及訂定評量機制



# 自評表

| 查檢項目                                                                                | 自評內容 |      |     |     | 簡述原因<br>(並檢附佐證資料)                         |
|-------------------------------------------------------------------------------------|------|------|-----|-----|-------------------------------------------|
|                                                                                     | 符合   | 部分符合 | 不符合 | 不適用 |                                           |
| 5.1資料安全管理                                                                           |      |      |     |     |                                           |
| 5.1.1是否訂定適用之資訊安全注意事項並公告周知？                                                          |      |      |     |     | (佐證資料如：公告說明或其他內部制度文件等)                    |
| 5.1.2運用電腦或自動化機器相關設備，是否訂定使用可攜式設備或儲存媒介物之規範？                                           |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關行動式設備之管理規範) |
| 5.1.3保有之個人資料內容，有加密或遮蔽之必要時，是否採取適當之加密或遮蔽機制？                                           |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關保管個資之管理規範)  |
| 5.1.4傳輸個人資料時，因應不同之傳輸方式，有加密必要時，是否採取適當加密機制？是否確認資料收受者之正確性？                             |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關傳輸個資之管理規範)  |
| 5.1.5依據保有資料之重要性，評估有備份必要時，予以備份，是否比照原件加密？儲存備份資料之媒介物，是否以適當方式保管？是否定期進行備份資料之還原測試，以確保有效性？ |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關備份個資之管理規範)  |
| 5.1.6儲存個人資料之媒介物於報廢或轉作其他用途時，以物理或其他方式是否確實破壞或刪除媒介物中所儲存之資料？                             |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關報廢個資之管理規範)  |
| 5.1.7是否妥善保存管理機制及加密機制中所運用之密碼？                                                        |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關加密個資之管理規範)  |



# 資安安全管理措施

## 辦法§20

- ◆ 人力供應業者蒐集、處理或利用個人資料，就資料安全管理，應採取下列措施：
  - 訂定作業注意事項。
  - 運用電腦或自動化機器相關設備，訂定使用可攜式設備或儲存媒介物之規範。
  - 保有之個人資料內容，有加密或遮蔽之必要時，採取適當之加密或遮蔽機制。
  - 傳輸個人資料時，因應不同之傳輸方式，有加密必要時，採取適當加密機制，並確認資料收受者之正確性。
  - 依據保有資料之重要性，評估有備份必要時，予以備份，並比照原件加密。儲存備份資料之媒介物，以適當方式保管，且定期進行備份資料之還原測試，以確保有效性。
  - 儲存個人資料之媒介物於報廢或轉作其他用途時，以物理或其他方式確實破壞或刪除媒介物中所儲存之資料。
  - 妥善保存管理機制及加密機制中所運用之密碼。



# 資訊安全管理措施 - 媒體管理

## 資訊安全

- 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

# 資訊安全管理措施 - 加密、傳輸、備份

## 資訊安全

- 加密
- 適當之加密或遮蔽機制（遠端存取、自動監控）
- 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）
- 備份
  - 系統備份（訂定最大容忍資料損失之時間要求）
    - 目標回復時點（RPO）
  - 系統備援（訂定最大可容忍中斷時間及最低可接受服務水準）
    - 最大容許中斷時間（Maximum Tolerable Period of Disruption：MTPD）
    - 目標回復時間（Recovery Time Objective：RTO）



# 自評表

| 查檢項目                                                                                | 自評內容 |      |     |     | 簡述原因<br>(並檢附佐證資料)                         |
|-------------------------------------------------------------------------------------|------|------|-----|-----|-------------------------------------------|
|                                                                                     | 符合   | 部分符合 | 不符合 | 不適用 |                                           |
| 5.1資料安全管理                                                                           |      |      |     |     |                                           |
| 5.1.1是否訂定適用之資訊安全注意事項並公告周知？                                                          |      |      |     |     | (佐證資料如：公告說明或其他內部制度文件等)                    |
| 5.1.2運用電腦或自動化機器相關設備，是否訂定使用可攜式設備或儲存媒介物之規範？                                           |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關行動式設備之管理規範) |
| 5.1.3保有之個人資料內容，有加密或遮蔽之必要時，是否採取適當之加密或遮蔽機制？                                           |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關保管個資之管理規範)  |
| 5.1.4傳輸個人資料時，因應不同之傳輸方式，有加密必要時，是否採取適當加密機制？是否確認資料收受者之正確性？                             |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關傳輸個資之管理規範)  |
| 5.1.5依據保有資料之重要性，評估有備份必要時，予以備份，是否比照原件加密？儲存備份資料之媒介物，是否以適當方式保管？是否定期進行備份資料之還原測試，以確保有效性？ |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關備份個資之管理規範)  |
| 5.1.6儲存個人資料之媒介物於報廢或轉作其他用途時，以物理或其他方式是否確實破壞或刪除媒介物中所儲存之資料？                             |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關報廢個資之管理規範)  |
| 5.1.7是否妥善保存管理機制及加密機制中所運用之密碼？                                                        |      |      |     |     | (佐證資料如：檢視資訊安全政策、個人資料檔案安全維護計畫有關加密個資之管理規範)  |



# 設備安全管理措施

## 辦法§21

### ◆ 人力供應業者就設備安全管理，應採取下列措施：

- 依據作業內容不同，實施必要之進出管制方式。
- 妥善保管個人資料之儲存媒介物。
- 針對不同作業環境，加強天然災害及其他意外災害之防護，並建置必要之防災設備



# 設備安全管理措施

## 設備安全

### 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）
- 儲存媒介物存放方式及位置
- 防災設備建置



# 自評表

| 查檢項目                                        | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                               |
|---------------------------------------------|------|------|-----|-----|-------------------------------------------------------|
|                                             | 符合   | 部分符合 | 不符合 | 不適用 |                                                       |
| 5.3設備安全管理                                   |      |      |     |     |                                                       |
| 5.3.1依據作業內容不同、作業環境及個人資料之種類與數量，實施必要之門禁管理？    |      |      |     |     | ( 佐證資料如：檢視個人資料檔案安全維護計畫有關實體安全或門禁管理之規範、內部制度文件等，人員進出登記簿) |
| 5.3.2是否以適當方式或場所保管個人資料之儲存媒介物？                |      |      |     |     | ( 佐證資料如：內部評估或稽核記錄、內部制度文件、人員進出登記簿等)                    |
| 5.3.3針對不同作業環境，是否加強天然災害及其他意外災害之防護並建置必要之防災設備？ |      |      |     |     | ( 佐證資料如：內部制度文件資產清單)                                   |





# 技術安全管理措施

## 辦法§22

### ◆ 人力供應業者就技術管理，應採取下列措施：

- 於電腦、自動化處理設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別及控管。
- 認證機制使用之帳號及密碼，具備一定之複雜度，並定期更換密碼。
- 於電腦、自動化處理設備或系統上設定警示與相關反應機制，以對不正常之存取進行適當之反應及處理。
- 個人資料存取權限之數量及範圍，依作業必要予以設定，且不得共用存取權限。
- 採用防火牆或入侵偵測等設備，避免儲存個人資料之系統遭受無權限之存取。
- 使用能存取個人資料之應用程式時，確認使用者具備使用權限。
- 定期測試權限認證機制之有效性。
- 定期檢視個人資料之存取權限設定。
- 於處理個人資料之電腦系統中安裝防毒、防駭軟體，並定期更新病毒碼。
- 對於電腦作業系統及相關應用程式之漏洞，定期安裝修補程式。
- 對於具備存取權限之電腦或自動化處理設備，不得安裝檔案分享軟體。
- 測試處理個人資料之資訊系統時，不使用真實個人資料，有使用真實個人資料之情形時，明確規定使用程序。
- 處理個人資料之資訊系統有變更時，確認其安全性並未降低。
- 定期檢查處理個人資料資訊系統之使用狀況，及個人資料存取情形。



# 技術管理措施-存取控制

## 技術安全

- 存取控制

- 存取控制 ( 存取控制清單、防火牆或入侵偵測 )
- 密碼控制 ( 密碼規則 )
- 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 )
- 示警功能 ( 對於異常存取進行反應及處理 )
- 最小權限 ( 管理角色應分開管理帳號，非全部使用最高權限、定期檢視 )
- 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、部安裝檔案分享軟體 )
- 防毒、防駭軟體 ( 定期檢視及更新 )
- 測試資料 ( 盡量不使用真實資料、若使用需核備 )



# 技術管理措施-識別鑑別與技術檢視

## 技術安全

- 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 )

- 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 )



# 技術安全管理措施-系統與資訊完整性

## 技術安全

- 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



# 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公告，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 ( 1 )

| 查檢項目                                                  | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                                 |
|-------------------------------------------------------|------|------|-----|-----|---------------------------------------------------------|
|                                                       | 符合   | 部分符合 | 不符合 | 不適用 |                                                         |
| 5.4.技術管理措施                                            |      |      |     |     |                                                         |
| 5.4.1是否於電腦、自動化處理設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別及控管？    |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄、IP限制、使用VPN加密通道或雙因子認證、內部制度文件)      |
| 5.4.2認證機制使用之帳號及密碼，是否具備一定之複雜度，並定期更換密碼？                 |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄、IP限制、使用VPN加密通道或雙因子認證、內部制度文件)      |
| 5.4.3是否於電腦、自動化處理設備或系統上設定警示與相關反應機制，以對不正常之存取進行適當之反應及處理？ |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄、IP限制、使用VPN加密通道或雙因子認證、內部制度文件)      |
| 5.4.4個人資料存取權限之數量及範圍，是否依作業必要予以設定？是否禁止共用帳戶和密碼？          |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄、IP限制、使用VPN加密通道或雙因子認證、密碼政策、內部制度文件) |
| 5.4.5是否採用防火牆或入侵偵測等設備，避免儲存個人資料之系統遭受無權限之存取？             |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄、內部制度文件、設備清單)                      |
| 5.4.6使用能存取個人資料之應用程式時，是否確認使用者具備使用權限？                   |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄、IP限制、使用VPN加密通道或雙因子認證、密碼政策、內部制度文件) |
| 5.4.7是否定期測試權限認證機制之有效性                                 |      |      |     |     | ( 佐證資料如：測試記錄)                                           |



