數位發展部 Ministry of Digital Affairs

數據公益運作指引、隱私強化技術應用指引辦理情形

多元創新司

2024.01.25

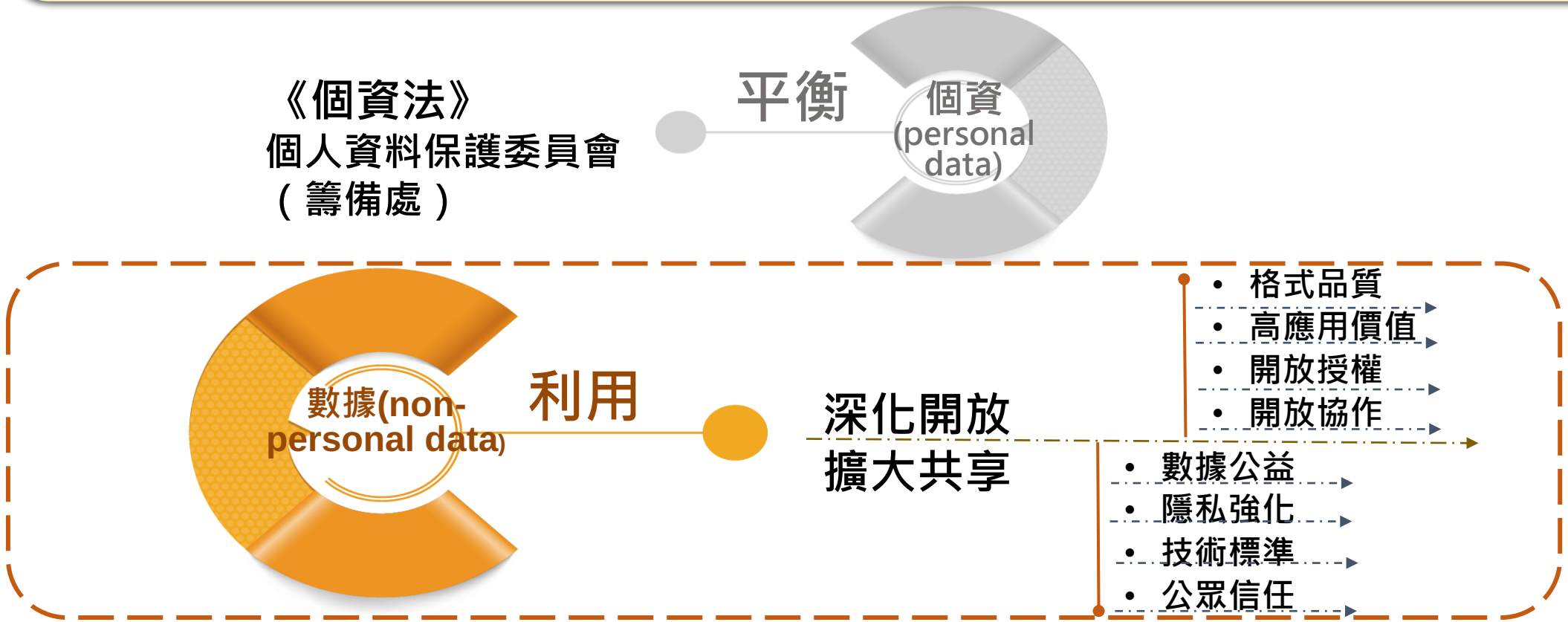
大綱

CONTENTS

1. 推動背景
2. 發展歷程
3. 指引重點說明
   - ●數據公益運作指引(草案)
   - ●隱私強化技術應用指引(草案)

一、資料治理政策趨勢

1. 數位時代，資料對推動創新發展的價值舉世公認，先進國家致力於調適相關法制與政策，以**降低資料流動及取得之障礙**，最大程度**釋放資料利用潛能**。
2. 強化**個資保護**、活化**非個資數據利用**，兩者之衡平兼顧，是適法運作之前提，也是取得個資當事人信任之關鍵。



