金融機構資料共享之資料治理諮詢文件

目　錄

一、 前言

(一)背景說明

為提升客戶體驗、降低作業時間及成本、管控風險及精準行銷等目的，金融機構資料共享與交換等需求日益普遍，較明顯之案例包含開放銀行(open banking)、開放資料串接(open API)及區塊鏈服務等。近年來 AI 與機器學習之發展迅速，運用數據進行資料訓練模型並分析客戶行為，亦為國內外金融界視為可提升客戶體驗及發展創新服務之機會。然而大眾逐漸關注個人資料的使用權益及隱私權保護，且客戶資料之洩露，不僅可能造成客戶及金融機構之損失，更可能影響大眾對金融機構風險管理的信任與對金融市場的信心，因此發展一套可資遵循之資料共享指引，並進而衡平發揮資料之價值、建立市場信心、落實風險管理及客戶權益保護等，係金融科技發展的重要方向。

金管會於 110 年發布「金融機構間資料共享指引」，針對金融機構間共享客戶資料提供辦理方針，後續金融機構與金融科技業者亦期待就金融機構辦理跨機構或跨市場共享客戶資料之作法給予明確指引，以進一步發揮資料或數據之效益。同時，由於金管會並無直接管轄非金融機構，因此金融機構將客戶資料共享予非金融機構，需仰賴雙方對客戶資料保護的正確認識及對資料共享時遵循個人資料保護及風險管理之約定。基此，金管會業於金融科技發展路徑圖 2.0 推動措施 1-3「深化資料共享」中，列入推動事項「發布跨市場資料共享之資料治理指引」，並規劃於 113 年 12 月完成。為能完整規劃上述指引之範圍、實用性及操作性，金管會提出本諮詢文件，對外徵求各界意見。

本諮詢文件所稱之資料共享之範圍不含個人資料保護法(以下簡稱個資法)之特種個資，且僅含金融機構在符合個資法前提下將客戶資料提供機構外部單位之資料共享，不包含(1)金融機構將其客戶資料於機構內分享運用，(2)金融機構就非屬客戶資料(如：員工資料、金融機構本身資料)於機構內及跨機構間運用，及(3)金融機構依其他法令得辦理運用(如：基於洗錢防制與

打擊資恐、檢調偵查、稅捐課徵等目的，及依作業委外相關規範所辦理之委外作業)之情境。

(二)本文件之目的

本諮詢文件目的在蒐集金融機構利害關係人(stakeholder)之意見回饋，作為金管會後續擬具「金融機構資料共享之資料治理指引」之參考。本文件首先探討資料治理對資料共享之重要性與我國客戶資料保護相關法規，並提出金融機構客戶資料之分級與應用場景，另透過探討國際上傳統去識別化技術及新興隱私強化技術(Privacy Enhancing Technologies, PET)發展趨勢及我國數位發展部對新興隱私強化技術之說明，提出我國金融機構客戶資料之分級及治理方式，最後彙整金融機構辦理資料共享時宜注意之資料處理原則，以利金融機構制定相關內部政策與機制。

(三)本文件之諮詢對象

金融機構資料共享之利害關係人，包含如下：

1. 金融機構、相關公協會及周邊單位。
2. 金融科技業、資訊服務業及提供金融機構相關業務服務之業者。
3. 學術與研究機構。
4. 相關政府機關(個人資料保護委員會籌備處、數位發展部及行政院消費者保護處等)。
5. 一般民眾、公司行號及商業團體。

(四)金管會後續規劃

金管會將參考收到的意見回饋及參考相關政府機關(個人資料保護委員會籌備處及數位發展部)在法制與隱私強化技術之發展進展等，擬具「金融機構資料共享之資料治理指引」，並預計於 113 年 12 月底前發布。

二、 資料治理對金融機構之意義

(一)資料治理的意義

依據經濟合作暨發展組織(OECD)對資料治理之說明[1]，資料治理是指影響資料及其循環(創建、蒐集、儲存、使用、保護、存取、共享及刪除)的各種安排，包括技術、政策、法規或制度的推出等，資料治理可以最大限度地提高資料存取和共享的好處，同時處理相關風險及挑戰。

(二)客戶資料保護與資料治理

近年因個人資料保護觀念興起與歐盟「一般資料保護規則(General Data Protection Regulation, GDPR)」及美國「加州消費者隱私法(California Consumer Privacy Act, CCPA)」等法規要求下，資料治理之內涵已進一步擴充，參酌歐盟 GDPR 相關規定，組織對於客戶資料處理應遵循以下原則[2]：

1. 遵法、公平及透明(lawfulness, fairness and transparency)：客戶資料的處理，必須秉持遵法、公平且透明之原則進行。尤其在向當事人取得或提供資料或溝通時，資料檔案必須採用簡單、透明、易懂且便於取得的格式，文字用語則必須採用淺顯易懂之語言。
2. 目的限制(purpose limitation)：資料處理的目的必須特定、明確且適法，且禁止以不合於蒐集目的之手段進一步處理個人資料。
3. 資料最小化(data minimization)：資料的蒐集必須對應處理客戶資料之目的，以最適當、具關聯性且最小限度之範圍內蒐集資料。
4. 正確性(accuracy)：客戶資料必須正確且更新，尤其必須採取合理的措施，確保不正確之客戶資料立即被刪除或更正。
5. 儲存限制性(storage limitation)：具可識別性之客戶資料的保存期限，必須符合客戶資料處理之目的。
6. 完整性與機密性(integrity and confidentiality)：客戶資料之處理必須使用

[1] 經濟合作暨發展組織(OECD)網頁。檢自 https://www.oecd.org/digital/data-governance/ (Jan. 18, 2024)