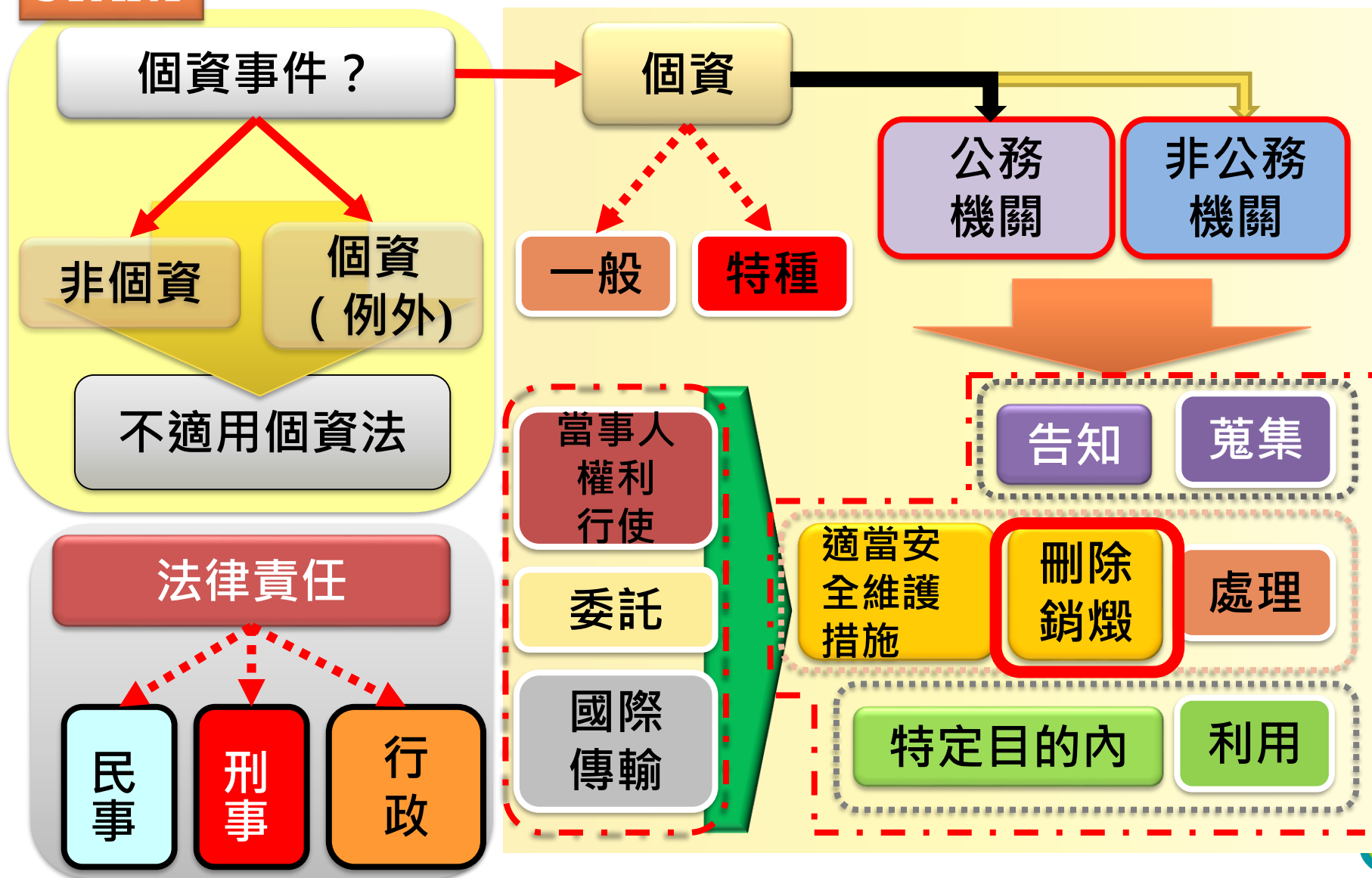
# 自評表 ( 2 )

| 查檢項目                                                       | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                         |
|------------------------------------------------------------|------|------|-----|-----|-------------------------------------------------|
|                                                            | 符合   | 部分符合 | 不符合 | 不適用 |                                                 |
| 5.4.技術管理措施                                                 |      |      |     |     |                                                 |
| 5.4.8是否定期檢視個人資料之存取權限設定？                                    |      |      |     |     | ( 佐證資料如：存取權限清單、檢視紀錄)                            |
| 5.4.9是否於處理個人資料之電腦系統中安裝防毒、防駭軟體?是否定期更新病毒碼？                   |      |      |     |     | ( 佐證資料如：存取控制措施(經過授權的使用者才能使用或契約協議、防毒防駭軟體清單、更新紀錄) |
| 5.4.10對於電腦作業系統及相關應用程式之漏洞，是否定期安裝修補程式？                       |      |      |     |     | ( 佐證資料如：弱點掃描、滲透測試等報告)                           |
| 5.4.11對於具備存取權限之電腦或自動化處理設備，是否禁止安裝檔案分享軟體？                    |      |      |     |     | ( 佐證資料如：IP限制、使用VPN加密通道或雙因子認證、軟體清單)              |
| 5.4.12測試處理個人資料之資訊系統時，是否不使用真實個人資料？有使用真實個人資料之情形時，是否明確規定使用程序？ |      |      |     |     | ( 佐證資料如：測試報告、內部程序文件)                            |
| 5.4.13處理個人資料之資訊系統有變更時，是否確認其安全性並未降低？                        |      |      |     |     | ( 佐證資料如：測試報告、內部程序文件)                            |
| 5.4.14是否定期檢查處理個人資料資訊系統之使用狀況，及個人資料存取情形？                     |      |      |     |     | ( 佐證資料如：存取權限管理、監控審核記錄等)                         |



# 個資法規範架構暨個資全生命週期

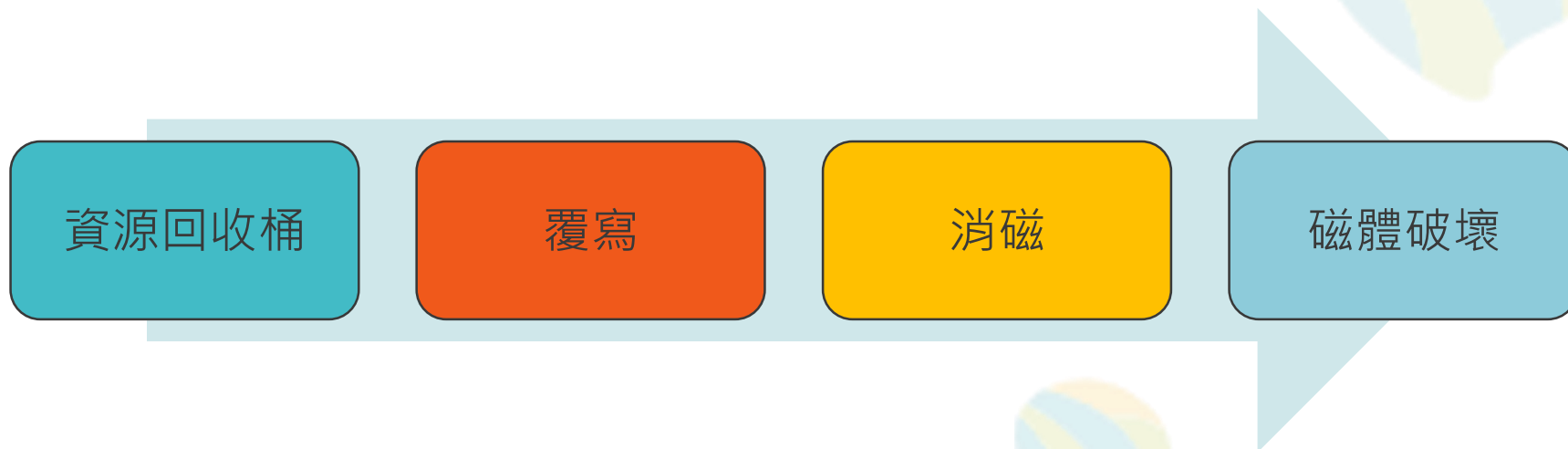
START





# 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



# 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。



# 業務終止後個人資料處理方法

## 辦法§23

- ◆ 人力供應業者業務終止後之個人資料處理，應採取下列措施：
  - 刪除或銷毀儲存個人資料之媒介物中所儲存之資料，記錄並留存刪除或銷毀之方法、時間、地點及證明刪除或銷毀之方式。
  - 受移轉之對象得合法保有該項個人資料，記錄並留存移轉原因、方法、時間及地點。
- ◆ 前項紀錄、軌跡資料及相關證據，應保存五年。