二、先進國家非個資數據法制趨勢

2019循證決策基本法修法（包含開放資料）
2020聯邦資料戰略

2019資料共享與治理法

2017公共資料提供與利用法（開放資料）
2020資料基本行政法（政府資料管理與循證決策）
2022資料產業振興與利用基本法

2018數據流通規則
2019開放資料指令（政府資料）
2020歐洲資料戰略
2022資料治理法
（特定政府資料、數據公益制度）
2023資料法

德國：2017政府電子化法、2022資料戰略

2016官民資料活用推進基本法
2021綜合資料戰略

2022資料可用性及透明度法（G2G）

- 提倡以公共利益為目的之無償及自願性的資料共享
- 增加資料之可利用性及可信任性
- 克服資料再利用的技術障礙

四、打造公眾信任之數據公益生態

數據公益運作情境

良善社會
共創共好

自願提供
數據

資料持有者

✓政府
✓企業
✓學研
✓NGO/NPO
…

隱私
強化

研擬
規範

數據
共享

數據公益
信任機制

數據公益運作者

公部門

公益組織

……

moda 數位發展部 Ministry of Digital Affairs

隱私強化技術指引

數據公益運作制度

數據公益運作場域

無涉個資
數據

數據公益
創新應用

數據利用者

✓政府
✓企業
✓學研
✓NGO/NPO
…

合規利用

公益效益
回饋

公益目的
相關應用

• 弱勢關懷 • 交通改善 • 長者照護
• 國民健康 • 環境保護 • ……

大綱

CONTENTS

1. 推動背景
2. 發展歷程
3. 指引重點說明
   - ●數據公益運作指引(草案)
   - ●隱私強化技術應用指引(草案)

一、數據公益運作指引(草案) -作業及公眾意見徵集歷程

數據公益運作指引(草案)

第一點	第二點	第三點	第四點	第五點	第六點	第七點	第八點	第九點
本指引之目的與性質	本指引用詞之定義	定明數據公益運作機制之公益目的與基本原則	定明涉及個人資料之資訊應處理為數據及其採取措施	定明資料持有者宜遵循之條件	定明數據公益運作者宜符合之條件	定明數據公益利用者接收數據用於公益目的時宜遵循之條件	定明利害關係人權益保護措施	定明數據公益運作機制之其他注意事項

修正內容

各界主要就**資料治理法制規劃、個資法適用、指引效力、「數據」用詞、公益目的範圍、商業利用、主管機關、FAIR原則、非專屬授權**等提供意見，除於眾開講綜整回應，並據以調整指引各點內容。

- **112/5-112/8** 專家撰擬與審稿
- **112/9/27** 開放政府協作會議
- **112/9/11-112/10/31** join平臺眾開講
- **112/11** 意見綜整及修訂
- **112/12/26** 資料創新法制分組工作會議
- **113/1/16** 完成指引修訂

二、隱私強化技術應用指引(草案) -作業及公眾意見徵集歷程

隱私強化技術應用指引(草案) HackMD線上版 https://gov.tw/Byk

第一章	第二章	第三章	第四章	第五章
簡介	什麼是隱私強化技術	具指標隱私強化技術	應用案例	相關文獻
1.1 指引目的 1.2 名詞解釋	2.1 技術概述 2.2 技術施用評估流程 2.3 技術之分類與應用 2.4 技術應用之挑戰	3.1 差分隱私 3.2 合成資料 3.3 聯合學習 3.4 同態加密 3.5 安全多方計算	4.1 應用案例整理與說明 4.2 模擬案例-共享糖尿病預測科研資料 4.3 模擬案例-金融欺詐事件偵測 4.4 模擬案例-犯罪資料雲端運算 4.5 模擬案例-隱私保護之平均薪資計算	國內外參考文獻

修正內容

- 增補**名詞定義**、確保用詞一致性等。
- 調整**技術應用效益**之舉例陳述，於評估隱私保護機制階段增補**技術選用決策樹**，補充技術限制說明。
- 參照**先進國家PETs指引**，充實個別技術相關說明 。
- 歸納對應之**技術應用案例**，以利技術施用者參考。

