個人資料去識別化之法令及實務問題

林其樺 專案經理

資策會服創所金融科技創新中心 | FinTech Space

2020.12.4

ariellin@iii.org.tw
www.iii.org.tw
https://www.fintechspace.com.tw/

大綱

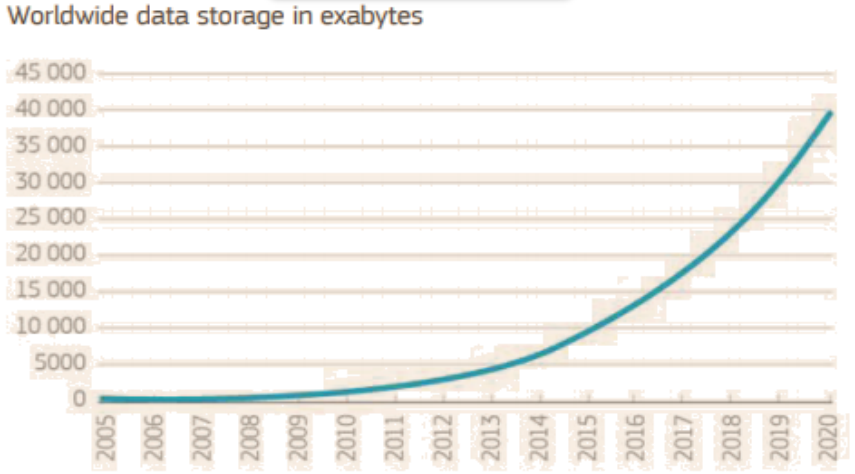
- 01 國際趨勢—資料經濟驅動數位發展
- 02 我國個資去識別化規範及實務現況
- 03 個資去識別化管理機制分享

01 | 03

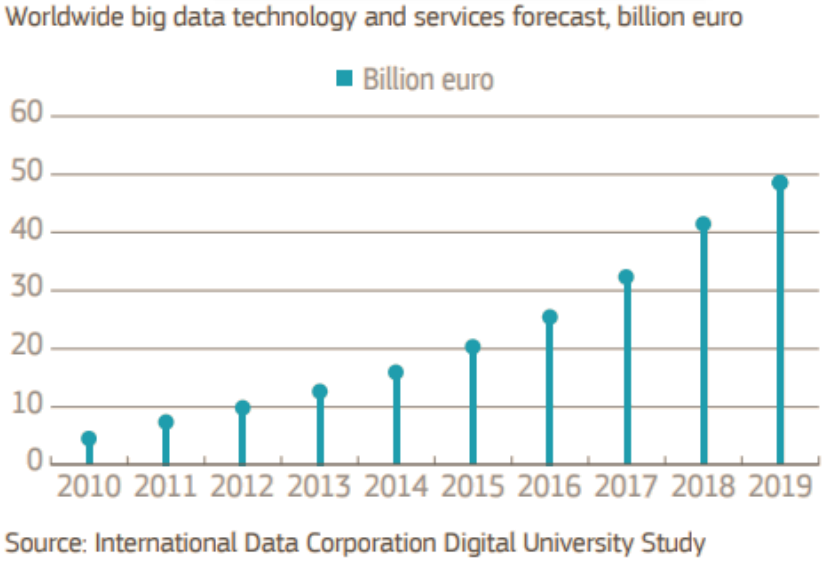
國際趨勢—資料經濟驅動數位發展

資料的經濟效益有多少？

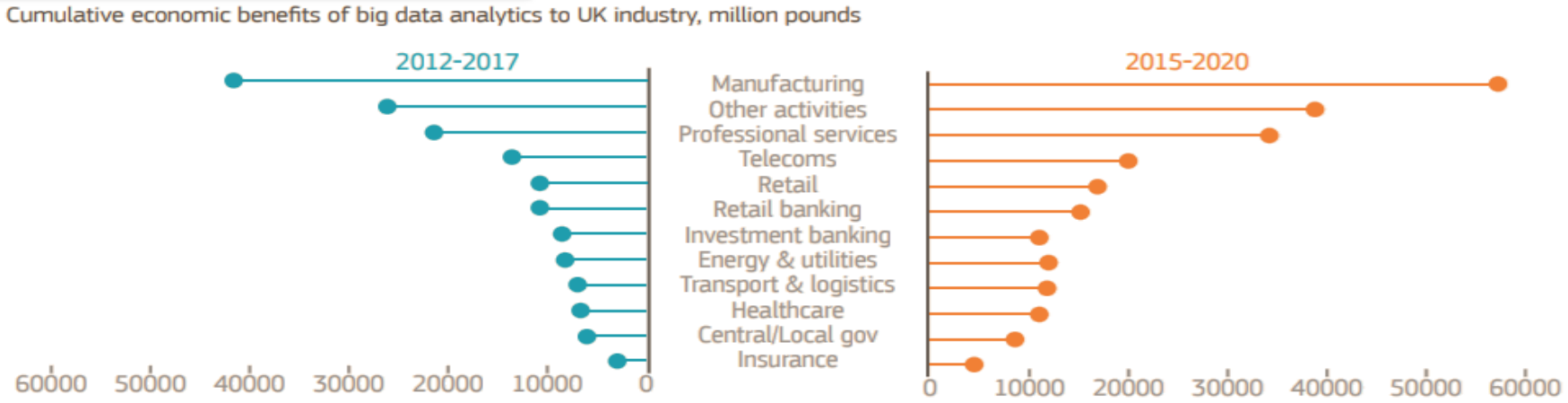
全球資料量



資料的經濟效益



愈來愈多行業擁抱資料金礦



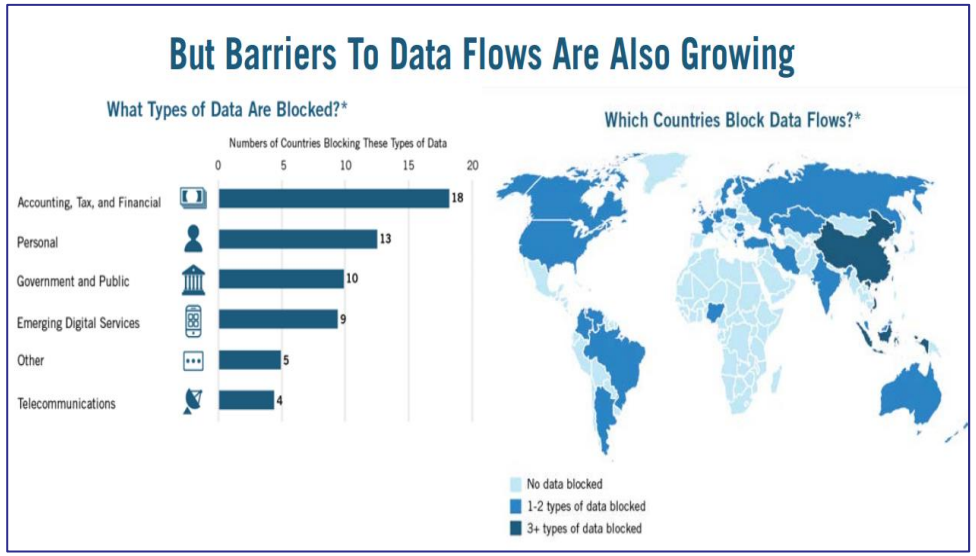
Source: SAS & Centre for Economics and Business Research Ltd, 2016