[2] 戴豪君、邱映儀(民 108)。從 GDPR 遵循角度看組織資料治理新意識。國發會*國土及公共治理*，7(4)，18-29。

適當之技術面或組織面的安全措施，以確保客戶個人資料之安全，避免未經授權或違法的處理，並防止資料遺失、破壞或毀損。

前述原則係為保護客戶資料，避免其遭受不當處理，惟若對於客戶資料均一律採高度保護，恐將喪失資料處理之便利性，並降低其效率及提高成本，對於發展 AI 模型及提供具參考價值之創新服務，都有不利之影響。因此，資料治理應採分級方式，就屬於個別客戶之敏感、重大性資訊採高度保護，而就已處理過且外觀上或分析時已不易識別個別客戶之資料、或不屬於個別客戶之整體市場統計資料，可評估採風險基礎原則方式保護，俾利滿足資料共享之需求，並發揮資料之價值。

(三) 資料分級治理對於金融機構辦理資料共享之重要性

1. **金融機構客戶資料多具有財務性質，宜受高度保護**：金融機構保有及儲存之客戶資料多具有財產性質，與一般資料相較，其應受保護之程度更高，若渠等資料外洩，非但不利於客戶財務及業務資訊保密，對金融機構本身商譽及民眾信任度亦有負面影響，爰金融機構除於法令上負有對客戶資料保密之義務外，於辦理資料共享時更須確保共享過程及範圍之安全及遵法性。
2. **對於業經隱私權保護目的處理後之資料或整體市場統計資料，可評估是否採風險基礎原則方式治理**：金融科技服務多涉及資料之運用，然各種資料之屬性不同，應可依資料是否涉及個人隱私、是否經隱私權保護目的處理過或是否經過加值或彙總等情況，而有不同之資料治理方式，對於業經隱私權保護目的處理後之資料或屬整體市場之統計資料，可評估是否採較輕量治理，毋須過度保護，俾利達成資料共享之效益及提升金融科技服務之創新。
3. **確保金融機構辦理資料共享時，金融機構與資料接收者或處理者任一方皆採取適當之資料治理措施**：科技發展越趨多元與專精化，面對 AI 與機器學習、區塊鏈、雲端系統、巨量資料等創新科技及前沿技術，金融

機構基於成本效益之考量，無法於自身組織內部部署充足之開發與運用資源，爰多與其他金融機構、金融科技業、資訊服務業或學研機構等合作。在跨機構資料共享時，金融機構與資料接收者或處理者皆須採取適當之資料治理措施，並需評估任一方是否同樣具備良好之資料治理能力，俾利在保護客戶資料與隱私權下，達成資料共享之效益。

三、 我國客戶資料保護之相關法規

(一)我國個資法與資料共享有關之相關法規及函釋[3]

依據我國個資法規，與自然人相關且足以直接或間接辨識自然人身分之資訊，即屬於個資法上保護之個人資料。公務機關與非公務機關對於個人資料之蒐集與處理，應有特定目的；對於個資之利用，原則上應於該特定目的之必要範圍內為之。

1. **「目的外利用」之規範**：目的外利用係指個人資料之利用並不在個資當事人原本可能預見之個資利用範圍內，故原則上禁止，例外許可。我國個資法第 16 條及第 20 條分別規範公務機關與非公務機關對於一般個資得為特定目的外利用之條件，包含法律明文、免除當事人之危險、防範他人權益之重大危害、經當事人同意、有利於當事人權益，亦包含公務機關或學研機構基於公共利益而有必要，且資料無從識別特定當事人之情形。
2. **「當事人同意」之規範**：依個資法規，目的外利用之條件之一為經當事人同意，因此，若其他業者欲取得金融機構客戶之個人資料(如：信用卡消費紀錄、保險資料等)，必須以客戶對資料分享的「同意」為前提，該業者始能取得客戶個人資料。又當事人同意之意思表示，需滿足告知後同意之要求，且利用目的、範圍須預先告知資料當事人，並單獨另為意思表示。
3. **「無從識別特定之當事人」之規範**：我國法規並無所謂「去識別化」一詞，而是以「無從識別特定之當事人」作為相關法定義務或限制規範之除外事由。依據個資法施行細則第 17 條之規定，個資法所稱「無從識別特定當事人」係指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。意即機關運用各種技術將個人資料予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，在符合特定法定前提要件下(如：在公務機關或學研機構基於公共利益而有必要時)，

[3] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

即與一般個人資料有別，而不適用一般個資有關告知義務、特定目的外利用之禁止等相關個資法規定。

(二)我國金融法規對於客戶資料保密之相關規範[4]

金融機構因與客戶往來或交易，過程中取得大量客戶身分資料、財務狀況及社會活動情形等個人資料，因此除個資法之一般性保護，金融法規更特別強調金融機構對客戶資料之保密義務，以確保金融機構對客戶資料之蒐集、處理及利用之嚴謹性。

以銀行法第 48 條第 2 項為例，其要求除有但書所定之情形(例如：法律另有規定或經主管機關規定等情形)外，銀行對於持有之客戶存款、放款與匯款等有關資料，原則上應負擔保密義務。司法院釋字第 293 號解釋並指出本條旨在保障銀行客戶財產上之秘密，並防止客戶與銀行往來資料被任意公開，以維護人民之隱私權。此外，銀行法第 28 條第 4 項針對銀行經營信託及證券業務之人員亦有類似規定，其立法理由明確提及，為確保客戶之權益，防範內部人交易、並建立防火牆制度，要求銀行經營信託及證券業業務之人員對於客戶之往來、交易資料亦需負擔保密義務。