# 個人資料管理程序

## 辦法§18

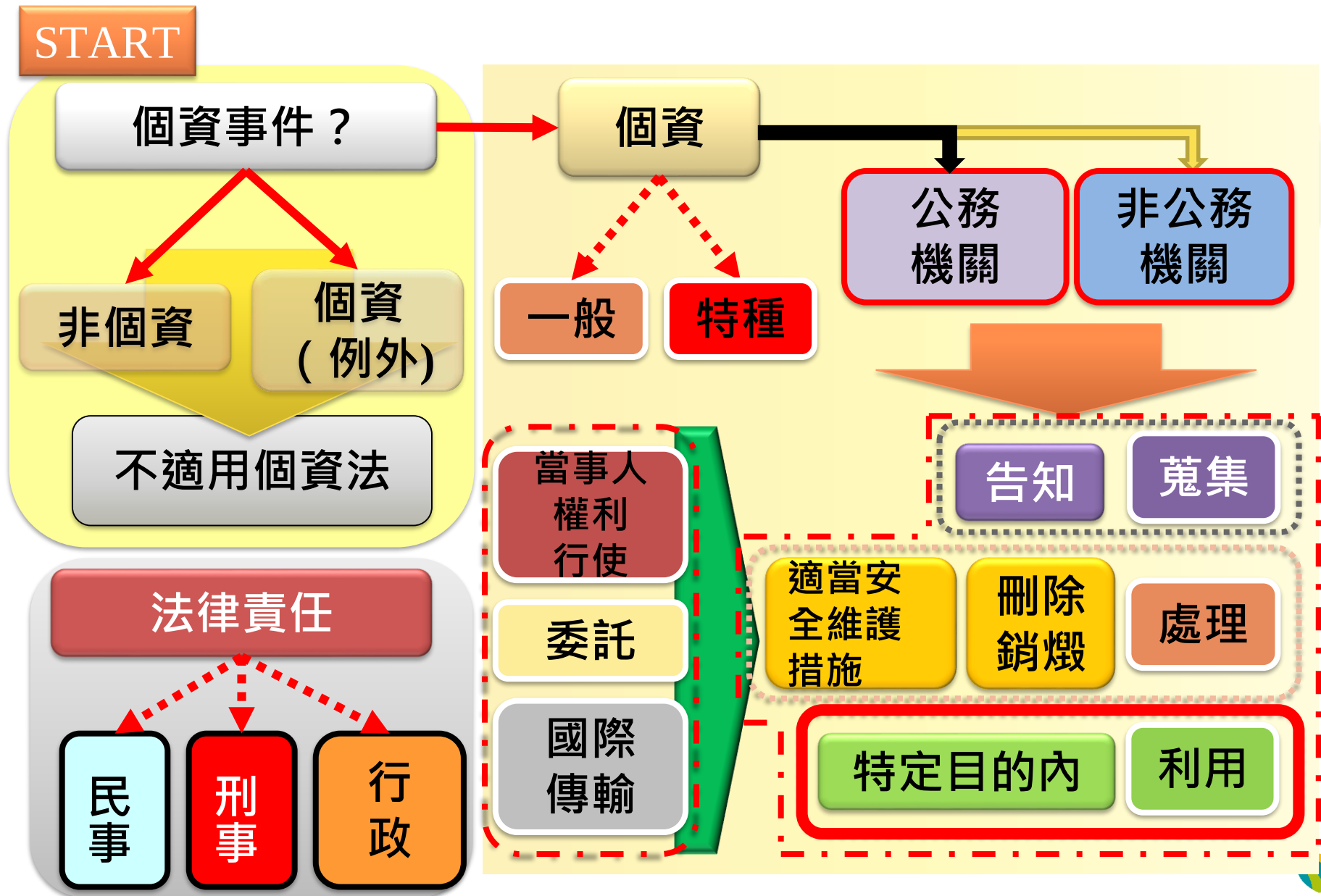
- ◆ 人力供應業者，應定期確認所保有個人資料之特定目的有無消失或期限屆滿。
- ◆ 個人資料之特定目的消失或期限屆滿時，應依本法第十一條第三項規定辦理。

## 個資法§11 第三項

- ◆ 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。



# 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。



# 特定目的外利用-行銷

## 辦法§14

- ◆ 人力供應業者利用個人資料行銷時，應建立下列作業程序：
  - 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。
  - 當事人表示拒絕接受行銷時，立即停止利用其個人資料行銷，並通知所屬人員。



# 利用（一）公務/非公務機關要件彙整

公務機關

非公務機關

原則：特定目的內利用 15 & 19

與蒐集之特定目的相符

執行法定職務必要範圍

例外：特定目的外利用 16 & 20

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/學術研究機構基於公共利益為統計或學術研究而有必要\*

經當事人同意

有利於當事人權益

維護國家安全

\* 資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人



# 個資的目的外利用要件彙整

## 個資法§6

- 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§16、20

- 一、法律明文規定。
- 二、為（維護國家安全或）增進公共利益所必要。
- 三、為免除當事人之生命、身體、自由或財產上之危險。
- 四、為防止他人權益之重大危害。
- 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 六、經當事人同意。
- 七、有利於當事人權益。



# 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

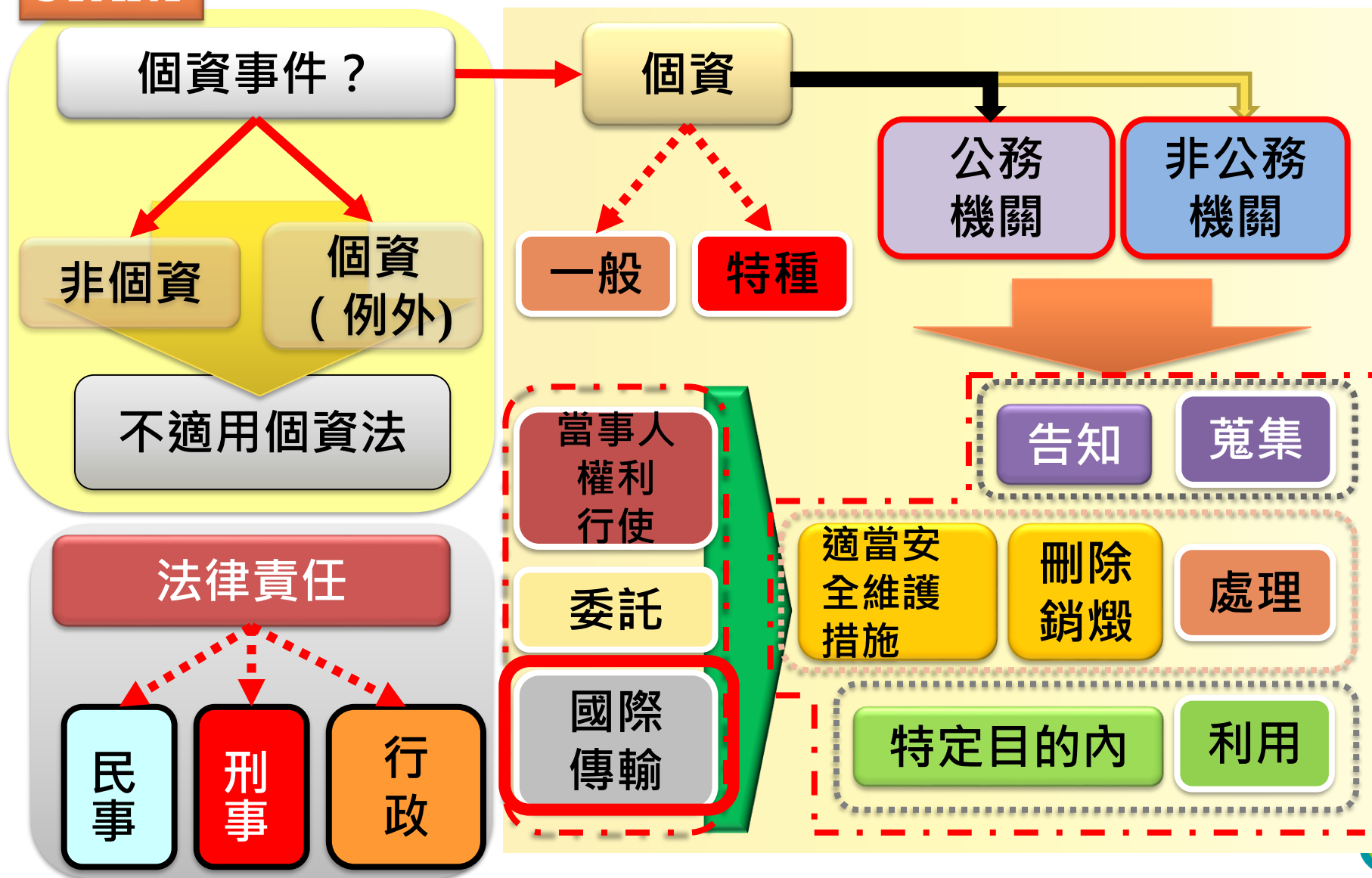


本人同意所蒐集之聯絡資料作為富邦產險日後進行共同行銷之特定目的使用。如未勾選不會影響本次投保權益，可直接進行下一步，視為不同意上述說明。



# 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。



# 關於本辦法對於國際傳輸相關條文

## 辦法§ 15

- ◆ 人力供應業者進行個人資料國際傳輸前，應檢視有無中央目的事業主管機關依本法第二十一條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域。
- ◆ 前項個人資料國際傳輸，人力供應業者應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。



# 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 - 對人力仲介業之限制

- 勞動部112年2月20日勞動發管字第1120500319A號公告

「限制人力仲介業將當事人個人資料國際傳輸至大陸地區」

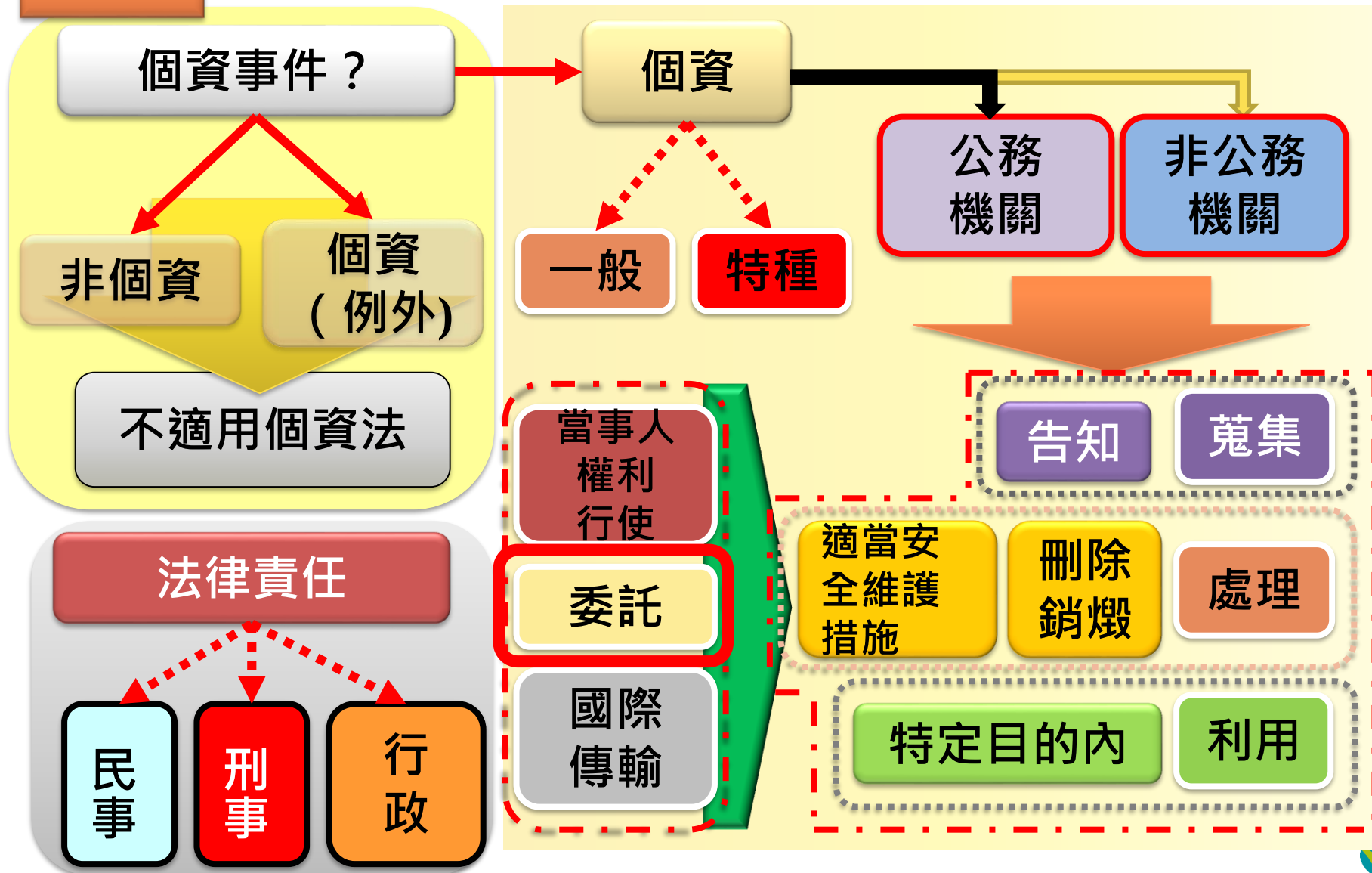
一、衡酌大陸地區之個人資料保護相關法律及法令規範尚未完備，人力仲介業以國際傳輸為蒐集、處理或利用當事人個人資料時，應考量接受國或地區對個人資料之保護具備完善之法規，爰依個人資料保護法第21條第3款規定之授權，限制人力仲介業將當事人個人資料國際傳輸至大陸地區。