國際對跨境資料流通及限制需求互有消長

資料流通促成經濟與科技及產業發展

國家對資料流通設限之狀況也日益增加

- McKinsey：傳產經濟效益約75%來自網路上的資料流通
- 2014年資料跨境流通於全球經濟貢獻2.8兆美元，麥肯錫預估2025年將達11兆美元



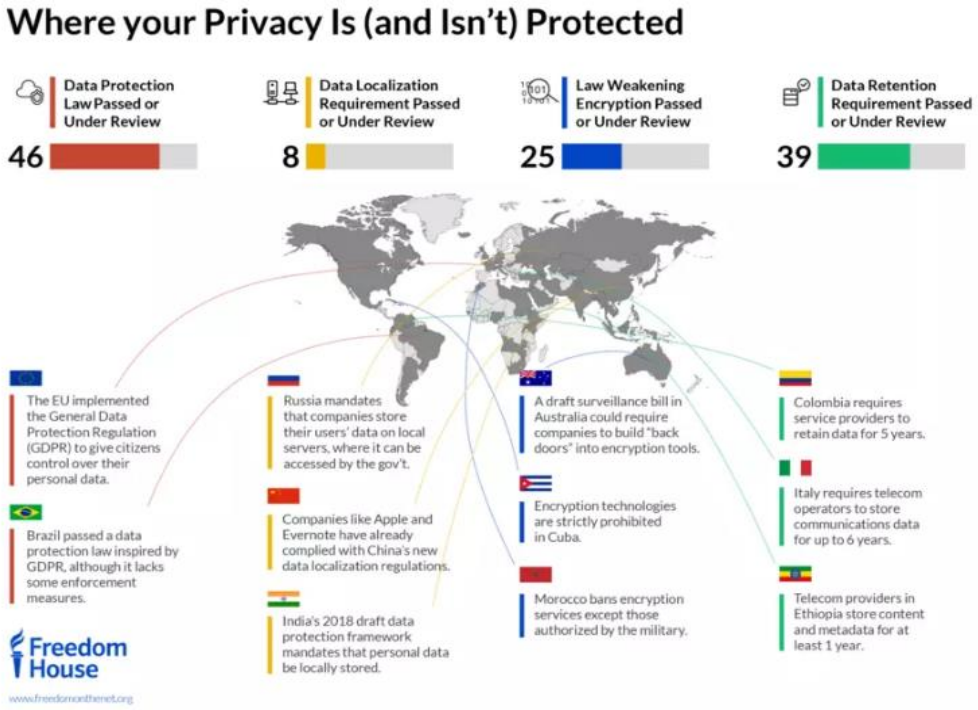
資料來源：ITIF, Cross-Border Data Flows, 2018.5 https://itif.org/publications/2018/05/03/cross-border-data-flows (last visited: March 13, 2020)

未來資料政策發展趨勢

世界經濟論壇歸納5趨勢

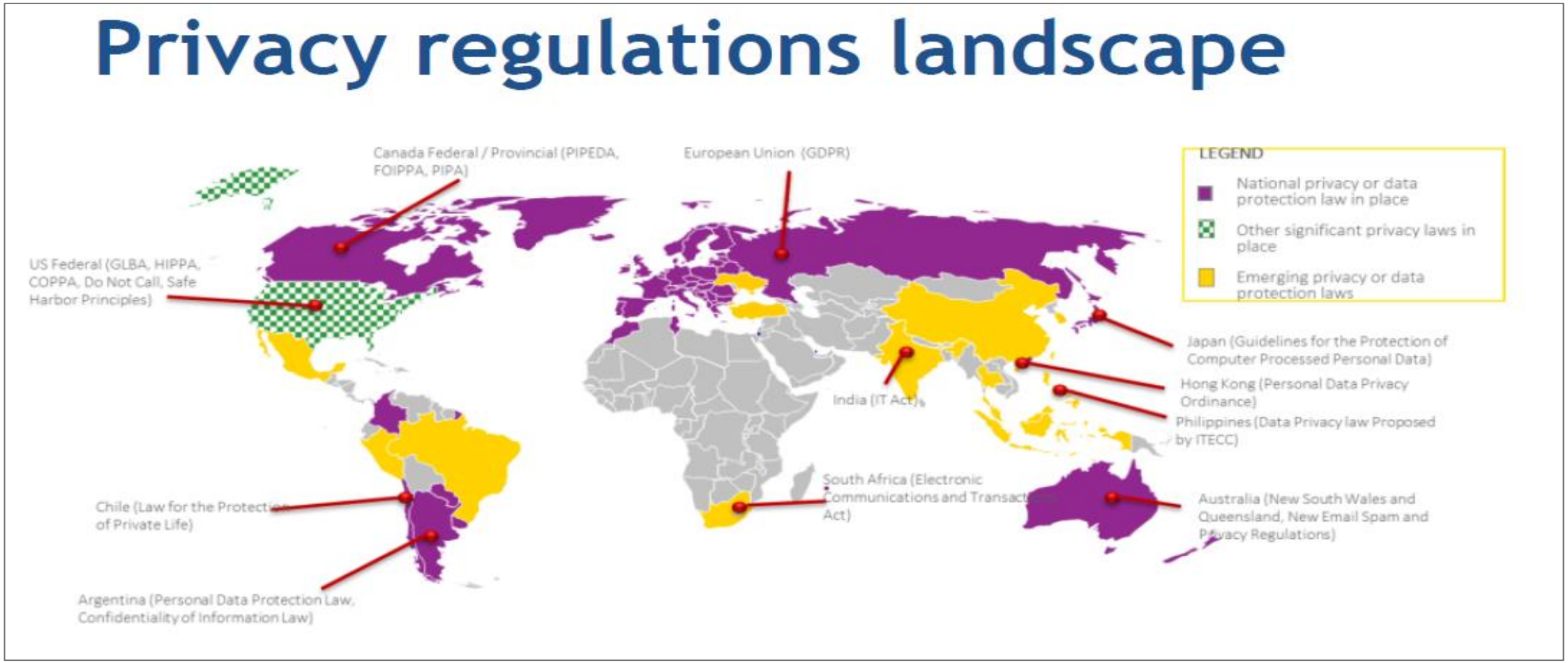
- 將由巨型平台掌握資料
- 用戶資料自主空間將提升
- **創新鼓勵資料分享**
- 協議促進資料分享、交換
- **政府提升資料管制力道**