112/4-112/8 技術專家撰擬與審稿

112/9/11-112/10/15 join平臺眾開講/HackMD留言協作

112/11/27 期末專家審查會議

112/12/26 資料創新法制分組工作會議

112/1/16 完成指引修訂

三、兩指引之關聯性

數據公益運作指引

- ✓ 遵循現有法令為前提
- ✓ 公益目的及基本原則
- ✓ 參與者共同信任基礎
- ✓ 機制公開透明

建構透明運作機制
增進數據共享正向價值

兼顧資料可用性及隱私保護之技術配套

隱私強化技術應用指引

- ✓ 隱私強化技術簡介
- ✓ 技術類型及適用情境
- ✓ 技術施用評估流程
- ✓ 技術應用效益

依資料適用情境
採取適當隱私保護技術

建立公眾信任
數據有感創新
促進社會共好

大綱

CONTENTS

1. 推動背景
2. 發展歷程
3. 指引重點說明
   - ●數據公益運作指引(草案)
   - ●隱私強化技術應用指引(草案)

數據公益運作指引(草案)重點-目的與基本原則

指引目的

- 針對**電子形式**且**非屬個人資料**之「數據」，明確揭示**自願**、**無償**用於公益目的之運作機制
- 推動社會整體之**數據共享機制**發展，構建可信任之數據生態，促進**社會**、**經濟**、**環境**永續發展

基本原則

- 參與者對**公益目的**認同與信任
- 運作領域包括**氣候環境、災害防救、交通運輸、健康醫療、能源管理、社會福利**，以及其他法令規範所保護公共利益之範圍
- 遵循現行相關法規、依誠實及信用方法、採行適當管理措施、採用隱私強化技術

數據公益運作指引(草案)重點-數據公益參與者遵循事項(1/2)

資料持有者

有權提供特定數據之自然人、法人、機關或團體

訂定重點

- 依法有權向他人提供
- 認同數據公益運作者或數據利用者之公益目的
- 不損害利害關係人權益
- 提供方式具備充分安全性
- 對提供行為保存相關紀錄

數據公益運作者

執行數據公益運作機制，協助數據共享之機關

訂定重點

- 建立數據管理制度(接收、處理、利用)
- 紀錄保存與資訊揭露制度
- 遵循可搜尋、可近用、可互通以及可再利用之原則
- 非專屬利用原則、適當技術措施
- 訂定書面契約，明確約定各方權利及義務

自願無償提供為原則
認同應用主題之公益目的

非以營利為主要目的
基於社會創新發展應用主題

數據公益運作指引(草案)重點-數據公益參與者遵循事項(2/2)

數據利用者

接收數據為利用之自然人、公司或其他法人、機關或團體

訂定重點

- 法令規範及契約約定
- 未逾越所涉公益目的之必要範圍。
- 不損害利害關係人權益
- 所採取之數據接收及利用方式具備充分安全性
- 接收及利用行為保存相關紀錄

促進社會福祉及公共價值
推動全民共享共好之多元應用

利害關係人

對數據公益運作機制有利害關係者

訂定重點

- 以正當方式取得利害關係人同意
- 數據不當利用通知利害關係人
- 利害關係人退出機制
- 利害關係人異議回應機制

多元角色參與
瞭解並信任數據公益機制

大綱

CONTENTS

1 推動背景

2 發展歷程

3 指引重點說明

- 數據公益運作指引(草案)
- 隱私強化技術應用指引(草案)

隱私強化技術應用指引(草案)重點-技術概述

傳統去識別化技術

- **抑制/編修**
  例如：僅保留身分證字號後6碼或將身分證字號欄位刪除
- **遮罩**
  對資料局部置換為特殊符號，如：〇或※
- **符記化**
  例如：將身分證字號置換為另一組符合編碼原則的虛假字號
- **泛化**
  例如：將年齡 25 歲，泛化為年齡 20~29 歲
- **k-匿名化**
  確保釋出之資料集中每筆紀錄皆至少有k-1筆相同的紀錄

新興隱私強化技術

- **合成資料**
  針對提供數據供機器學習或數據分析應用，可產生合成資料，避免直接利用原始資料所衍生的風險，亦保留數據的可用性
- **同態加密**
  隨雲端運算盛行，同態加密技術，可讓資料維持在加密狀態進行運算，運算過程中皆無需解密，為機密性提供最根本的保障
- **聯合學習**
  醫療影像藉由聯合學習，讓參與方不需分享機密性資料，只需共享AI模型，即可發展精準且民眾有感的醫療服務
- **…**