銀行外之其他金融業雖適用不同法規，但整體而言，均有保密義務之規定。例如：金融控股公司法第 42 條、電子支付機構管理條例第 31 條、證券投資信託及顧問法第 7 條、金融資產證券化條例第 8 條、證券商管理規則第 34 條第 2 項及第 37 條第 16 款、期貨商管理規則第 31 條第 2 項、證券投資信託事業管理規則第 19 條第 3 項、證券投資顧問事業管理規則第 13 條第 3 項等。

保險業雖並未於法律、行政規則中規定保密義務，但相關條文散見於個別業務之自律規範中。總歸來說，保密義務為金融業各業別均應遵守之原則。

在資料共享之目的下，金融機構於取得客戶同意後，方可依客戶指示將其資料提供予其他金融機構辦理資料共享，始無違反上開保密義務之規定。

[4] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

【諮詢問題】

1. 您認為金融機構辦理客戶資料共享時，還受到哪些本文件尚未敘及之規範？尤其在遵循個資法相關規定情形下，金融機構實務運作上還遇到什麼挑戰？

四、 金融機構之客戶資料分級及應用場景

(一)金融機構客戶資料分級

本文件旨在促進金融機構於跨機構間辦理資料共享及落實資料治理，爰依是否可採較輕度治理、是否有利於隱私權保護等角度，嘗試提出下列資料分級之作法，本分級作法所涵蓋之客戶不限於個人，尚包含法人、機關及團體客戶。

第1級.原始客戶資料：

(1) 由客戶提供，如：姓名、生日、身分證字號、稅籍編號、地址、法人之受益人及董(理)監事、收入等。

(2) 金融往來紀錄，如：帳戶號碼、交易明細。

(3) 針對個別客戶之分析評估資料，如：信用評分。

第2級.經隱私權保護目的處理後，仍易遭還原而識別客戶之資料：第 2 級資料係指雖已將客戶原始資料進行處理，但透過外部資料比對及連結或運用新興資料庫重建技術等方式，仍可能遭還原而能識別客戶之資料。

第3級.經隱私權保護目的處理後，較不易遭還原而識別客戶之資料：第 3 級資料係指已將客戶原始資料進行處理，且依據現有之技術及科技條件，難以還原並識別客戶之資料。

第4級.不屬於個別客戶之資料：經統計處理後之統計資料、或經隱私權保護目的處理後，非真實客戶之模擬資料。

(二)本分級作法目的係為確保金融機構遵循個資法，同時就業經隱私強化之資料提出給予較輕度治理之彈性，以利資料共享之順暢

1. **本分級作法與資料治理之關聯**：在本分級作法下，除第 4 級不屬於個別客戶之資料外，其餘 3 級皆須遵循個資法中取得當事人同意等相關規範。若金融機構欲使用第 1 級原始客戶資料進行蒐集目的外之利用(如：某場景運用或研究等)，運用前即須投入許多資源以取得客戶同意，其付出

之時間與人力等作業成本十分沉重，因此將降低金融機投入該項目的外利用之動機。若金融機構使用第 3 級不易識別客戶之資料，雖其尚存在識別客戶之風險，然因其業經隱私權保護目的處理，且在資料最小化、儲存限制性等治理原則下，其仍具備某程度之隱私權保護效果，有助於降低客戶被識別後之可能受損害程度，故本文件提出金融機構可評估採取較簡易之取得客戶同意方式，以降低作業成本，提升客戶同意之機會，達成資料共享之目標。

2. **本分級作法對於個別客戶資料可使用程度之說明**：在本分級作法下，客戶個人資料經隱私權保護處理之程度通常與客戶資料可使用之程度成反比[5]，亦即經隱私權保護處理程度越高之資料(如：第 3 或第 4 級資料)，因經常會移除越多屬於個別客戶之資料，所以越無法呈現原本客戶之屬性而失去可用性(如：精準行銷)。因此金融機構宜注意二方面之取捨，依據擬應用之場景，決定所擬採用之客戶資料級別。

【諮詢問題】

2. 針對本文件提出之客戶資料分級作法，您認為是否有利於辦理跨機構間資料共享？亦即是否可發揮資料共享之效益及是否可發揮隱私權保護之目的？
3. 這樣的分級作法，您認為是否有潛在風險，為什麼？
4. 您是否認同本分級作法與資料治理之關聯？
5. 您是否有其他客戶資料分級之建議？

(三)金融機構辦理客戶資料共享之應用場景

1. 金融往來：驗證客戶身分、新辦業務(如：開戶、投保時帶入客戶在其他金融機構已存有之資料)、交易業務(如：客戶之證券交易資料提供予投顧業者)。

[5] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

2. 便利客戶作業：減少客戶重複輸入其原始資料。
3. 分析比對及風險控管：KYC、防範詐騙、負面消息及各類風險控管(如：信用風險、體況風險)。
4. 業務發展(如：新商模設計或探索)及精準行銷。
5. AI 及機器學習之訓練模型。
6. 產業或市場調研。
7. 與學研機構合作學術研究。

【諮詢問題】

6. 您認為所列金融機構辦理客戶資料共享之應用場景是否足夠？是否還有其他場景應列出?
7. 您對應用場景是否有其他建議？

五、 傳統去識別化技術及新興隱私強化技術之探討

依據前述金融機構客戶資料分級之作法，客戶資料經隱私權保護目的處理後，可再區分為可識別客戶、不易識別客戶及不屬於個別客戶之資料等3級，其差別在於處理技術，爰本章針對處理技術進行說明。