國際上目前嚴格要求資料在地儲存/處理之國家計8國



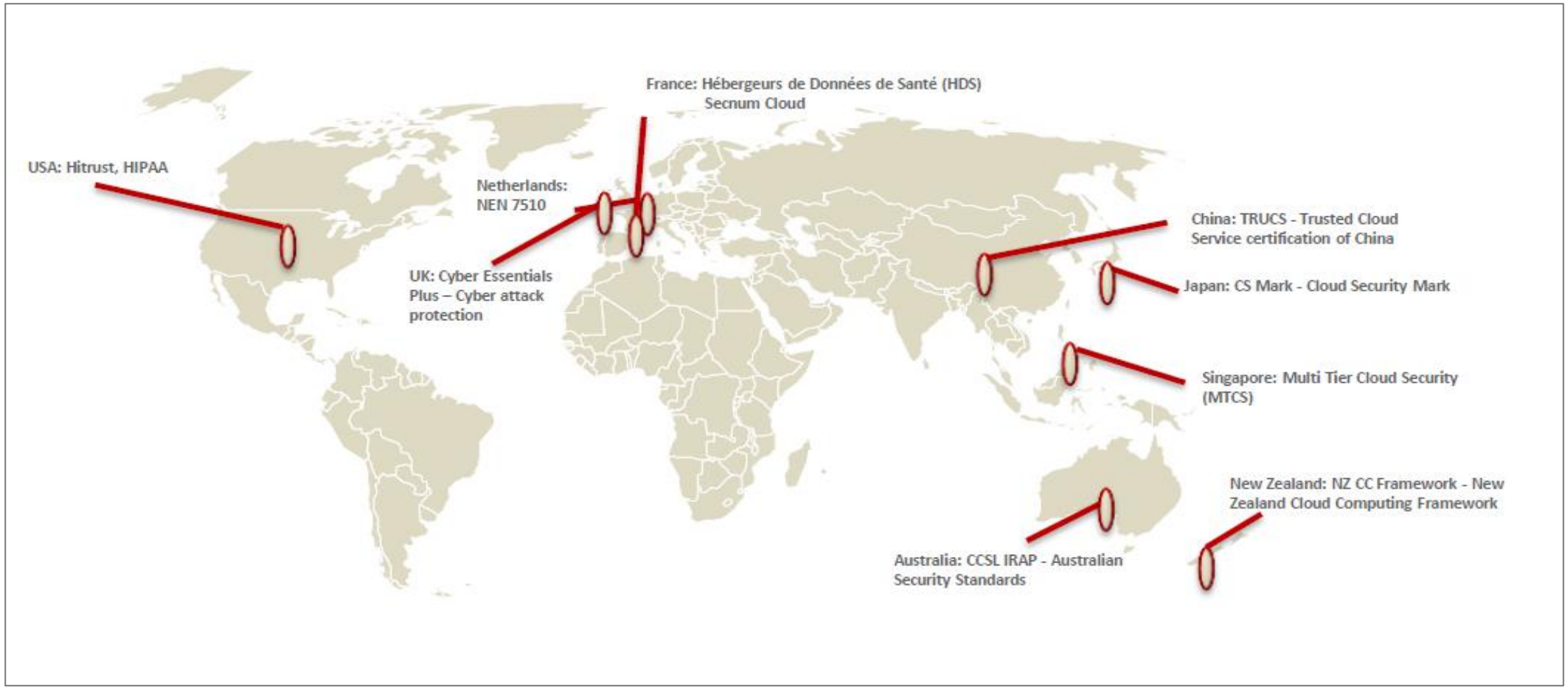
資料來源：WEF, It's time to redefine how data is governed, controlled and shared. Here's how, 2020.1 https://www.weforum.org/agenda/2020/01/future-of-data-protect-and-regulation/ (last visited: April 6, 2020)

全球隱私規範



Source: IAPP Europe Data Protection Congress 2019

全球隱私及安全標準



Source: IAPP Europe Data Protection Congress 2019

重要國家資料活用概況
共通痛點：資料創新受阻/法規不明確

EU

依據	• 一般資料保護規則(GDPR)
活用方式	• **資料可攜、近用**：機器可讀、並可以轉移到其他服務
資料	• 如當事人主動提供、統計資料

英國

依據	• **Midata** (企業與規制改革法案) • 資料保護法
活用方式	• **資料可攜、近用**：機器可讀、並可以轉移到其他服務
資料	• 如能源、手機、信用卡、供應商所保有資料

美國

依據	• **Smart Disclosure**(Blue Button、Green Button、Get Transcript, etc.)(依各領域規範)
活用方式	• **資料近用、自主**
資料	• 依各領域規範而定(如金融：金融商品、交易紀錄等)

日本

依據	• 依各領域規範(如金融：銀行法考慮修正**開放API**)
活用方式	• 金融：當事人透過電支等代理商確保**資訊自主**
資料	• 金融：餘額查詢、卡費、付款明細等

資料來源：經產省，データ利活用とデジタルガバナンス，2019年3月 (最後瀏覽日：2020年5月3日)

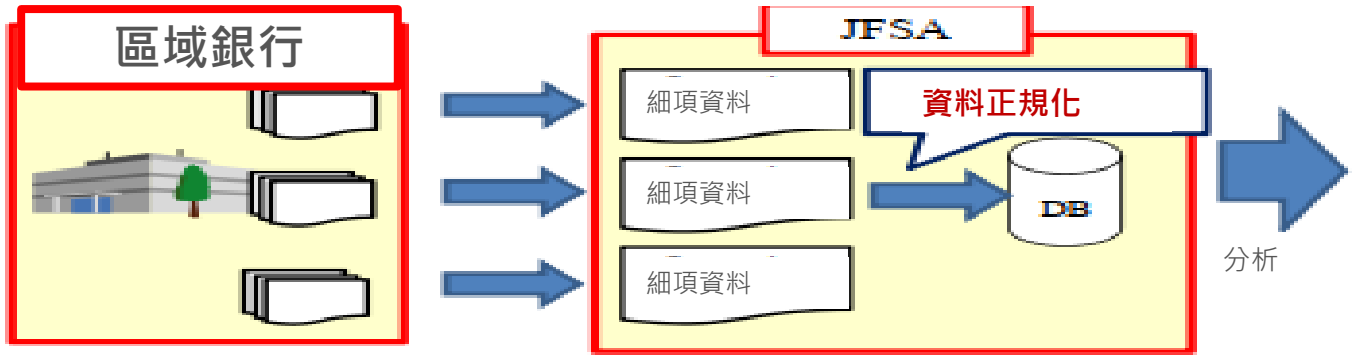
日本金融廳之監理數位化轉型
資料活化擘劃金融科技生態系

金融廳2019年開始推動數位監理PoC：

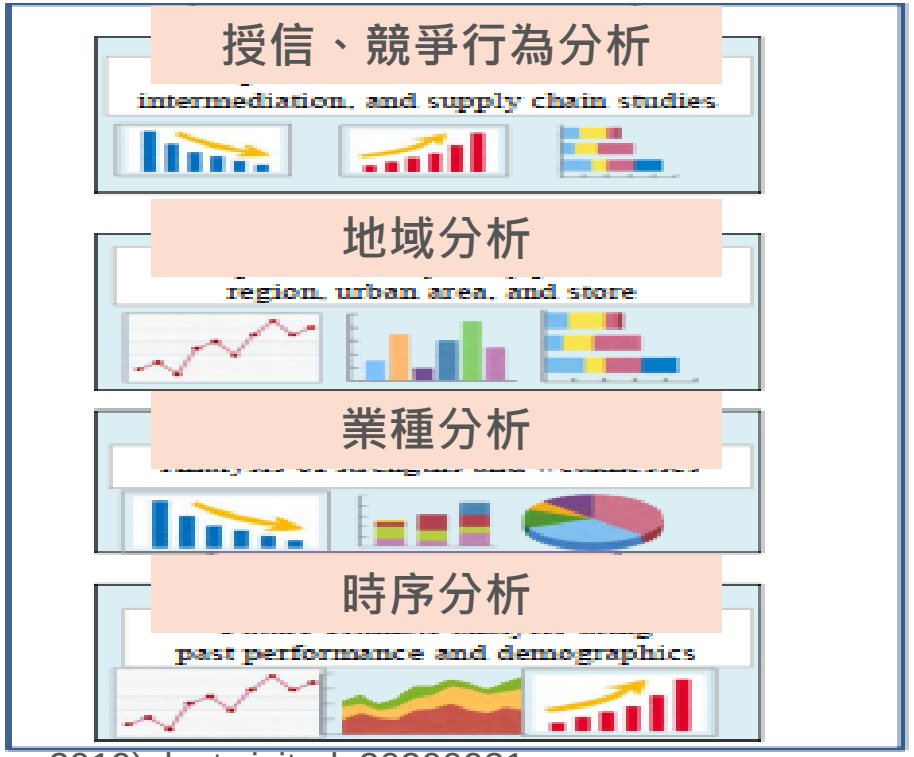
【優化**金融監理**流程】
- 金融廳主導銀行資料集中化
- 流程機器人(RPA)