隱私強化技術應用指引(草案)重點-技術效益

提升隱私保護

提供契合使用情境之隱私保護方案，降低直接利用原始資料之風險。

促進資料提供

以技術方法取得僅限分析所需之數據，使其無從辨識個別提供者資訊，資料提供更安心。

支持跨域資料協作

具促進多方資料協作之特性，可協助組織間以安全之方式共享數據。

建構數據信任

透過技術方法達成資料最小化，避免直接利用原始資料，增進資料安全治理信心。

隱私強化技術應用指引(草案)重點-技術適用情境

資料蒐集 隱私保護

本地差分隱私

不蒐集原始資料
僅蒐集經雜訊保護後的數據

資料運算 隱私保護

同態加密

資料保持加密狀態
進行資料運算

可信執行環境

僅經授權的程式碼和
記憶體區塊可存取機敏資料

資料分享 隱私保護

差分隱私　合成資料

不直接提供原始資料
僅提供添加雜訊數據、合成數據

內部資料

外部資料1 | 外部資料2

多方資料協作隱私保護

安全多方運算　聯合學習

不揭露原始資料，進行模型訓練、函式運算協作

資料運算

公開隱私強化運算結果

資料集　統計數據/分析結果　機器學習模型

授權使用運算結果

函式運算結果　機器學習模型

隱私強化技術應用指引(草案)重點-技術應用案例

1.2014年智慧型行動裝置採用本地差分隱私搜集用戶回饋

智慧型行動裝置業者，透過用戶知情同意機制同意共享操作資訊並搭配本地差分隱私及聯合學習等技術，達成不用取得真實數據，亦可進行分析應用。

2. 2016年波士頓女性勞動力委員會舉辦區域性薪資調查

波士頓女性勞動力委員會透過安全多方運算技術，在不透露原始資料的情況下，統計波士頓地區之性別和種族薪資差距。

3. 2018年加拿大統計局以合成資料增進黑客松競賽資料品質

透過合成資料技術，可在不侵犯個人隱私的情況下，產製高可用性且貼近真實的資料讓黑客松競賽參賽者進行分析。

4.2020年美國人口普查

美國普查局公開普查資料讓大眾使用時，透過差分隱私技術加入雜訊，兼顧隱私保護力與資料實用性。以保障美國不同種族人口與住房相關敏感資料，同時兼顧資料實用性。

5.2024年韓國統計局：開發保護隱私的統計數據中心平台

韓國刻正研發推動具同態加密、差分隱私和合成數據等隱私保護技術之資料平台，期鏈接分散之人口、家庭和機構統計登記冊資料，促進政府數據之間的聯繫，從而最大限度地發揮數據的潛在價值。

隱私強化技術應用指引(草案)重點-技術應用挑戰

- 隱私強化技術並非萬靈丹
- 適當的使用方可降低資料隱私風險和保有資料可用性
- 資料處理仍須符合法律規範、公平及透明原則
- 建議於考量技術採行與否時，納入潛在挑戰

挑戰1-部分技術仍在發展中

隱私強化技術種類多樣，但並非所有技術皆發展成熟，因此使用隱私強化技術時，需仔細評估其成熟度

挑戰2-技術門檻較高

若實作或使用隱私強化技術工具時，缺乏專業知識、理解錯誤，可能造成所實作出的工具與理論之間存在落差，或是輸出資料無法達到保護力與實用性的適當平衡

挑戰3-驗測機制及標準未臻明確

部分隱私強化技術屬於新興科技，尚未發展統一之技術標準、國際規範或得以驗證其隱私保護效力之機制

挑戰4-技術使用之合規性

這些新興的技術採用有別於傳統去識別化技術之技術原理，經運用隱私強化技術處理後的特定資料是否脫離個資法適用範圍，尚需法規主管機關個案判斷，但隱私強化技術能於合規前提下為個人資料之蒐集、處理及利用提供實質的隱私保護