(一)傳統去識別化技術之相關規範及案例

1. **傳統去識別化技術**[6]：包含 k-匿名(k-anonymization)、泛化等匿名化(anonymization)技術，與記號化(tokenization)等假名化(pseudonymization)技術，以下說明常見的傳統去識別化技術。
   (1) 抑制/編修(suppression/redaction)：將資料集內的識別資料移除或以標籤置換之，如：僅保留身分證字號後6碼或將身分證字號欄位刪除。
   (2) 遮罩(masking)：對資料局部置換為特殊符號，如：○或※。
   (3) 記號化(tokenization)：將原始資料變化為另一組隨機產生，但與真實資料樣態相同之值，如：將身分證字號置換為另一組符合身分證字號編碼原則的字號，但不是真實資料。
   (4) 雜湊化(hashing)：將敏感資訊套用函數產生出固定長度的雜湊值，並取代原始資料，如 SHA-256。
   (5) 泛化(generalization)：依預先定義之層次結構，降低識別資料之精確度，如：將年齡25歲，泛化為年齡20~29歲。
   (6) k-匿名化(k-anonymization)：結合各種去識別化技術，並確保經處理之資料集的任何一筆資料，其可用於識別出個體的背景資訊皆至少與 k-1 筆資料相同。
2. **我國涉及去識別化之相關判決**[7]：歐盟及日本等國皆對去識別化訂有相關規範(詳附件二)，目前我國法規並無所謂「去識別化」一詞，而是以個資法「無從識別特定之當事人」作為相關法定義務或限制規範之除外事由，「去識別化」(無從識別特定當事人)之內涵與程度以及如何達成去識別

[6] 數位發展部「隱私強化技術應用指引」(民113)。檢自 https://moda.gov.tw/digital-affairs/plural-innovation/operations/270 (Mar. 20, 2024)

[7] 洪杉源、楊秉哲、徐煒儀、李佳熹、吳佳琳(民112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

化係重要法律爭點。相關判決[8]整理如下：

(1) 判決一：個人資料經過編碼方式加密處理即完成去識別化—臺北高等行政法院 103 年度訴更一字第 120 號判決要旨，略以：「資料經過編碼方式加密處理後，處理後之編碼資料已無從直接或間接識別特定之個人，只要原資料保有者並未將對照表或解密方法等連結工具提供給資料使用者，其釋出之資料無法透過該資料與其他公眾可得之資料對照、組合、連結而識別出特定個人時，該釋出之資料即屬無法直接或間接識別之資料而達法律規定去識別化之程度。」

(2) 判決二：雖個人資料之去識別化作業尚有漏洞，但識別作用實際上已大幅度降低—最高行政法院 106 年度判字第 54 號行政判決要旨，略以：「大型資料庫之建置，對量化之實證研究極其重要，如容許自由資料之自由退出，易造成取樣偏誤。而資料庫內容所能適用之實證研究領域，職掌視野較大之公務部門亦較有認識可能性，主管機關將資料交給其上級機關建置資料庫，目的在追求資料之更高使用效率，此項高使用效率之追求為資料處理之給定目的；在此目的下，如能夠去識別化，即無比例原則下必要性要件之違反。此外，雖個人資料之去識別化作業尚有漏洞，但識別作用實際上已大幅度降低。」

(3) 判決三：去識別化是否大幅降低對個人資訊隱私權所生之侵害—憲法法庭 111 年憲判字第 13 號判決未明確說明資料去識別化之程度，而係針對經處理之資料是否仍屬個資進行說明，其判決內容略以：「個資若經處理，依其資料型態與資料本質，客觀上仍有還原而間接識別當事人之可能時，無論還原識別之方法難易，若以特定方法還原而可間接識別該個人者，其仍屬個資。」該判決亦進一步說明經處理之健保資料仍屬個資之判斷因素：「查個人健保資料包含系爭規定一之高敏感特種個資，具有高度個體差異，於客觀上非無以極端方式還原而間接識別特定當事人之可能性，此為科學上之事實。因此，個人健保資料無論為原始型

[8] 臺北高等行政法院 103 年度訴更一字第 120 號判決。

態或經處理，均必然仍屬『得直接或間接識別該個人』之資料，當事人對於此類資料之自主控制權，受憲法保障。」另該判決亦闡釋所謂「去識別化措施之義務」:「使一般人採取當時存在技術與合理成本，在不使用額外資訊時，不能識別特定當事人。雖個人健保資料於客觀上非無以極端方式還原而間接識別特定當事人之可能性，惟系爭規定一所採之去識別化手段已足大幅降低蒐用個人健保資料所生之個人資訊隱私權所生之侵害。」

(二)國際上主要國家運用傳統去識別化技術後遭還原之案例[9]

近來各國皆有運用去識別化技術後遭還原之相關案例(詳附件三)，相關案例並非機構因為資安議題導致被駭客取走個資，而是機構在進行資料共享時認為資料業經過一定程度去識別化處理而公開，但仍被有心人士或學術機構結合其它資料嘗試推論，導致部分個資仍產生被還原之狀況。

根據統計，截至 2022 年，全球金融產業因資料外洩所付出之平均成本高達 597 萬美元，較 2021 年的 572 萬美元為高，由於金融產業屬高度監理產業，相關法遵成本相對較高，因此亦高於全球不分產業別之平均成本 435 萬美元。臺灣企業在資料隱私保護上投入之成本約 200 萬美元，相較之下恐仍有不足。同時基於上述個資去識別化還原之案例，顯示即使經去識別化後之資料，仍有機會結合外部資料進行推論，進而還原成原始資料，無法完全規避相關法律風險。

(三)對於客戶資料保護及傳統去識別化技術之正確觀念[10]