【提升**數據分析**效益】
- 資料活化
- 金融科技生態系

【日本銀行資料交換及活化PoC】



此PoC驗證之細項資料為「企業融資」、「投資信託」



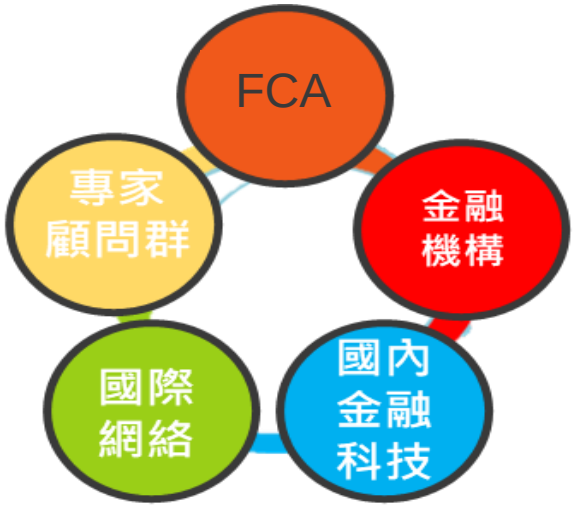
Ref.：JFSA, Status of digitalization efforts in financial monitoring (June 2019), last visited: 20200921

英國金融主管機關主導TechSprint 目前致力於傳遞數據價值

英國FCA自2016年始，發展TechSprint共創機制，由主管機關提出主題，邀集產官學創跨域專家，每年舉辦兩次TechSprint活動，共同協作金融監理數位化與未來數位風險探索。

FCA定主題	參與對象邀集	舉辦方式	預期產出	數位監理試行

- 重點政策推動
- 業務痛點解決
- 數位科技/流程探索



國際網絡

GFIN GLOBAL FINANCIAL INNOVATION NETWORK

黑客松

焦點訪談

工作坊

高 → 成熟度 → 低

第一類: 創新解決方案招募

AML+防詐欺(5^{th}, 7^{th}+GFIN)

養老金投資普惠化(6^{th})

第二類:技術規格/白皮書

監理申報自動化(4^{th})

第三類:雛形實作

監管申報自動化(2^{nd})

Consumer Access(1^{st})

第四類: 概念驗證

改善勞工心理健康(3^{rd})

2020 → 階段 → 2018

第三階段：傳遞數據價值
- 資料標準化
- 改善法規解釋、實施及執行

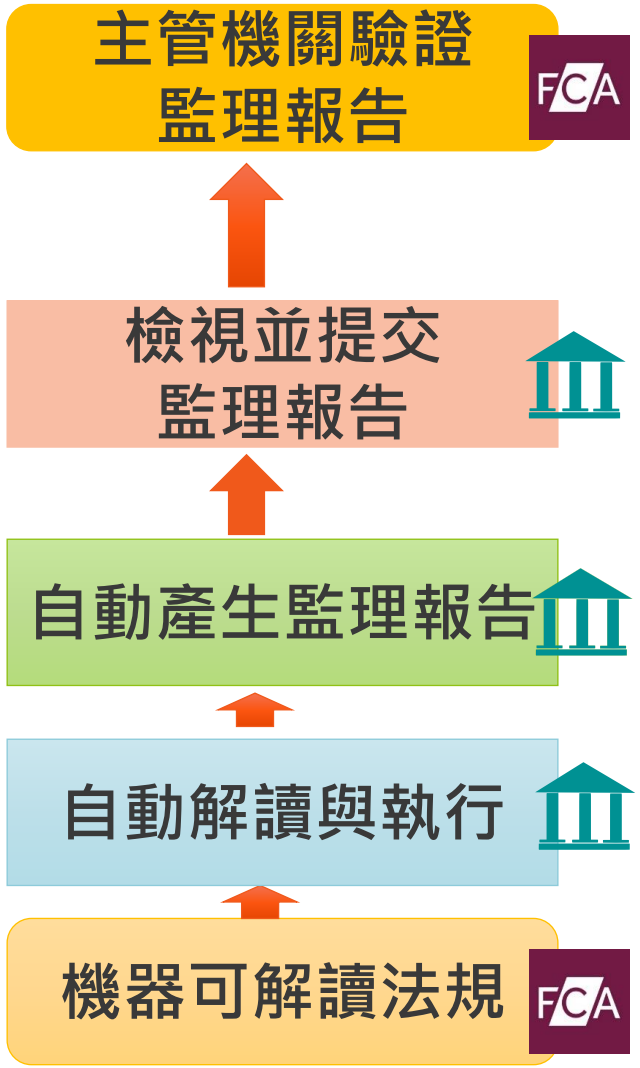
第二階段：可行性評估
- 業務情境建模

第一階段：DRR建構
- 法規轉換為程式碼
- 提供監理機構可靠數據

英國TechSprint階段性推動透過技術建構金融科技生態系

FCA 2020資料策略

數據價值轉化	**規範性作業** **分析結果** **資料分析平台**
分析人力 資料處理 分析框架	**能力建構** **FCA資料操作模型、樞紐** 資料、分析節點 ⟳ 資料服務單位(DSU) 商業及科技解決方案、人力資源、安全
資料管理	**資料服務** 治理 | 品質 | 來源 | 共享 | 政策及標準
基礎建設 (平台及工具)	**資料管理及分析工具** 資料管理 | 分析平台 | 標準化服務 | 視覺化 **核心科技平台** 資料蒐集 | 資料儲存及回報 | 通知 | 發布



Ref.：FCA, Data Strategy, https://www.fca.org.uk/publications/corporate-documents/data-strategy, last visited: 20200918

二、我國金融科技發展挑戰及機會
金管會鼓勵負責任創新

2020年金管會發布3年期「金融科技發展路徑圖」

(一) 強化金管會創新中心作為議題溝通窗口及跨部會合作之平台，協助業者解決共通性議題，並由周邊單位協力設置金融科技共創平台，協助推動金融科技發展事項

(二) 調適數位金融相關法令，因應跨業跨域及場景金融之發展

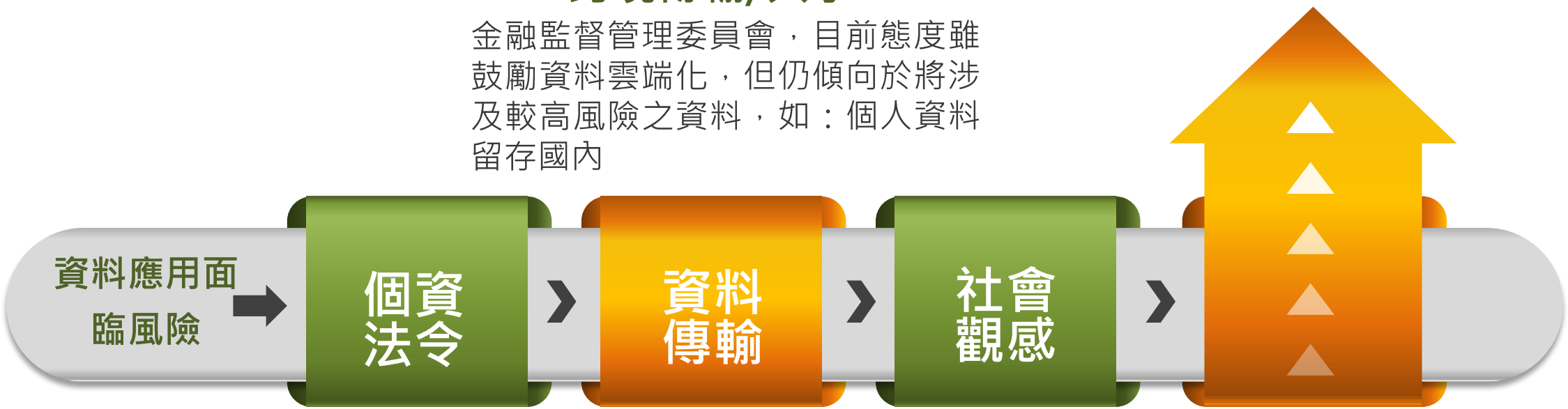
(三) 整合政府與民間資源，共同創造數據價值及提供貼近消費者需求的金融服務

(四) 研議推廣金融科技證照，提升市場整體研發應用之量能

加速推動「開放銀行」；建立與第三方服務機構合作資訊揭露制度；訂定金控轄下子公司客戶資料共享之相關機制與規範；訂定金融市場跨機構間客戶資料共享之相關機制與規範；訂定跨市場客戶資料共享之相關機制與規範