隱私強化技術應用指引(草案)重點

✓ 更詳細的技術說明

已研擬含技術概述、技術可解決的問題、發展沿革、技術現況、施用情境、施用風險、開源工具與社群等章節，期增進各界對技術本質之了解

✓ 更豐富的應用案例

收納國內外技術應用實例及示範性案例，供各界了解技術應用趨勢，掌握技術革新契機，並將持續彙集更多應用案例

✓ 技術選用策略

就技術原理及適用場景進行歸納分類，協助技術施用者對應需求情境選用適宜的技術方案

✓ 個別技術施用流程

提供技術施用者了解實作及運作階段之關鍵步驟及考量

- 規劃系統架構
- 整備所需資源
- 實作隱私強化技術
- 經隱私保護之資料利用

✓ 5種具指標性技術介紹

差分隱私、聯合學習、同態加密、合成資料、安全多方運算等技術之深入介紹

滾動更新

未來將持續觀測國際最新技術趨勢，以及配合本年隱私強化技術應用推動計畫，逐步擴充有關技術可用性分析、驗測機制及應用案例等內容，因時制宜更新本指引。

感謝您的聆聽

Thank You

moda

數位發展部

Ministry of Digital Affairs

附錄一 數據公益運作指引(草案)(1/4)

PDF版 https://gov.tw/Ge7

數據公益運作指引(草案)

一、 目的

為推動社會整體之數據共享機制，建構可信任之數據公益生態，促進社會、經濟、環境永續發展，爰訂定本指引，針對電子形式且非屬個人資料之「數據」，明確揭示自願、無償用於公益目的之運作機制，以行政指導促進數據之公益利用，創新數據應用與公共服務。

二、 名詞解釋

（一） 本指引所稱之數據，係指以電子形式存在，且非屬個人資料保護法所稱個人資料之資訊；涉及個人資料之資訊應處理為數據。

（二） 本指引所稱之數據公益運作機制，係指促進自願、無償提供數據用於公益目的之機制。

（三） 數據公益運作機制之參與者包括：

1. 資料持有者：即有權提供特定數據之自然人、法人、機關或團體。
2. 數據公益運作者：即執行數據公益運作機制，協助資料持有者、數據利用者與利害關係人間共享數據之機關、非以營利為目的之法人或團體。數據公益運作者自身得兼為資料持有者或數據利用者。
3. 數據利用者：即接收數據為利用之自然人、公司或其他法人、機關或團體。
4. 利害關係人：即資料持有者、數據利用者、數據公益運作者以外，對數據公益運作機制有利害關係者。

三、 數據公益運作機制，係以參與者對公益目的之認同與信任，作為核心理念，其運作領域包括氣候環境、災害防救、交通運輸、健康醫療、能源管理、社會福利，以及其他法令規範所保護公共利益之範圍。

數據公益運作機制，宜注意下列基本原則：

（一） 遵循下列相關法令規範：

1. 涉及個人資料之資訊處理為數據以用於數據公益目的時，

附錄一 數據公益運作指引(草案)(2/4)

遵循個人資料保護法及相關規範。

2. 涉及政府資訊時，遵循政府資訊公開法及相關規範。

3. 涉及智慧財產或商業上之機密資訊時，遵循智慧財產權、營業秘密保護之相關規範。

4. 其他相關法令規範。

（二） 依誠實及信用方法為之，尊重利害關係人之權益。

（三） 採行適當管理措施，確保數據利用符合公益目的。

（四） 採用隱私強化技術，並以不升高風險之方式公開揭露資訊，以確保資料蒐集、資料處理、數據利用之透明性。

前項第四款所稱之隱私強化技術，得參閱數位發展部公告之隱私強化技術應用指引。

四、 數據公益運作機制涉及個人資料之資訊，處理為數據前，就該資訊之蒐集、處理與利用（含數據公益運作機制參與者間之傳送），宜注意下列事項：

（一） 依個人資料保護法向當事人充分告知法定事項，包括處理該個人資料之公益目的、所涉個人資料範圍、該個人資料之來源、處理為數據之方式及當事人享有之權利等。

（二） 依個人資料保護法取得當事人同意，或具備個人資料保護法關於個人資料蒐集、處理或利用之其他法律依據。

（三） 限於足以實現公益目的之最小範圍並保障其安全，包括於可行範圍內採取適當技術措施，以無從識別方式處理該個人資料。

前項涉及個人資料之資訊處理為數據之時點，由資料持有者於提供該資訊予數據公益運作者前，或數據公益運作者於提供該資訊予數據利用者前為之。

五、 資料持有者自願、無償提供數據用於公益目的，宜注意下列事項：

（一） 依法有權向他人提供。

（二） 認同數據公益運作者或數據利用者之公益目的。

（三） 不損害利害關係人權益。

（四） 提供方式具備充分安全性。

（五） 對提供行為保存相關紀錄。

附錄一 數據公益運作指引(草案)(3/4)