從上述我國法規、函釋、判決及國際上個資去識別化後遭還原之案例可知，去識別化後之個資，仍為個資，應遵循個資法規範。曾有金融機構認為經傳統去識別化技術後之客戶資料即非個資，不受個資法規範，惟實務上仍

[9] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

[10] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

可能存有還原或識別之風險，因此應導正金融機構對於傳統去識別化技術之觀念：去識別化主要係作為強化隱私權保護之手段，而非採行相關技術後即可豁免個資規範。去識別化之資料運用，仍須搭配我國相關目的事業主管機關及金管會發布之相關規範或指引，且金融機構仍宜建置內稽內控、資安防護措施以及風險評估機制，將風險控制在可控範圍後，始得進行運用。

(四)新興隱私強化技術之發展與案例

1. **國際上新興隱私強化技術之發展**[11]：有鑑於傳統去識別化技術存在安全性及有效性之疑慮，國際上陸續推動新興隱私強化技術之政策與法規制度，如：聯合國於 2020 年成立聯合國隱私強化技術實驗室(UN PET Lab)，並與美國人口普查局(U.S. Census Bureau)、荷蘭中央統計局(Statistics Netherlands)、義大利國家統計局(Italian National Institute of Statistics)以及英國國家統計局(UK's Office for National Statistics)共同合作，展開測試計畫，藉由隱私強化技術的導入，促進資料共享並同時兼顧資料之安全性與遵法性。此外，為了推廣隱私強化技術，英國資訊委員辦公室(Information Commissioner's Office，ICO)於 2023 年 6 月發布「隱私強化技術指引」，介紹常見的 8 種新興隱私強化技術(包含：同態加密、安全多方運算、私有集合交集、聯合學習、可信執行環境、零知識證明、差分隱私、合成資料等)，並詳細說明各技術之優缺點、與「個人資料保護相關法規」遵循之關聯、應用時之注意事項、相關風險等內容，提供組織依其目的，評估並選擇適當之隱私強化技術。
2. **我國數位發展部對於隱私強化技術之說明**：數位發展部於 113 年 1 月發布「隱私強化技術應用指引」[12]，指出廣義上之隱私強化技術係包含傳統去識別化技術(常見技術有：抑制/編修、遮罩、記號化、雜湊化、泛化及 k-匿名化等)，並針對 5 種具指標性之新興隱私強化技術(包含同態加

[11] 數位發展部「隱私強化技術應用指引」(民 113)。檢自 https://moda.gov.tw/digital-affairs/plural-innovation/operations/270 (Mar. 20, 2024)
[12] 數位發展部「隱私強化技術應用指引」(民 113)。檢自 https://moda.gov.tw/digital-affairs/plural-innovation/operations/270 (Mar. 20, 2024)

密、差分隱私、安全多方運算、合成資料及聯合學習)說明其運作概念、應用情境、施用風險與限制等。

(1) 同態加密(Homomorphic Encryption)：是一種密碼學技術，採用有同態性的加密演算法可以直接對已加密的資料進行運算，且可產生與運算未加密資料一致的結果。這項技術可用以確保資料在傳輸、運算及輸出運算結果的過程中，全程將資料維持在加密狀態，對須將機敏或隱私資料傳輸委由他人執行運算的情境下，保障了資料的機敏性。

(2) 差分隱私(Differential Privacy)：是一種保護個人資料隱私的方法，通過在資料中加入一定的雜訊，使得資料釋放後不會揭露個人資訊。差分隱私廣泛應用於資料共享、資料挖掘、機器學習等領域，可有效保護敏感資訊的隱私，同時保持資料的可用性和可分析性。

(3) 安全多方運算(Secure Multiparty Computation)：安全多方運算允許多個參與者在不洩漏自身秘密輸入(值)的情況下，實現聯合計算。

(4) 合成資料(Synthetic Data)：是一種生成資料的技術，藉由數學模型或演算法，產生與真實資料相近的人造資料，其具有真實資料的統計特徵與結構，可以在不透漏真實資料的情況下，替代真實資料進行統計分析、機器學習訓練等應用。此技術被廣泛應用於軟體測試、消除機器學習模型偏差、標註深度學習資料標籤與保護隱私資料等不同用途。

(5) 聯合學習(Federated Learning)：是一種具隱私保護機制的分散式機器學習方式，其主要架構是由多個擁有訓練資料的分散式端點及一個伺服器所構成。透過聯合學習各分散式端點可利用其資料集訓練本地模型，並僅傳輸該本地模型之參數至伺服器進行全域模型更新，從而實現毋須傳輸本地端真實資料但仍可參與機器學習訓練的目的。

3. **國際上新興隱私強化技術之應用案例**[13]：聯合學習及合成資料等 2 項技術因個別客戶原始資料不離開金融機構，為目前主要國家監理機關及金融業較常使用之技術，其應用案例列舉如下。

[13] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

(1) 聯合學習應用案例 1—新加坡主管機關打造聯合學習平臺提供中小企業信貸風險評估：新加坡政府為解決中小企業信貸資料蒐集不易之議題，於 2021 年年底基於新加坡國立大學(Nationa University of Singapore, NUS)亞洲數位金融研究所(Asian Institute of Digital Finance, AIDF)培育的新創 Criat 發展之「智慧信用分析資料共享系統(Intelligent Credit Analytics Sharing System, iCASS)」，由新加坡金融管理局(MAS)推出首個聯合學習平臺「中小企業信貸資料共用聯盟(SME Credit Analytics Consortium)」，參與本平臺之金融機構可透過該聯合學習之方式，貢獻各自機構機器學習訓練後之參數，再集結多間金融機構之參數，統整產出一優化之信貸評估模型，各金融機構可共享此信貸評估模型，用以減少金融機構風險、並降低中小企業所須承擔的利率，並可衍生開發更好的違約與債務回收評估模式。