資料應用面臨風險

資料應用上
應優先針對個人資料
有所評估與因應措施



跨境傳輸/共享

金融監督管理委員會，目前態度雖鼓勵資料雲端化，但仍傾向於將涉及較高風險之資料，如：個人資料留存國內

個資法令

公司將保有資料全部進行加值利用、數據剖析或統計分析等，我國個資法令所要求之特定目的、保有依據及其告知內容是否均已齊備

社會觀感

目前民眾之權利意識抬頭，加上媒體渲染，容易造成公司經營或商譽風險，如何降低社會疑慮亦為風險因子

02 | 03

我國個資去識別化規範及實務現況

個資去識別化目的

A

降低資料機敏性

將個人資料去識別化成為單純數據資料，而無法識別至特定人之情形下，資料機敏性即大幅度降低，同時，亦促使減少我國個資法令之拘束性，同時減少資料集中後，遭受攻擊所需承受之衝擊

B

信賴環境提高操作性

單純數據資料，相較於個人資料而言，跨境傳輸或共享受主管機關關切、疑慮之風險為低，輔以提高透明性、滾動式管理的去識別化管理制度，這樣機關內部實際利用之操作性即提高

C

風險防火牆

有所依據之去識別化機制，將可作為機關對外隱私政策，資安事件發生個資外洩機率亦有所降低，降低外部疑慮與風險

個資法重點快速回顧

- 適用於所有行業
- 全面適用各種類型之資料
- 引進特種資料概念
- 強化蒐集與利用法定要件
- 增加告知義務

- 加重民事、刑事與行政責任
- 監督委託責任
- 提供當事人行使權利
- 團體訴訟與舉證責任
- 安全管理責任

GDPR、APEC隱私框架與我國個資法規範重點比較

GDPR	APEC隱私框架	我國個資法

- 假名化(pseudonymisation)：在不利用額外資料的情形下，即無法認定個人資料歸屬於特定資料當事人；該額外資料係分別保管，並有採取技術或組織上等措施，確保該個人資料無法被歸屬於一個特定或可識別之自然人
- 匿名化(anonymisation)：與特定或可識別之自然人無關聯之資訊，或原本屬於個人資料，但經過匿名化處理，已無從識別當事人

GDPR、APEC隱私框架與我國個資法規範重點比較

GDPR	APEC隱私框架	我國個資法

- 無，依據APEC經濟體國內法規定

GDPR、APEC隱私框架與我國個資法規範重點比較

GDPR	APEC隱私框架	我國個資法

- 「無從識別特定之當事人」指個人資料以**代碼、匿名、隱藏部分資料或其他方式，無從識別該特定個人**

個人資料之「目的內利用」與「目的外利用」

- **個人資料的利用**
  - ✓ 原則：特定目的範圍之外
  - ✓ 例外：合法之「目的外利用」

例外：

一、法律明文規定

二、為增進公共利益

三、為免除當事人之生命、身體、自由或財產上之危險

四、為防止他人權益之重大危害

五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過**提供者處理**後或**蒐集者依其揭露方式**無從識別特定之當事人

六、經當事人書面同意

國內個人資料去識別化規範

個人資料(個資法§2(1)、細則§2、§3)

- 指現生存之自然人...等得**直接或間接識別該個人的資料**

去識別化(細則§17)

- 指個人資料以代碼、匿名、隱藏部分資料或其他方式，**無從識別該特定個人**

法務部103年11月17日法律字第10303513040號函

- 經**去識別化後**的資料，即非個資法上之個人資料
- 去識別化，**應達無從直接或間接識別特定當事人**之程度

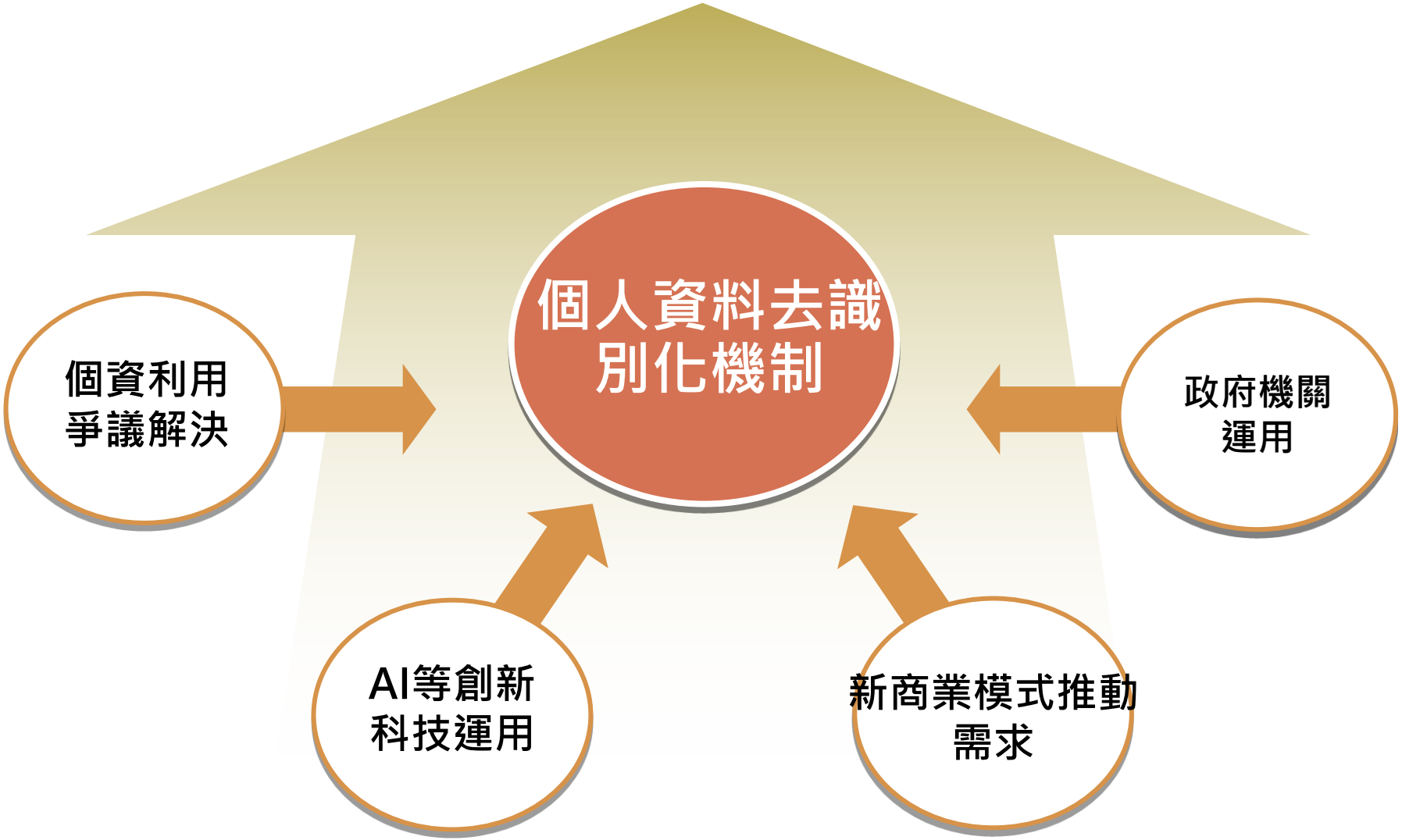
法務部，個資利用與去識別化議題，2015/04/24

我國個資法於去識別化之法制結構

- 個資法第27條、細則第12條安全維護事項

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、軌跡資料及證據之保存。
十一、個人資料安全維護之整體持續改善。