二、所稱人力仲介業，指人力仲介業個人資料檔案安全維護計畫及處理辦法第2條所定，依就業服務法第34條規定經許可設立之私立就業服務機構，及依身心障礙者權益保障法第35條第3項規定經許可設立從事身心障礙者就業服務之機構。



# 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



# 個人資料管理程序

## 辦法§13

- ◆ 人力供應業者委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者建立下列監督作業程序：
  - 確認所委託蒐集、處理或利用之個人資料之範圍、類別、特定目的及期間。
  - 確認受託者採取必要安全措施。
  - 有複委託者，確認複委託之對象。
  - 受託者或其受僱人違反個人資料保護法令或委託契約條款時，要求受託者向委託人通知相關事項，及採行補救措施。
  - 委託人對受託者有保留指示者，其保留指示之事項。
  - 委託關係終止或解除時，要求受託者返還個人資料之載體，及銷毀或刪除因委託事項儲存而持有之個人資料。
- ◆ 人力供應業者應定期確認受託者執行前項要求事項之情況，並將確認結果記錄之。



# 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

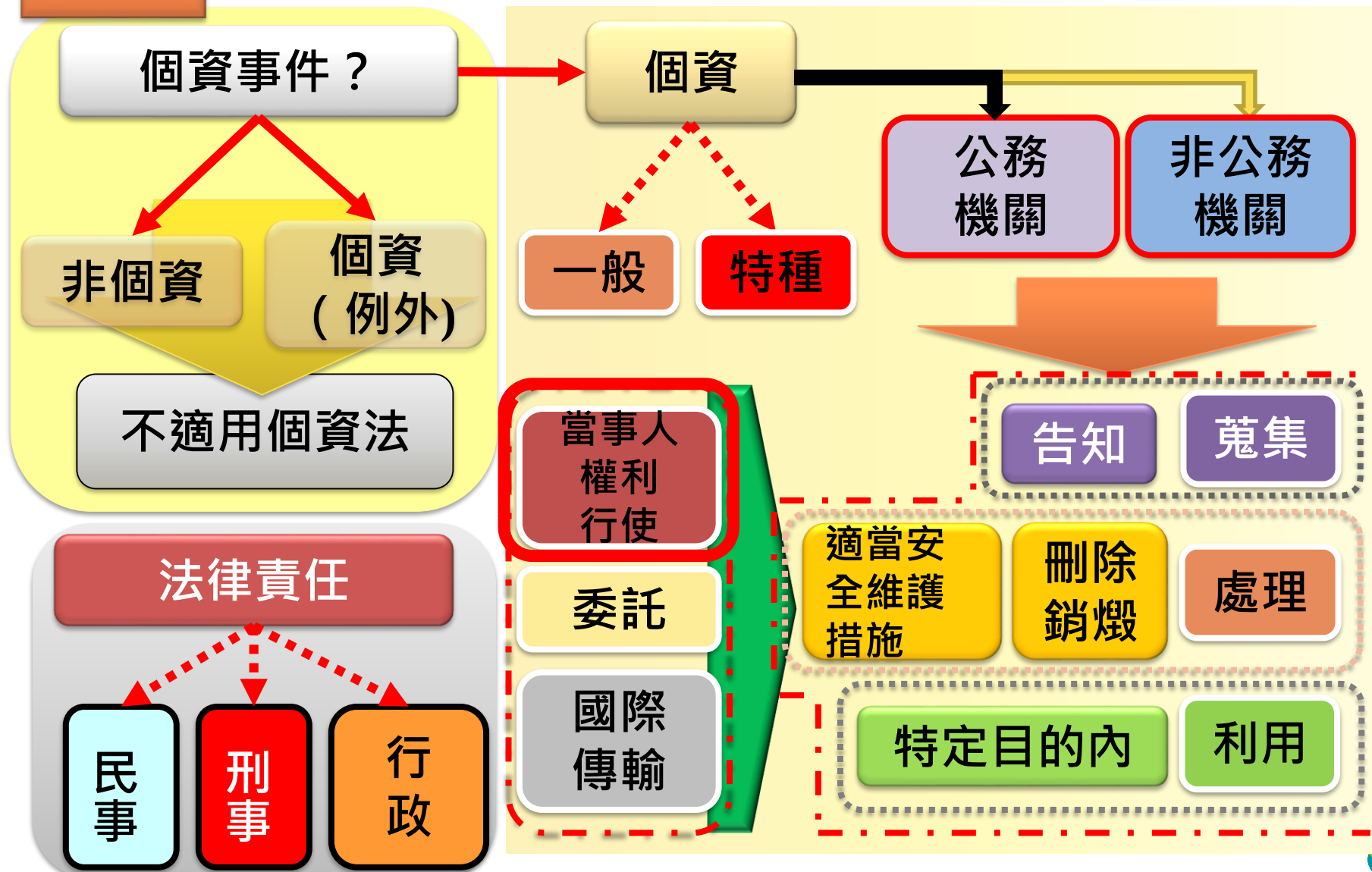
## 委外廠商查核之表單設計（例示）

| 查核項目                                             | 查核內容 | 查核結果                                                                                     | 說明 |
|--------------------------------------------------|------|------------------------------------------------------------------------------------------|----|
| 1.人員及資源配置                                        |      | <input type="checkbox"/> 符合 <input type="checkbox"/> 不符合<br><input type="checkbox"/> 不適用 |    |
|                                                  |      | <input type="checkbox"/> 符合 <input type="checkbox"/> 不符合<br><input type="checkbox"/> 不適用 |    |
| 2.界定個人資料<br><br>(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) |      | <input type="checkbox"/> 符合 <input type="checkbox"/> 不符合<br><input type="checkbox"/> 不適用 |    |
|                                                  |      | <input type="checkbox"/> 符合 <input type="checkbox"/> 不符合<br><input type="checkbox"/> 不適用 |    |
|                                                  |      | <input type="checkbox"/> 符合 <input type="checkbox"/> 不符合<br><input type="checkbox"/> 不適用 |    |



# 個資法規範架構暨個資全生命週期

START





# 個人資料管理程序

## 辦法§16

- ◆ 當事人就其個人資料行使本法第三條所定之權利者，人力供應業者應建立下列作業程序：
  - 確認當事人為個人資料之本人。
  - 提供當事人行使權利之方式，並依本法第十三條所定處理期限辦理。
  - 確認有無本法第十條及第十一條得拒絕當事人行使權利之事由；拒絕時，並附理由通知當事人。
  - 告知得收取之費用標準。

## 辦法§17

- ◆ 人力供應業者為維護其保有個人資料之正確性，應建立下列作業程序：
  - 檢視個人資料於蒐集、處理或利用過程，有無錯誤。
  - 定期檢查資料，發現錯誤者，適時更正或補充。未為更正或補充者，於更正或補充後，通知曾提供利用之對象。
  - 有爭議者，依本法第十一條第二項規定就爭議資料之處理或利用，建立相關作業程序。



# 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-蒐集、處理、利用（1）

| 查檢項目                                                        | 自評內容 |      |     |     | 簡述原因<br>( <u>並檢附佐證資料</u> )                     |
|-------------------------------------------------------------|------|------|-----|-----|------------------------------------------------|
|                                                             | 符合   | 部分符合 | 不符合 | 不適用 |                                                |
| 4.個人資料蒐集、處理及利用之內部管理程序                                       |      |      |     |     |                                                |
| 4.1有無蒐集、處理或利用特種個人資料？如有，其蒐集、處理、利用及其他相關規定是否已遵守？               |      |      |     |     | ( 佐證資料如：資料盤點表或檢視個人資料檔案安全維護計畫，針對特種個人資料之管理程序審查等) |
| 4.2是否進行告知？如否，有無法定免告知事由？告知之時點與方式是否合法、適當？                     |      |      |     |     | ( 佐證資料如：當事人同意書等)                               |
| 4.3蒐集、處理或利用個人資料是否具備並符合特定目的及特定情形是否遵守其他依法令應遵守之事項              |      |      |     |     | ( 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)             |
| 4.4是否有特定目的外利用？如有是否有合法事由？                                    |      |      |     |     | ( 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)             |
| 4.5是否進行行銷？行銷是否符合特定目的？如進行行銷，是否提供當事人拒絕行銷之管道？是否於當事人拒絕行銷時，停止行銷？ |      |      |     |     | ( 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)             |