(2) 聯合學習應用案例 2—日本銀行業運用聯合學習於貸款違約率預測：日本三井住友銀行曾與五家不同銀行進行聯合學習之概念實證，以測試機器學習模型在貸款違約率預測上之表現。資料分別是位於關東地區的 A 銀行，約有 4 萬筆客戶資料，以及另外 B、C、D、E 四間銀行，分別為 4 萬、1 萬 5、8 千、4 千筆資料，資料欄位約 180 個(例如：年齡、年收、帳戶餘額等)。實證時切分各銀行資料分為訓練資料與測試資料，分別透過 A-B、A-C、A-D、A-E 兩兩採用聯合學習方式，利用訓練資料訓練模型後再以測試資料進行驗證，實驗結果雖然對於資料量最多的 A 銀行在借貸違約率準確率並無顯著提高，但對於資料量較小的銀行在借貸違約率準確率上得到提升。

(3) 聯合學習應用案例 3—日本銀行業運用聯合學習偵測非法匯款：日本國家研究單位情報通信研究機構(National Institute of Information and Communications Technology, NICT)網路安全研究所與國立神戶大學共同開發「DeepProtect」技術，在 2022 年與千葉銀行、三菱 UFJ 銀行、中國銀行(中国銀行)、三井住友信託銀行、伊予銀行以及數位風險科技

公司艾特拉斯(Eltes)合作進行概念驗證，結果對非法匯款交易之偵測準確率達 80%，可用於提早偵測疑受詐欺之帳戶。

(4) 合成資料應用案例 1—英國銀行業運用合成資料服務於系統開發測試資料：Synthesized 是一間人工智慧新創，聚焦於解決人工智慧與機器學習在領域資料缺乏的難點，例如：金融、醫療等領域的資料，因為領域受高度監理，在取得資料之授權上成本高，除了需時間逐筆取得使用者同意以外，若資料運算量大，需要傳輸至雲端執行機器學習訓練，還有資料至雲端之合規管理議題需處理。Synthesized 目前在金融領域合成資料上已有實際商業化的應用，例如：協助德意志銀行(Deutsche Bank)改善開發系統產品在測試時遇到的難點。Synthesized 的合成資料服務效益主要有以下三點：第一、在無須使用者同意授權下，可由系統產生具品質且符合規範之合成資料，減少金融機構資料蒐集所需時間，提升人工智慧、機器學習模型在雲端上的訓練效能。二、協助用於金融機構提供外部資訊服務供應商發展新應用時之測試資料，資訊服務供應商可透過合成資料確認所開發新應用是否符合需求，縮短金融機構概念驗證之迭代週期。三、協助金融機構本身資訊部門在開發新應用初期即導入測試左移(Shift Left Testing)的安全性開發原則，在設計開發階段即透過合成資料進行相容性測試，可在產品正式發布前，提早部署測試計畫，降低產品正式發布後修正所需成本與時間。目前 Synthesized 提供銀行軟體開發套件(Software Development Kit, SDK)的方式，應用於偵測詐欺的機器學習模型訓練，透過 SDK 可在約 10 分鐘時間內產出 500 萬筆符合規定及銀行需求之合成資料，機器學習模型之表現較未導入合成資料前，約可提升 4~15%。實際上亦節省銀行資料處理所需 2~4 個月之處理時間。

(5) 合成資料應用案例 2—歐盟銀行業運用合成資料服務於系統開發測試資料：歐盟奧地利第一儲蓄銀行(Erste Bank)在開發系統時，因測試資料需調用歷史資料，且部分系統功能如通知(notifications)或觸發事件

(triggers)等亦需歷史以及未來的資料，但在這種功能測試情境中，歷史資料無法滿足需求，因此該銀行採用 2017 年成立於奧地利的金融科技公司 Mostly AI 之系統，在需要通知或觸發事件的測試資料時，僅設定好合成資料條件，即生成一套包含歷史與未來資料的合成資料供測試。另外，為遵循歐盟 GDPR 規範，測試資料有強制的資料保存期限(data retention)，成立於 2019 年的義大利金融科技公司 Clearbox AI 透過生成 120 萬筆合成資料，協助銀行將即將到期須刪除的資料轉成合成資料，並且在機器學習模型表現上，可達原始資料 95%以上的水準。

(6) 合成資料應用案例 3—新加坡主管機關運用合成資料於隱私增強技術沙盒中：由新加坡通訊及媒體發展管理局(Info-communications Media Development Authority, IMDA)與新加坡 PDPC 共同推出，該隱私增強技術沙盒亦與金融科技業者合作。成立於 2021 年的新加坡金融科技新創 BetterData 被選為隱私增強技術沙盒的技術供應商，該公司所研發之技術，可基於企業原始資料進行無人為介入的學習，生成合成資料，並視需求採用本地端或雲端架構服務，針對日期、數字、浮點數以及分類，進行生成式 AI 的模擬。目前 BetterData 使用合成資料應用於金融機構提升風險模型表現，及用於洗錢防制與詐欺偵測，目前仍在概念驗證階段。