個資去識別化機制建立之需求



104去識別化驗證導航—財政部財資中心

資料來源：財政部財資中心104年12月4日「個人資料去識別化過程驗證案例報告」

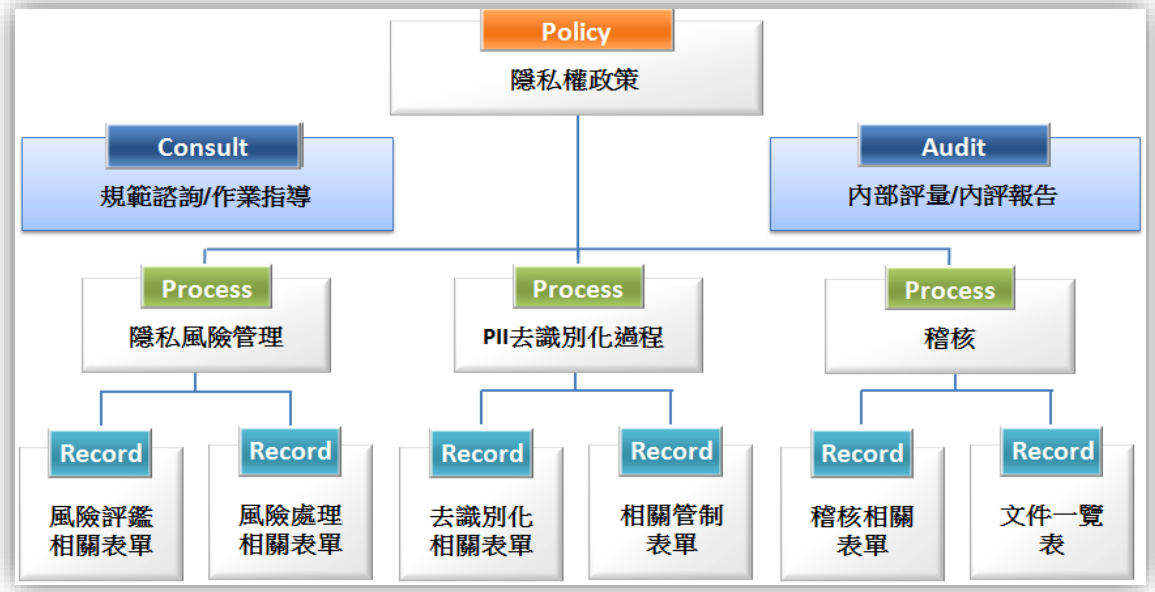
驗證範圍

- 所得稅核定資料—綜合所得稅核定檔
- 以102年度綜合所得稅核定檔為實作案例
- 資料檔共7,200,807筆紀錄

公務機關首度導入去識別化管理制度

105去識別化驗證—衛福部統計處

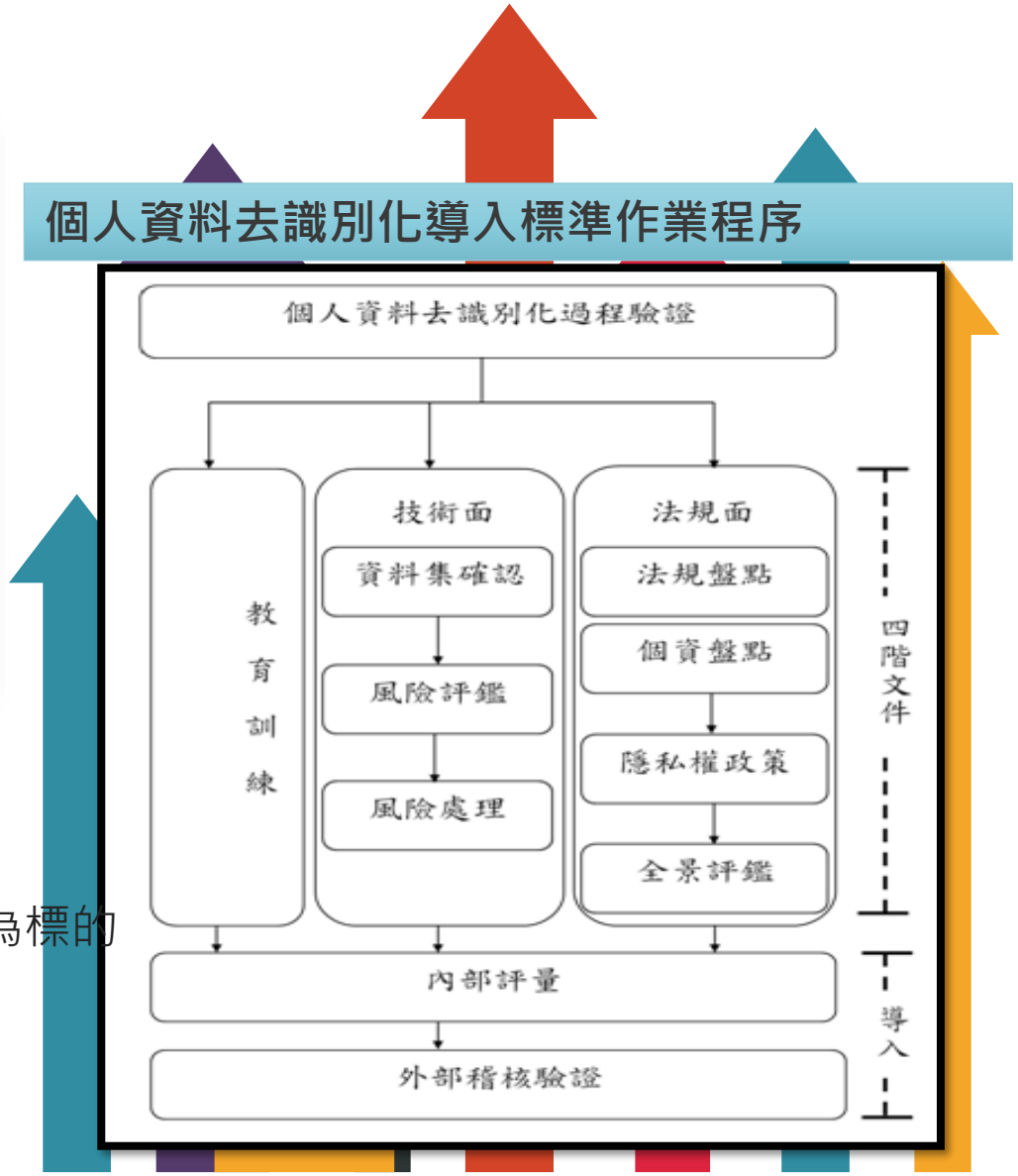
衛福部個人資料安全管理制度



驗證範圍

- 身心障礙者生活狀況及各項需求評估調查外釋資料
- 以100年度身心障礙者生活狀況及各項需求評估調查為標的
- 資料檔共1,077,544筆紀錄

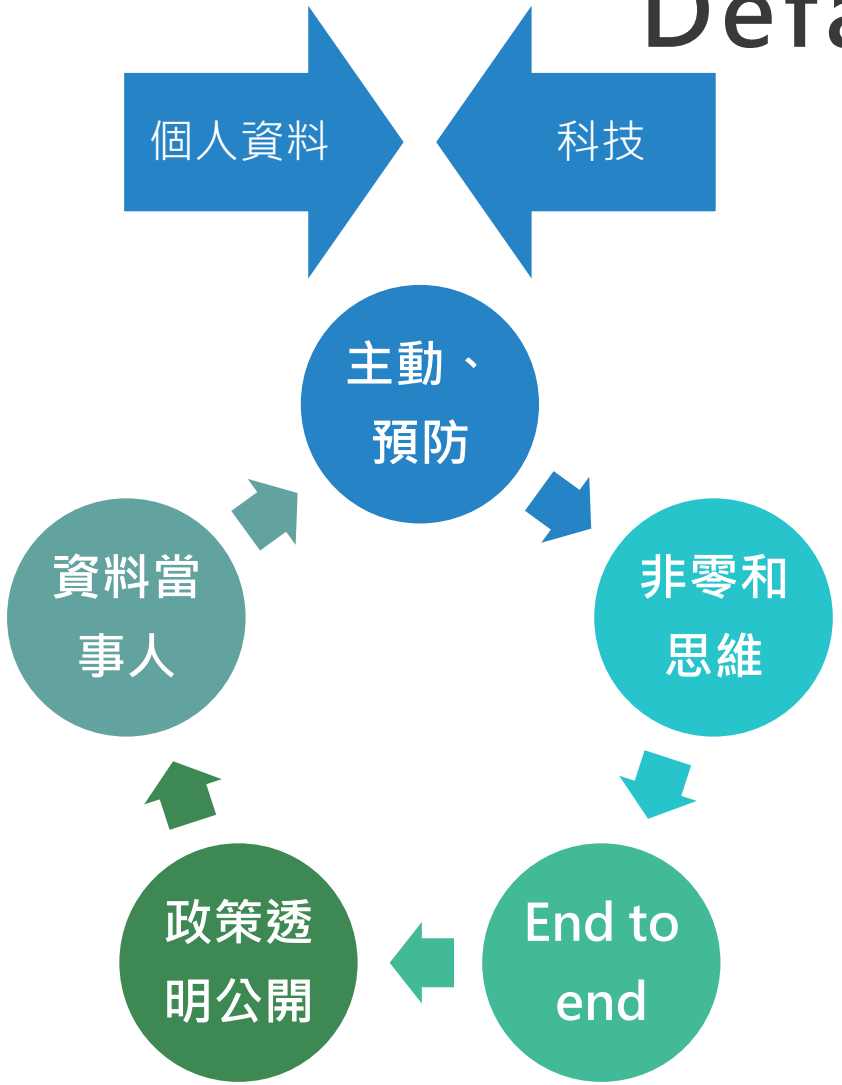