# 自評表-蒐集、處理、利用（2）

| 查檢項目                                                                                    | 自評內容 |      |     |     | 簡述原因<br>( 並檢附佐證資料 )                          |
|-----------------------------------------------------------------------------------------|------|------|-----|-----|----------------------------------------------|
|                                                                                         | 符合   | 部分符合 | 不符合 | 不適用 |                                              |
| 4.個人資料蒐集、處理及利用之內部管理程序                                                                   |      |      |     |     |                                              |
| 4.6如何決定是否委外？委外時如何選任受託人？與受託人間是否就個人資料保護法要求事項簽訂合約或設計監督規劃？                                  |      |      |     |     | ( 佐證資料如：資料盤點表、資料流程說明(圖)、內部評鑑貨機合記錄或其他內部制度文件等) |
| 4.7是否進行個人資料國際傳輸？是否於傳輸前檢視有無中央目的事業主管機關依個人資料保護法第21條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域？           |      |      |     |     | ( 佐證資料如：資料盤點表、資料流程說明(圖)、內部評鑑貨機合記錄或其他內部制度文件等) |
| 4.8對資料接收方預定處理或利用個人資料之範圍、類別、特定目的期間、地區、對象及方式是否有監督機制？是否監督資料接收方有提供當事人行使個人資料保護法第3條所定權利等 相關事項 |      |      |     |     | ( 佐證資料如：資料盤點表、資料流程說明(圖)、內部評鑑或稽核記錄或其他內部制度文件等) |

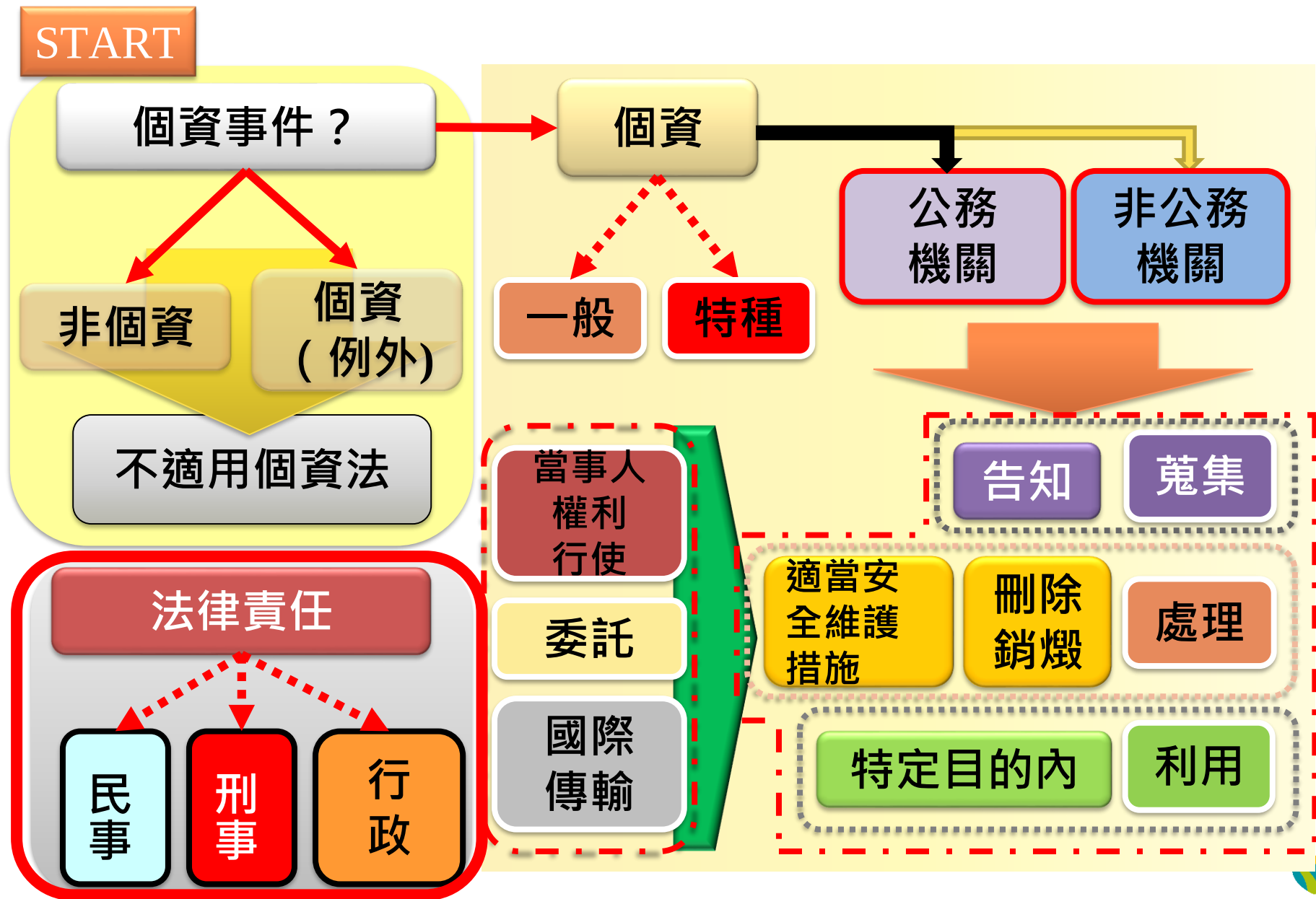


# 自評表-蒐集、處理、利用（3）

| 查檢項目                                                                     | 自評內容 |          |     |     | 簡述原因<br>( 並檢附佐證資料 )                  |
|--------------------------------------------------------------------------|------|----------|-----|-----|--------------------------------------|
|                                                                          | 符合   | 部分<br>符合 | 不符合 | 不適用 |                                      |
| 4.個人資料蒐集、處理及利用之內部管理程序                                                    |      |          |     |     |                                      |
| 4.9是否提供當事人權利行使管道<br>是否於法定期限內回復當事人？如<br>展延回復，是否依法定要式為之？<br>拒絕當事人時是否有合法事由？ |      |          |     |     | ( 佐證資料如：內部制度文件等)                     |
| 4.10是否主動更正或補充當事人之<br>個人資料？                                               |      |          |     |     | ( 佐證資料如：權利行使之記錄等)                    |
| 4.11是否曾（合法）提供資料予第<br>三人？如提供內容有誤或不備之資<br>料如何通知更正？                         |      |          |     |     | ( 佐證資料如：內部制度文件、評估機制記錄或<br>其他權利行使紀錄等) |
| 4.12特定目的消失或期限屆至時，<br>是否刪除、銷毀、停止蒐集、處理<br>利用個人資料？如否，有無法定事<br>由？            |      |          |     |     | ( 佐證資料如：評估機制記錄或其他內部制度文<br>件等)        |
| 4.13業務終止時是否對個人資料進<br>行妥善、合法之安排？                                          |      |          |     |     | ( 佐證資料如：契約、查核記錄或其他內部制度<br>文件等)       |
| 4.14是否定期檢視個人資料管理之<br>狀況並持續改善？                                            |      |          |     |     | ( 佐證資料如：會議記錄、查核記錄或其他內<br>部制度文件等)     |



# 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）<br>第十九條（無特定目的或特定情況而蒐集、處理資料）<br>第二十條第一項（利用資料逾越特定目的）<br>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）<br>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）<br>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， <b>其情節重大者</b>                                   | 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><br>-> <b>兩罰主義</b>                                       |
| §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。<br>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）



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



# 個人資料管理程序

## 辦法§6

- ◆ 人力供應業者應依據個人資料保護相關法令，定期清查所保有之個人資料，納入本計畫之範圍及建立檔案，並隨時確認法令有無變動。



# 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<br>1.蒐集<br>2.處理<br>3.利用<br>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



# 蒐集或處理個人資料應具備特定目的

修正「電腦處理個人資料保護法之特定目的及個人資料之類別」，並修正名稱為「個人資料保護法之特定目的及個人資料之類別」，定自中華民國101年10月1日生效。

|     |                                                                                   |
|-----|-----------------------------------------------------------------------------------|
| ○○一 | 人身保險                                                                              |
| ○○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) |
| ○○三 | 入出國及移民                                                                            |
| ○○四 | 土地行政                                                                              |
| ○○五 | 工程技術服務業之管理                                                                        |
| ○○六 | 工業行政                                                                              |
| ○○七 | 不動產服務                                                                             |
| ○○八 | 中小企業及其他產業之輔導                                                                      |
| ○○九 | 中央銀行監理業務                                                                          |
| ○一〇 | 公立與私立慈善機構管理                                                                       |
| ○一一 | 公共造產業務                                                                            |
| ○一二 | 公共衛生或傳染病防治                                                                        |
| ○一三 | 公共關係                                                                              |
| ○一四 | 公職人員財產申報、利益衝突迴避及政治獻金業務                                                            |
| ○一五 | 戶政                                                                                |
| ○一六 | 文化行政                                                                              |



# 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<br>編號 | 作業<br>流程<br>名稱 | 個資行為態樣<br>1.蒐集<br>2.處理<br>3.利用<br>4.國際<br>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<br>刪除銷燬 |          |          |          | 數量 |
|          |                |                                              | 檔案<br>名稱 | 種類<br>及類別 | 類型 | 方式   | 特定<br>目的 | 法定<br>情形 | 來源    | 特定<br>目的 | 法定<br>情形 | 告知<br>與否 | 免告知<br>之法定<br>事由 | 有無    | 委託者<br>或<br>受託者 | 資料<br>載體      | 儲放<br>場所 | 保存<br>期限 | 刪除<br>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<br>編號 | 作業<br>流程<br>名稱 | 個資行為態樣<br>1.蒐集<br>2.處理<br>3.利用<br>4.國際<br>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<br>刪除銷燬 |          |          |          | 數量 |
|          |                |                                              | 檔案<br>名稱 | 種類<br>及類別 | 類型 | 方式   | 特定<br>目的 | 法定<br>情形 | 來源    | 特定<br>目的 | 法定<br>情形 | 告知<br>與否 | 免告知<br>之法定<br>事由 | 有無    | 委託者<br>或<br>受託者 | 資料<br>載體      | 儲放<br>場所 | 保存<br>期限 | 刪除<br>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