(7) 合成資料應用案例 4—日本保險公司運用醫療合成資料於核保風險評估：保險公司為了精算醫療保險之風險，往往需要借重大數據進行輔助判斷，然而保險公司客戶有限，往往需要外部資料之協助。日本 LifeNet 保險公司(ライフネット生命保険株式会社)在 2023 年 3 月 29 日宣布與日本最大醫療數據公司 JMDC(株式会社 JMDC)合作概念實證，保險公司將針對 JMDC 的「AI 核保風險預測服務」以及基於合成資料的「虛擬 My Number Portal Data(仮想マイナポータルデータ)」進行概念實證。JMDC 自 2005 年開始累積醫療數據，至今已累積超過 1,400 萬名用戶資料，包含醫療收據資料以及健康檢查結果；為提升資料運用效益，

JMDC 透過模擬方式產生 1,200 萬人合成資料，提供保險公司在核保上更精準之判斷。

【諮詢問題】

8. 您認為這些隱私強化技術是否有利於資料共享時之資料保護？
9. 您認為這些技術是否有潛在風險？

(五)金融機構客戶資料分級與各項處理技術之關係

依據前述金融機構客戶資料分級之作法，本文件嘗試將客戶資料經隱私權保護目的處理後，再區分為易遭還原而識別客戶、較不易遭還原而識別客戶及不屬於個別客戶之資料等，各分級與處理技術之關係如下。

第1級.原始客戶資料：未經處理之資料。

第2級.經隱私權保護目的處理後，仍易遭還原而識別客戶之資料：經傳統去別化技術處理後之資料。

第3級.經隱私權保護目的處理後，較不易遭還原而識別客戶之資料：經新興隱私強化技術處理後之資料。

第4級.不屬於個別客戶之資料：經聯合學習所產生之參數資料，及合成資料。

【諮詢問題】

10.您認為上述客戶資料分級與處理技術之關係是否妥適？
11.您對技術處理是否有其他建議？

六、 金融機構客戶資料分級及治理方式

金融機構規劃資料共享及其利用場景時，應同時考量隱私權保護之資料安全面與取得客戶同意之作業成本面因素，以決定採取何種級別資料辦理資料共享，並遵循下列各級資料之對應治理方式。

第1級.原始客戶資料：因屬原始客戶資料，須於高度保護環境下進行資料共享。

1. 高度保護環境：

(1) 須遵循個資法規，並逐項取得客戶同意。

(2) 資料共享之對象：以金融機構為原則，惟依據開放銀行等機制辦理之資料共享，不在此限。

2. 運用情境舉例：辦理金融往來業務或便利客戶作業。

第2級.經隱私權保護目的處理後，仍易遭還原而識別客戶之資料：因尚可識別客戶，宜於高度保護環境下進行資料共享。

1. 高度保護環境：

(1) 遵循個資法規，並逐項取得客戶同意。

(2) 資料共享之對象：以金融機構為原則，惟對於資料治理及隱私權保護強度等同金融機構之非金融機構，亦可評估納入分享對象。

2. 運用情境舉例：辦理分析比對及風險控管。

第3級.經隱私權保護目的處理後，較不易遭還原而識別客戶之資料：因不易識別客戶，爰可採較具彈性之資料治理方式，於中度保護環境下進行資料共享。

1. 中度保護環境：

(1) 遵循個資法規，並可採取較簡易之方式以取得客戶同意。

(2) 資料共享之對象：金融機構及非金融機構，其中非金融機構應具備妥適之資料治理及隱私權保護能力。

2. 運用情境舉例：辦理業務發展及行銷策略。

第4級.不屬於個別客戶之資料：因不屬於個別客戶之資料，可於低度保護環境下進行資料再利用(不涉及共享個別客戶之資料)。

1. 低度保護環境：

(1) 無個資法規之適用。

(2) 資料再利用之對象：金融機構及非金融機構。

2. 運用情境舉例：辦理 AI 及機器學習之訓練模型、產業市場調研或與學研機構合作學術研究。

【諮詢問題】

12.您認為這樣的分級治理方式是否妥適？

13.您對於運用情境之舉例，是否有建議新增之例子？

14.針對第 1 級與第 2 級之「高度保護」並須逐項取得客戶同意之作法，您覺得實務上應如何處理較符合「高度保護」？應如何提升客戶之信賴？有何種方式可逐項取得客戶之同意且遵循個資法規範？

15.針對第 3 級之較簡易方式以取得客戶同意之作法，您覺得實務上應如何處理較符合「中度保護」？應如何提升客戶之信賴？有何種方式可較簡便取得客戶之同意且遵循個資法規範？

16.針對第 3 級，倘採取較簡易方式取得客戶同意者，是否應一併讓客戶明確瞭解運用情境(如：辦理業務發展及行銷策略)及資料共享對象(如：具備妥適之資料治理及隱私權保護能力之非金融機構)，以減少後續產生爭議之可能？

17.您認為聯合學習所產生之參數資料及合成資料是否不屬於個別客戶之資料，而毋須適用個資法規？

18.您認為資料治理方式是否需就倘共享資料於蒐集、處理及利用過程中，不當處理而受侵害，增訂應如何處理之指引，以供相關利害關係人參考？

19.您對資料分級治理是否有其他建議？

七、 金融機構辦理資料共享治理之原則與政策

(一)資料共享治理之原則

1. 遵循二(二)所述客戶資料保護與資料治理一節所揭示之「遵法、公平及透明」、「目的限制」、「資料最小化」、「正確性」、「儲存限制性」及「完整性與機密性」等 6 原則。
2. 避免利益衝突[14]：金融機構資料共享應避免損及資料當事人權益、避免利益衝突或影響市場之情事。
3. 公開、透明及告知[15]：提供予資料當事人有關金融機構處理資料之政策、程序及實務等資訊，包含共享之單位、共享目的、資料當事人表達同意或不同意共享之選項及方式。
4. 資料當事人有權參與及存取[16]：以簡單、快速及有效率之方式，給予資料當事人存取、審查、修正或移除其資料之權利。
5. 可歸責性[17]：