個人資料去識別化導入標準作業程序



03 | 03

個資去識別化管理機制分享

資料保護設計/預設 (Data Protection by Design and by Default, DPbDD)

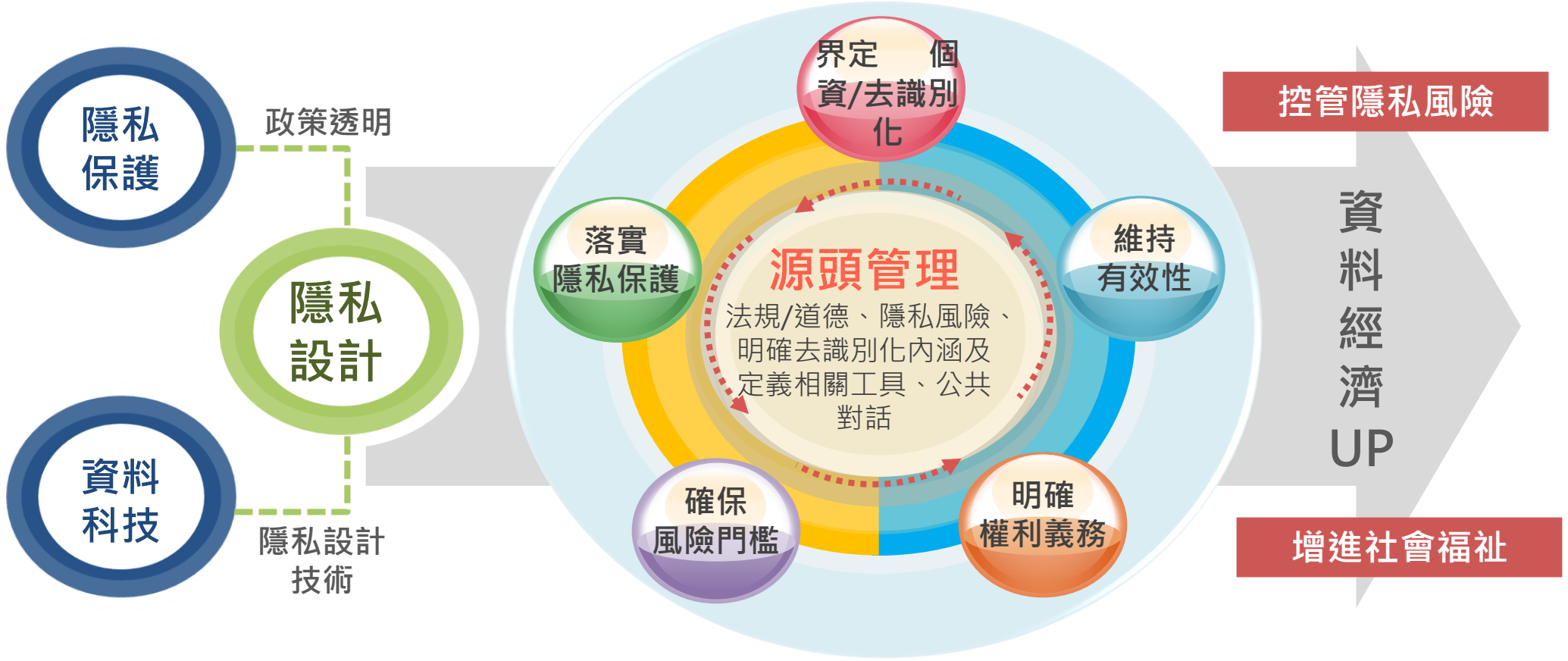


隱私技術
所在地法規、資料使用需求與目的、隱私衝擊評估等

倫理議題
透明性、目的一致性、資料分析結果適當運用、個資主管機關解釋等

法令遵循
資料當事人權利、域外傳輸妥適性、隱私政策、個資主管機關回報義務等

隱私設計之去識別化治理



- 資料跨域應用已逐漸為各國所重視，藉由分析巨量資料，可以開拓資料經濟，進而創造產品創新價值並培育新興市場
- 藉由「政策透明」、「隱私設計」等措施，輔以隱私設計技術，將可提升資料當事人之信賴，促進資料之流通與加值應用，實現資料經濟