# 人才招募流程個資盤點表範例

| 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<br>1. 蒐集<br>2. 處理<br>3. 利用<br>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   |         |     |
| 1    | 人才招募   | 1.2.3.                                       | 104履歷 | 姓名、聯絡方式、學歷等 | 紙本電子檔    |      |      |      | 104網站 | 人才招募 | 契約   | 網頁告知  |          |       | 無       |           | 紙本與電子檔 | 上鎖櫃個人電腦    | 自訂10年  | 期限後刪除銷毀 | 100 |
| 2    | 人才招募   | 1.2.3.                                       | 履歷    | 姓名、聯絡方式、學歷等 | 紙本電子檔    | 紙本蒐集 | 人才招募 | 契約   |       |      |      | 紙本告知  |          |       | 無       |           | 紙本與電子檔 | 上鎖櫃個人電腦    | 自訂10年  | 期限後刪除銷毀 | 100 |
| 3    | 人才招募   | 1.2.3.                                       | 員工資料表 | 姓名、聯絡方式、學歷等 | 紙本電子檔資料庫 | 紙本蒐集 | 雇用契約 | 契約   |       |      |      | 紙本告知  |          |       | 無       |           | 紙本與電子檔 | 上鎖櫃個人電腦資料庫 | 系統存續期間 | 期限後刪除銷毀 | 200 |



# 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<br>(可複選)<br>1.蒐集<br>2.處理<br>3.利用<br>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<br>(概數) |
|------|--------|---------------------------------------------------|-------|---------------|--------------------------------------|------|------|------|------|------|------|------|---------|-------|---------|-----------|------|------------------------------|---------|------------|
|      |        |                                                   | 檔案名稱  | 種類及類別         | 類型<br>1.紙本<br>2.電子檔<br>3.資料庫<br>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<br>1.法定<br>2.自訂<br>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<br>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<br>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

| 查檢項目                                                          | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                                |
|---------------------------------------------------------------|------|------|-----|-----|--------------------------------------------------------|
|                                                               | 符合   | 部分符合 | 不符合 | 不適用 |                                                        |
| 1.個人資料保護規劃                                                    |      |      |     |     |                                                        |
| 1.1是否指定專人或專責單位，負責辦理個人資料保護管理政策之研議、認知宣導與教育訓練、資料與設備安全管理、稽核等工作事項？ |      |      |     |     | ( 佐證資料如：企業組織圖，得以看出個資專責人員配置、會議記錄、教育訓練規劃、資安管理程序文件、稽核計畫 ) |
| 1.2是否有個人資料管理人員組織配置？並依分工執行？                                    |      |      |     |     | ( 佐證資料如：個資成員組織圖)                                       |
| 1.3是否有個人資料保護管理政策是否公告公司人員周知？                                   |      |      |     |     | ( 佐證資料如：政策文件等)                                         |
| 1.4就個人資料之蒐集、處理及利用是否有相關程序規定？是否公告公司人員周知？                        |      |      |     |     | ( 佐證資料如：內部程序文件、佈達證據等)                                  |
| 1.5是否進行個人資料盤點並備有清冊？盤點之方式為何？結果之正確性？                            |      |      |     |     | ( 佐證資料如：個資盤點清冊、稽核紀錄等)                                  |



# 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



# 個人資料管理程序

## 辦法§7

- ◆ 人力供應業者應依據前條所界定之範圍，分析蒐集、處理及利用過程中可能產生之風險，並依據分析結果，訂定適當管控措施。



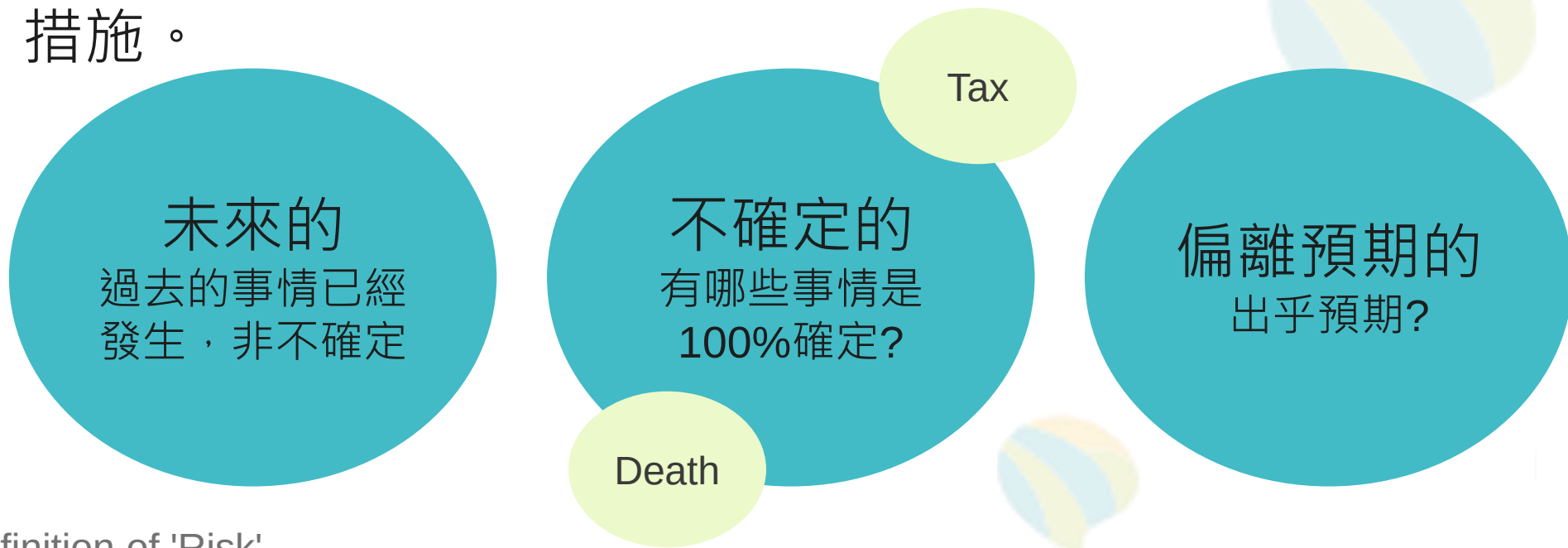
# 因應風險之規劃

- 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

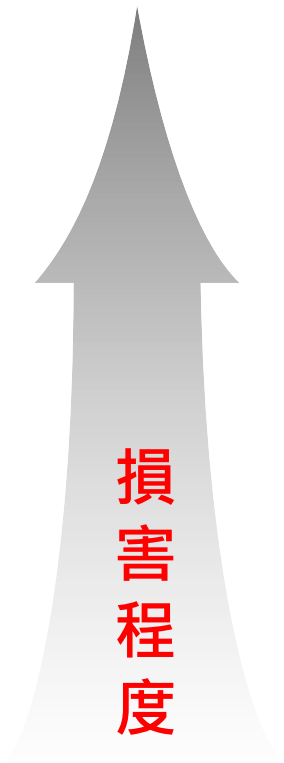
如某公司個資風險之分析進行方式包含：

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



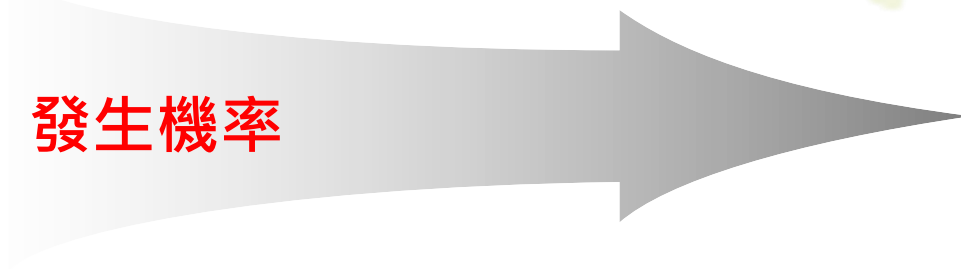
例：目的外利用



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。<br>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。<br>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            |    |      |
| 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 | 備註 | 單位名稱 |
|                |          | 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 |



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



# 自評表

| 查檢項目                                   | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                               |
|----------------------------------------|------|------|-----|-----|-------------------------------------------------------|
|                                        | 符合   | 部分符合 | 不符合 | 不適用 |                                                       |
| 2.個人資料之風險評估及管理機制                       |      |      |     |     |                                                       |
| 2.1是否進行個人資料風險評估並進行相應處理？風險評估之方式？結果之正確性？ |      |      |     |     | ( 佐證資料如：風險評估表，可分辨出資產價值，以便採取適當的避險措施；風險評鑑表，包含風險識別與風險預估) |
| 2.2是否訂定風險處理計畫，並根據該計畫導入控制措施，以降低風險？      |      |      |     |     | ( 佐證資料如：風險處理計畫、區分風險分級等)                               |





# 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



# 個人資料管理程序

## 辦法§9

- ◆ 人力供應業者應定期對所屬人員施以基礎認知宣導或專業教育訓練，使其瞭解個人資料保護相關法令規定、責任範圍、管理措施或方法。



# 教育訓練

- 原則
  - 組織應以適當方式確保組織人員對個人資料管理、管理與獎懲制度具有正確的認知及能力。
- 基本教育訓練
  - 組織針對組織人員應提供必要的個人資料管理教育訓練。
- 權責人員教育訓練
  - 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。
- 成果維持及改善措施
  - 組織應針對組織人員教育訓練成果建立紀錄與持續改善機制。



# 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

| 查檢項目                                | 自評內容 |      |     |     | 簡述原因<br>( <u>並檢附佐證資料</u> )                  |
|-------------------------------------|------|------|-----|-----|---------------------------------------------|
|                                     | 符合   | 部分符合 | 不符合 | 不適用 |                                             |
| 6.認知宣導及教育訓練                         |      |      |     |     |                                             |
| 6.1 管理階層是否有要求員工，依照公司訂定之政策及程序施行安全事宜？ |      |      |     |     | ( 佐證資料如：個人資料檔案安全維護計畫)                       |
| 6.2 是否對所有員工提供個人資料保護認知宣導及教育訓練？       |      |      |     |     | ( 佐證資料如：訓練記錄及其他內部制度文件等，應能呈現教育訓練主題、對象、頻率等資訊) |