六、 數據公益運作者依第三點第一項擇定其數據公益目的及運作領域後，宜建立下列管理制度：

（一） 數據接收管理制度，包括數據利用目的及限制條件遵循措施、資料持有者提供數據之相關成本補償等。

（二） 數據處理管理制度，包括數據之分類、儲存、分析、安全維護、違法或不當利用數據情事之應變等。

（三） 數據利用管理制度，包括數據利用者取得數據應符合之條件、申請程序、數據取得方式、取得數據後應採取之利用及保護措施等。

（四） 紀錄保存與資訊揭露制度，包括對接收、處理及提供行為，保存完整之紀錄、年度活動報告之準備與揭露等。

數據公益運作者宜採取下列措施，以利提升數據公益運作機制之成效：

（一） 遵循可搜尋（findable）、可近用（accessible）、可互通（interoperable）以及可再利用（re-usable）之原則，以結構化且機器可讀之通用格式接收、處理與提供數據，並揭示數據來源及利用條件，強化數據之互通性與易用性。

（二） 採用適當技術措施，強化數據接收、處理與提供過程中對數據之機密性、完整性與可用性保護，提升利害關係人及社會各方對數據公益運作機制之信任。

（三） 設計取得、確認及管理利害關係人同意數據公益利用之標準程序，強化數據利用適法性保障。

數據利用條件之約定，宜與數據內容、公益目的、利用方式等因素相稱，且原則宜以非專屬利用方式為之；必要時得以專屬利用方式為之，並宜先公開專屬利用約定之主要內容，且與數據利用者約定適當利用期間。

數據公益運作者宜與資料持有者、數據利用者訂定書面契約，明確約定各方權利及義務，例如：是否有對價及商業利用限制等；其書面契約得依電子簽章法之規定，以電子文件為之。

七、 數據利用者之接收及利用行為，宜注意下列事項：

（一） 法令規範及契約約定。

附錄一 數據公益運作指引(草案)(4/4)

（二）未逾越所涉公益目的之必要範圍。

（三）不損害利害關係人權益。

（四）所採取之數據接收及利用方式具備充分安全性。

（五）對接收及利用行為保存相關紀錄。

數據利用者宜適當採取前點第二項所列措施，以利提升數據公益利用之成效。

八、 資料持有者、數據公益運作者及數據利用者就數據公益之運作，如需取得利害關係人同意，不得以誤導、欺瞞、強迫等不正方式為之。

資料持有者、數據公益運作者及數據利用者宜就數據公益之運作，建立數據不當利用通知機制，於發生數據利用超出利害關係人同意或約定範圍、不符同意或約定條件等情事時，通知受影響之利害關係人。

資料持有者、數據公益運作者及數據利用者宜建立保障利害關係人權益之適當機制，例如同意撤回機制（同意之撤回，不影響撤回前依據該同意所作蒐集、處理及利用之適法性）、異議之受理及回應機制（包括異議處理期間暫停利用數據之情形等）。

九、 資料持有者、數據公益運作者及數據利用者就數據公益之運作，應按其組織屬性、擇定之數據公益目的及運作領域，遵循相關法令規範。

資料持有者、數據公益運作者及數據利用者如委託他人蒐集、處理或利用數據，宜於委託契約約定以適當方式監督，例如：可適時實地稽核、請求說明或提出報告等方式，確保受託者嚴格遵守其指示及採取適當數據安全維護措施。

資料持有者、數據公益運作者及數據利用者宜對其所屬人員適時辦理認知宣導及教育訓練，使其明瞭相關法令規範之要求、所屬人員之責任範圍，以及蒐集、處理、利用及保護機制、程序及措施。數據公益運作者並宜辦理相關宣導或推廣活動，以增進各界對數據公益運作機制之瞭解與信任。

文件結尾 ■

附錄二 隱私強化技術應用指引(草案)

PDF版 https://gov.tw/ePy　　HackMD線上版 https://gov.tw/Byk