DPbDD之技術思維

有關匿名化治理，從歐盟工作小組2014年之「匿名化技巧意見書」觀察其經驗：

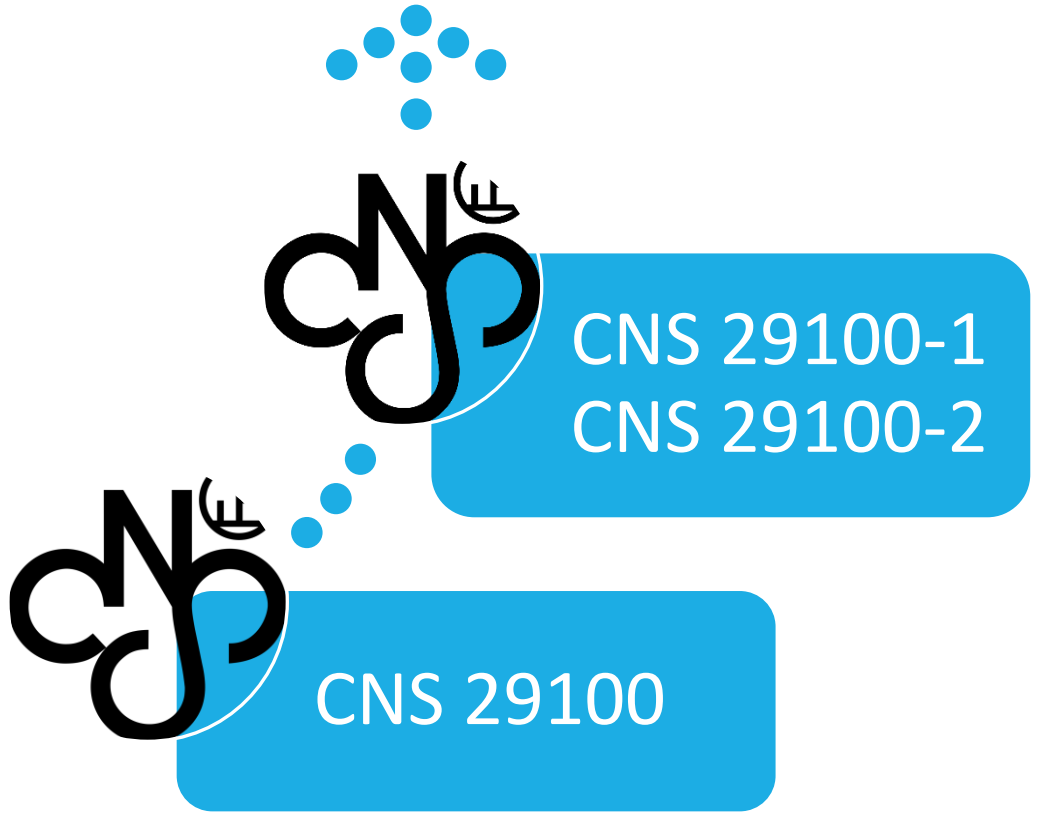
- 匿名化治理強調「可信賴性」。
- 可信賴性判斷方式，由風險門檻之設定與控管著手。
- 未完全匿名化時，仍回歸資料保護規範。

匿名化技巧意見書

匿名化技術法遵(可信賴性)判斷	剩餘風險(residual risk)判斷
(1) 是否仍有可能分辨出特定當事人？ (2) 是否有可能將紀錄與特定當事人產生連結？ (3) 與個人有關的資料是否有可能被推斷出來？ *技術例示：「隨機化」(randomization)以及「概化」(generalization)	(1) 盤點新的風險，並定期進行剩餘風險之風險檢驗 (2) 對於已存在之風險，分析相關控制措施是否有效或者已進行調整 (3) 監督並控制風險

企業選驗證標準體現法遵

- 由於資料蒐集、處理及利用可能涉及跨國、所在地法特別要求、合法再利用等不同需求，尋求合適隱私資訊管理制度因此為各界關注
- 我國目前去識別化標準：個人資訊去識別化過程管理系統(CNS 29100-2:2019)
- 國際最新隱私資訊管理標準：ISO/IEC 27701

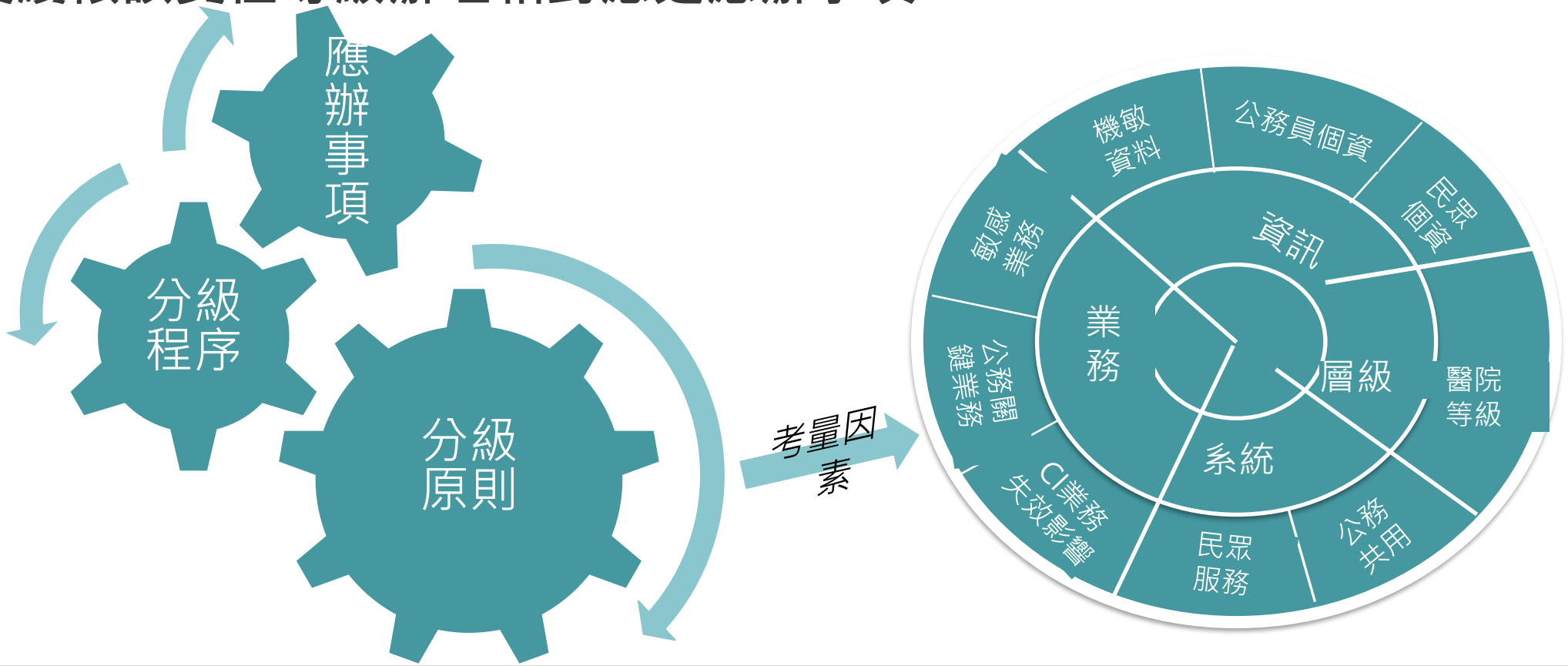


隱私資訊管理之有責性展現

- 領導與監督
- 風險評估
- 政策與程序
- 透明性
- 訓練與風險意識
- 偵測與核實
- 復原與執行

借鑑1：資通安全責任等級分級辦法

- 機關應考量其業務、資訊、系統、機關層級等因素訂定機關資安責任等級。
- 後續依該責任等級辦理相對應之應辦事項。



借鑑2：ISO 29115信賴等級

- 信賴等級(LoA)：意指機制之流程的信賴程度，從而保證使用特定身分的個體實際上就是被賦予該身分的個體。LoA共分四等級，各級用於表示對所主張之身分的信賴程度意義如下：
- LoA1（低）：具少許或幾乎無可信度。
- LoA2（中）：具某種程度的可信度。
- LoA3（高）：可信度高。
- LoA4（極高）：可信度極高。

Thank you