# 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



# 個人資料管理程序

## 辦法§24

- ◆ 人力供應業者執行本計畫各項程序及措施，應保存下列紀錄五年：
  - 因應事故發生所採取之行為。
  - 受託者執行委託人要求之事項。
  - 提供當事人行使之權利。
  - 個人資料之維護及修正。
  - 所屬人員權限之異動。
  - 所屬人員違反權限之行為。
  - 備份及還原之測試。
  - 個人資料之交付及傳輸。
  - 個人資料之刪除、銷毀或移轉。
  - 存取個人資料者之資訊。
  - 定期檢查處理個人資料之資訊。
  - 教育訓練。
  - 計畫稽核及改善措施之執行。



# 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

| 查檢項目                                                                                                                                                            | 自評內容 |      |     |     | 簡述原因 ( <u>並檢附佐證資料</u> )                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|-----|-----|----------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                 | 符合   | 部分符合 | 不符合 | 不適用 |                                                                                                          |
| 7.紀錄機制                                                                                                                                                          |      |      |     |     |                                                                                                          |
| 7.1是否保存「因應事故發生所採取之行為、受託者執行委託人要求之事項、提供當事人行使之權利、個人資料之維護及修正、所屬人員權限之異動、所屬人員違反權限之行為、備份及還原之測試、個人資料之交付及傳輸、個人資料之刪除銷毀或移轉、存取個人資料者之資訊、定期檢查處理個人資料之資訊教育訓練、計畫稽核及改善措施之執行紀錄」5年？ |      |      |     |     | ( 佐證資料如：紙本部分-存取及利用紀錄、調閱紀錄、軌跡資料、銷毀紀錄;Log Files保存-包含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、EDR偵測回應紀錄、第三方鑑識分析報告 ) |



# 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



# 個人資料管理程序

## 辦法§8

- ◆ 人力供應業者為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應建立下列機制：
  - 採取適當應變措施，以控制事故對當事人之損害。
  - 查明事故狀況，並以適當方式通知當事人相關事故事實、因應措施及諮詢服務專線等。
  - 檢討預防機制，避免類似事故再次發生。
- ◆ 人力供應業者發現前項事故時，應於**七十二小時**內填具通報紀錄表（如附表），通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關；中央目的事業主管機關或直轄市、縣（市）政府接獲通報後，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。



# 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。



# 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              | <input type="checkbox"/> 竊取<br><input type="checkbox"/> 洩漏<br><input type="checkbox"/> 竄改<br><input type="checkbox"/> 毀損<br><input type="checkbox"/> 滅失<br><input type="checkbox"/> 其他侵害 事故 | 個資侵害之總筆數<br>(大約) _____ 筆                                                       |
|                     |                                                                                                                                                                                             | <input type="checkbox"/> 一般個資 _____ 筆<br><input type="checkbox"/> 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 | <input type="checkbox"/> 是 <input type="checkbox"/> 否，理由                                                                                                                                    |                                                                                |



# 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

| 查檢項目                                                         | 自評內容 |      |     |     | 簡述原因<br>( <u>並檢附佐證資料</u> )                           |
|--------------------------------------------------------------|------|------|-----|-----|------------------------------------------------------|
|                                                              | 符合   | 部分符合 | 不符合 | 不適用 |                                                      |
| 3.個人資料事故之預防、通報及應變機制                                          |      |      |     |     |                                                      |
| 3.1針對個人資料事故是否有可行之應變機制？                                       |      |      |     |     | ( 佐證資料如：個人資料事故通報與應變程序書或個人資料檔案安全維護計畫，事故發生時，是否訂定應變機制等) |
| 3.2發生個人資料事故時，是否適時以適當方式通知當事人相關事故事實、因應措施及諮詢服務專線等？              |      |      |     |     | 當年度無事故者，3.2-3.4應填不適用 ( 佐證資料如：通報單等)                   |
| 3.3是否訂有檢討預防機制，避免類似事故再次發生？                                    |      |      |     |     | ( 佐證資料如：說明所採預防措施等)                                   |
| 3.4發現個人資料事故時，是否於72小時內填具通報紀錄表，通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關？ |      |      |     |     | ( 佐證資料如：通報紀錄等)                                       |



# 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



# 個人資料管理程序

## 辦法§25

- ◆ 人力供應業者應定期檢查本計畫執行情形，並建立未落實執行之改善措施。



# 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。



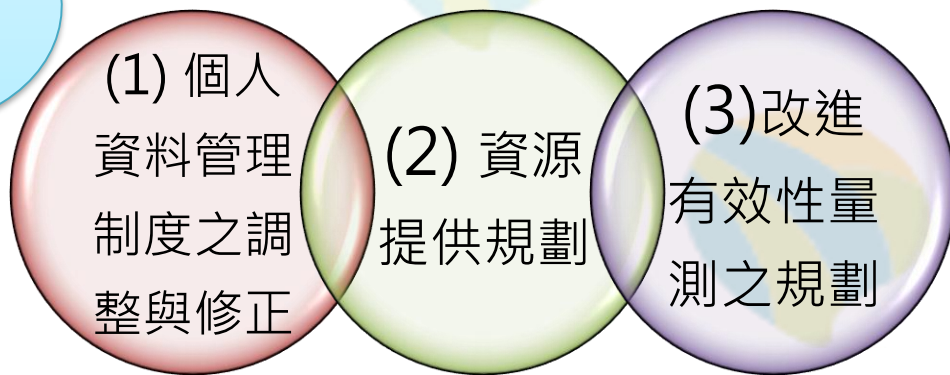
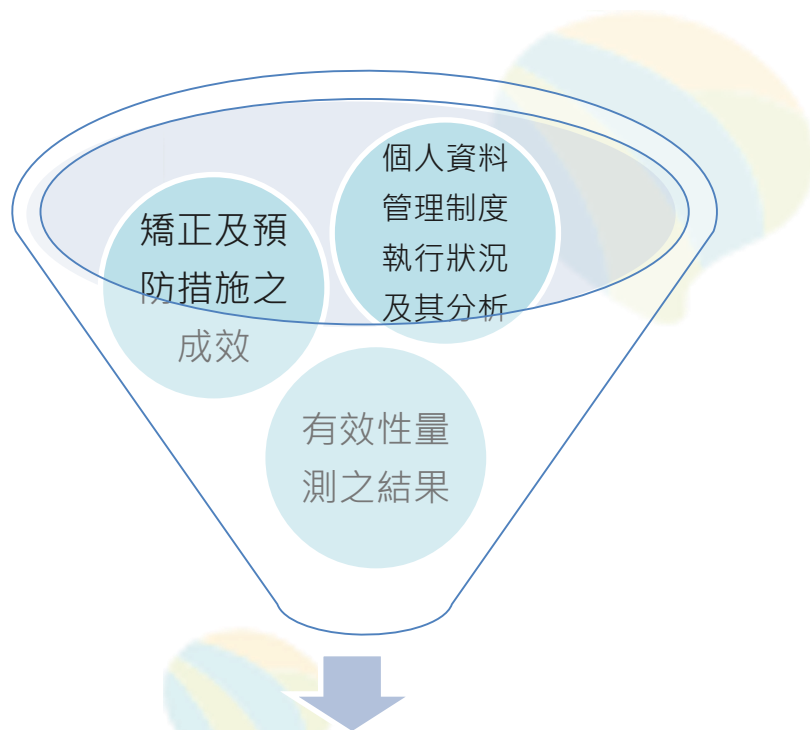
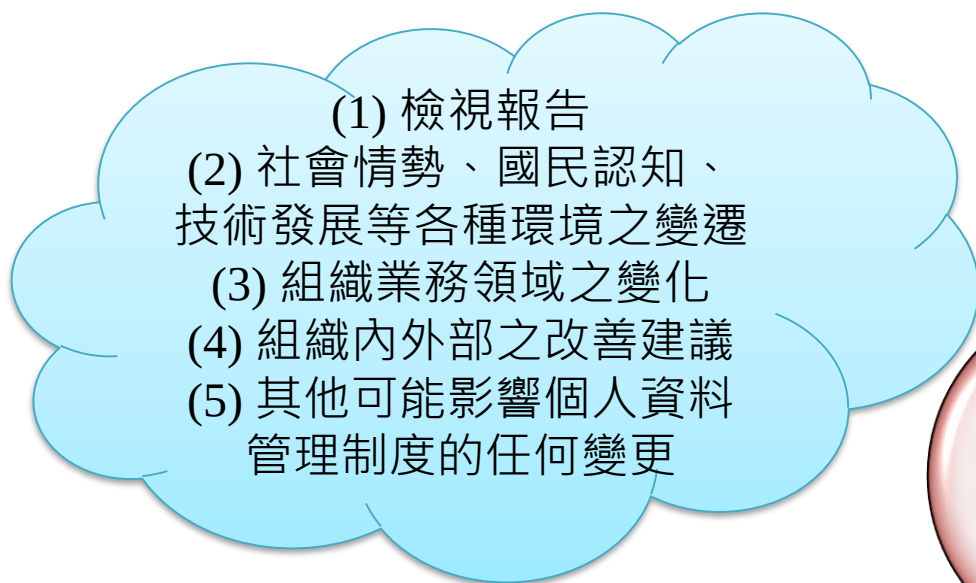
# 內部評量

- 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。
- 內部評量計畫應由具備個人資料內評師或個人資料驗證師資格者規劃，並由其確保內部評量執行之有效性與出具內部評量報告。



# 定期檢視

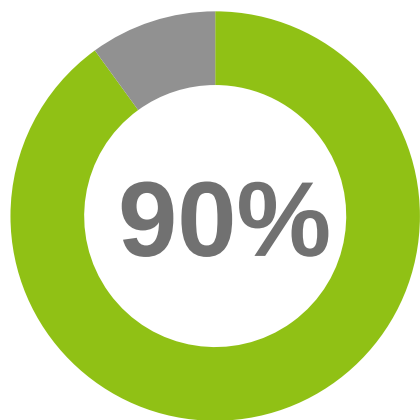
每年定期開會，召集相關權責人員，檢視個人資料保護管理制度，將檢視結果以書面紀錄，並報告最高管理階層。





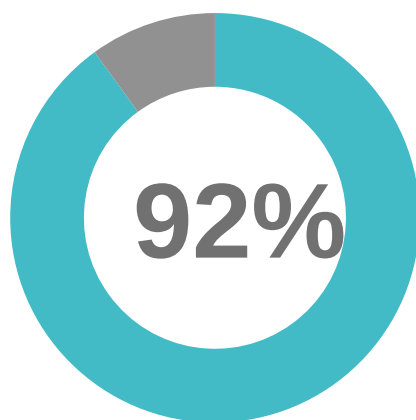
# 投資隱私的整體價值

個資管理能力為  
爭取消費者信賴關鍵



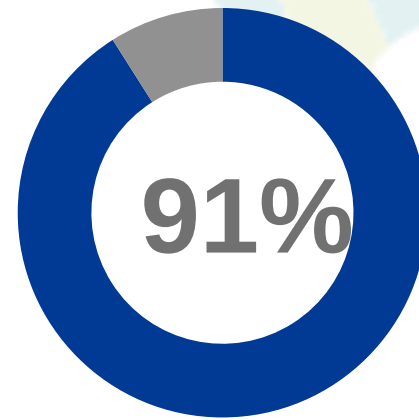
**90%**消費者認為，若無法信賴企業具有妥善管理個資的能力，即無意願購買其商品或服務。

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。

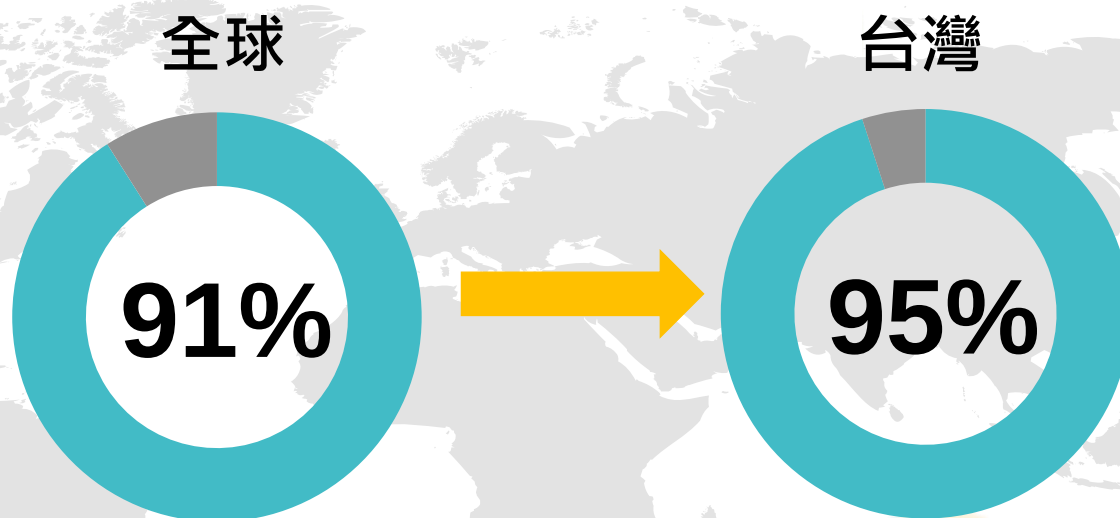
資料來源：

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 | <ul style="list-style-type: none"> <li>● 唯一依照我國個人資料保護法為基礎設計</li> <li>● 銜接 APEC CBPR 國際要求</li> </ul> | ● 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：<br>ISO27001、<br>ISO27002、<br>ISO29100 |
| 所涉法令標準 | 國際法                      | 我國個資法                                                                                               | GDPR              | 國際標準              | 國際標準                                      |





# 首先，讓我們來了解什麼是TPIPAS



## TPIPAS

臺灣個人資料保護與管理制度



導入TPIPAS—培訓內部人才



dp.mark  
資料隱私保護標章

驗證—取得標章



## 唯一政府建置及推動的 個資保護制度

2010年

為完善國內商務交易安全環境，在經濟部商業司的委託下，資策會科技法律研究所(科法所)自起建置及推動「臺灣個人資料保護與管理制度」(TPIPAS)。

2017年

受經濟部委託，資策會持續擴大維運dp.mark資料隱私標章。

2019年

資策會辦理TPIPAS十年有成，受國發會青睞及力薦，於2019年7月指定**資策會以TPIPAS為基礎，向APEC提出當責任機構**(Accountability Agent, AA)。

2021年

資策會**獲准成為亞太經濟合作跨境隱私規則體系當責機構**。我國成為第5個擁有當責機構的APEC會員體。

2022年

TPIPAS個資業務移轉至**數位發展部(數位部)**，資策會持續提供個資驗證服務。



# TPIPAS個資保護管理制度特色



經濟部商業司劉雅娟副司長(中)擔任頒證人，親自頒發TPIPAS績優廠商獎座。

## 個資人才培育

定期辦理個資證照課程，及個資隱私講座掌握趨勢。

## 個資管理制度驗證

可依公司需求，選擇組織全領域或特定範圍驗證。

## 以臺灣個資法量身訂做

唯一以臺灣個資法為基礎設計，最符合臺灣法規要求。

## 導入最具成本效益

依據組織規模規畫導入所需人力及成本，最大化臺灣企業導入成本效益。

## 唯一政府認證標章

臺灣唯一由政府推動的個人資料管理制度。驗證通過可獲頒數位部「資料隱私保護標章」。



# TPIPAS 驗證流程四階段

TPIPAS 驗證係指以臺灣個人資料保護與管理制度規範為驗證標準，對組織所進行之驗證。TPIPAS 維運機構已將 TPIPAS 驗證委外給外部驗證機構。

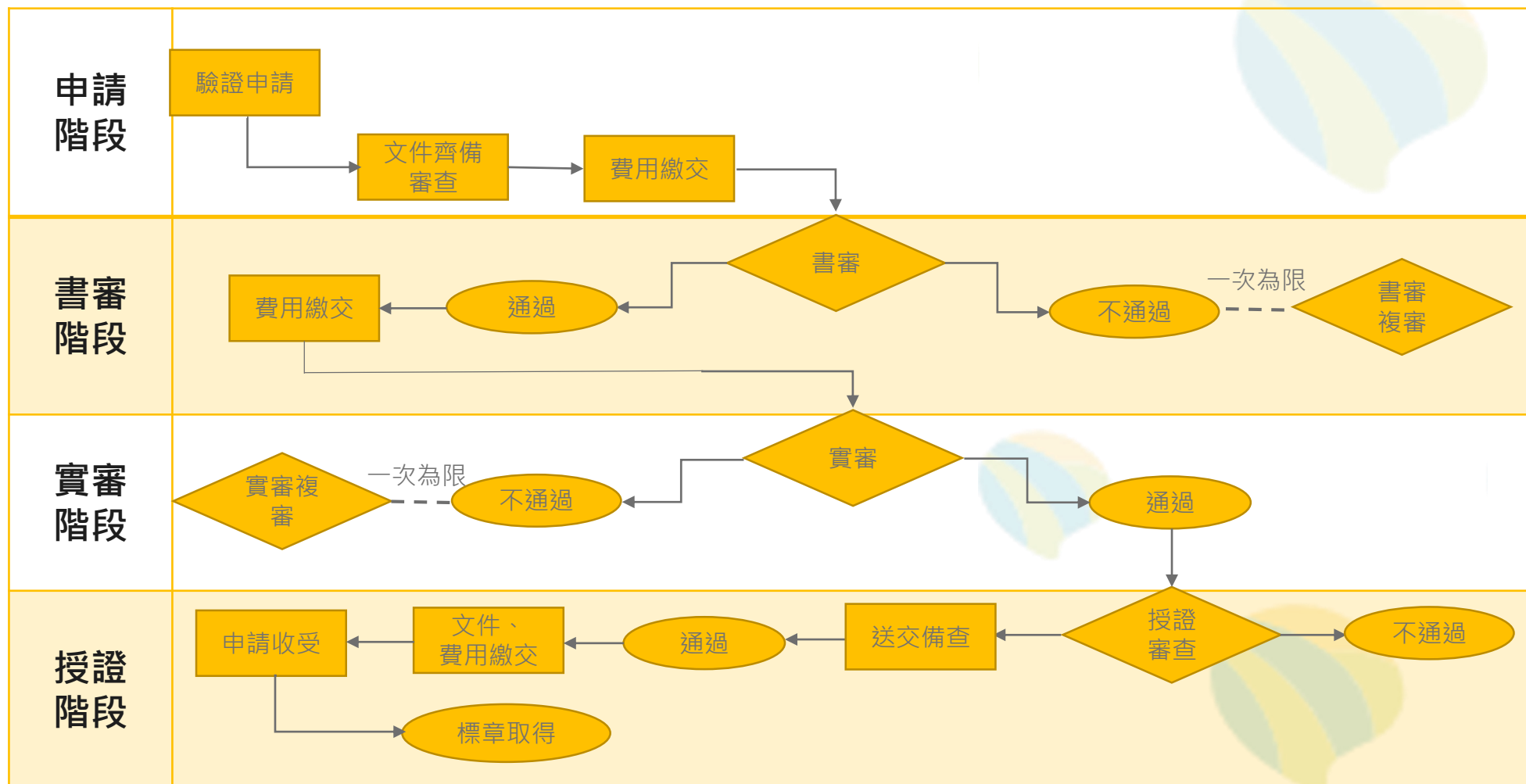
驗證流程主要分4階段：申請、書審、實審、授證階段。

1. **申請階段**：申請組織向TPIPAS維運機構提出申請文件並完成費用繳納，TPIPAS維運機構將文件交付予外部驗證機構進行審查後，接續將由外部驗證機構開始進行TPIPAS驗證。
2. **書審階段**：書審係TPIPAS驗證首要程序，外部驗證機構審查組織內部文件，書審通過，方可續進入實審。
3. **實審階段**：實審係TPIPAS驗證時外部驗證機構實地造訪組織進行訪談、觀察、抽樣。
4. **授證階段**：通過實審之組織，待TPIPAS維運機構進行授證審查，確認符合授證資格後，即可取得標章使用資格。



# TPIPAS 驗證流程

## • 驗證流程圖





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