(1) 金融機構、資料接收者或處理者皆須採取適當之資料治理措施，並須評估任一方是否同樣具備良好之資料治理能力，以確保對方提供相同等級之隱私權保護(如：經由契約或對方內部政策)。

(2) 設立有效率之申訴管道及補救措施供資料當事人使用，包含資料當事人於隱私權受侵害時之可採取方案。

【諮詢問題】

20.您認為所列資料共享治理之原則，是否足夠且妥適？

21.您對資料共享治理原則是否有其他建議？

[14] 洪杉源、楊秉哲、徐燁儀、李佳熹、吳佳琳(民 112)。*金融服務提供者跨機構或跨市場資料共享之資料分級及資料治理規範*。財團法人金融聯合徵信中心委託之專題研究成果報告，未出版。

[15] 參考 CNS29100 之隱私權原則。

[16] 參考 CNS29100 之隱私權原則。

[17] 參考 CNS29100 之隱私權原則。

(二)建立資料共享治理之政策及制度

1. **金融機構應訂定資料共享治理政策**：金融機構於衡量資料共享之風險因素後，依風險程度參採前述原則，訂定資料共享治理政策或制度，內容包含但不限於：
   (1) 符合個資法規範之程序、隱私權保護政策及其風險評估與管理機制、定期評估資料治理妥適性、員工教育訓練及相關內控規範。
   (2) 該政策或制度須包含資料共享前、共享期間及共享後之措施。
2. **建立資料治理制度**：參考 ISO/IEC 38505-1:2017 國際標準，建立資料治理制度。

【諮詢問題】

22.您認為所列資料共享治理政策或制度，是否足夠且妥適？

23.所列資料治理制度之國際標準，您認為其是否妥適？

24.您對金融機構訂定資料治理政策或制度是否有其他建議？

八、 結語

隨著金融機構對於資料共享之需求日益擴大，如何讓業者在遵循個資法相關規範及隱私權保護的前提下，發揮資料之價值與效益，係金融科技發展之未來方向之一。金管會觀察國際新興隱私強化技術之發展趨勢，期望在符合我國個資法規範與隱私權保護相關機制下，促進金融業跨機構、跨市場進行資料共享，爰發布本諮詢文件以蒐集利害關係人之意見，作為後續擬具「金融機構資料共享之資料治理指引」之參考，希冀金融機構、科技與資訊業者及數據與法律專家等跨界交流，共同提出資料共享之創新解決方案，提升整體金融市場之數位發展及客戶之金融服務體驗。

九、 意見回饋

如您對本諮詢文件所詢任一問題欲表達意見，請於本文件發布日起 60 日內，以電子郵件寄至 fintechcenter@fsc.gov.tw。如您就本諮詢文件辦理程序有疑問，可電話洽詢金管會創新中心：(02)8968-0120。

附件一：諮詢問題

1. 您認為金融機構辦理客戶資料共享時，還受到哪些本文件尚未敘及之規範？尤其在遵循個資法相關規定情形下，金融機構實務運作上還遇到什麼挑戰？
2. 針對本文件提出之客戶資料分級作法，您認為是否有利於辦理跨機構間資料共享？亦即是否可發揮資料共享之效益及是否可發揮隱私權保護之目的？
3. 這樣的分級作法，您認為是否有潛在風險，為什麼？
4. 您是否認同本分級作法與資料治理之關聯？
5. 您是否有其他客戶資料分級之建議？
6. 您認為所列金融機構辦理客戶資料共享之應用場景是否足夠？是否還有其他場景應列出?
7. 您對應用場景是否有其他建議？
8. 您認為這些隱私強化技術是否有利於資料共享時之資料保護？
9. 您認為這些技術是否有潛在風險？
10. 您認為上述客戶資料分級與處理技術之關係是否妥適？
11. 您對技術處理是否有其他建議？
12. 您認為這樣的分級治理方式是否妥適？
13. 您對於運用情境之舉例，是否有建議新增之例子？
14. 針對第 1 級與第 2 級之「高度保護」並須逐項取得客戶同意之作法，您覺得實務上應如何處理較符合「高度保護」？應如何提升客戶之信賴？有何種方式可逐項取得客戶之同意且遵循個資法規範？
15. 針對第 3 級之較簡易方式以取得客戶同意之作法，您覺得實務上應如何處理較符合「中度保護」？應如何提升客戶之信賴？有何種方式可較簡便取得客戶之同意且遵循個資法規範？
16. 針對第 3 級，倘採取較簡易方式取得客戶同意者，是否應一併讓客戶明確瞭解運用情境(如：辦理業務發展及行銷策略)及資料共享對象(如：具

備妥適之資料治理及隱私權保護能力之非金融機構)，以減少後續產生爭議之可能？

17.您認為聯合學習所產生之參數資料及合成資料是否不屬於個別客戶之資料，而毋須適用個資法規？

18.您認為資料治理方式是否需就倘共享資料於蒐集、處理及利用過程中，不當處理而受侵害，增訂應如何處理之指引，以供相關利害關係人參考？

19.您對資料分級治理是否有其他建議？

20.您認為所列資料共享治理之原則，是否足夠且妥適？

21.您對資料共享治理原則是否有其他建議？

22.您認為所列資料共享治理政策或制度，是否足夠且妥適？

23.所列資料治理制度之國際標準，您認為其是否妥適？

24.您對金融機構訂定資料治理政策或制度是否有其他建議？

附件二：國際上主要國家針對去識別化技術之相關規範

1. 英國對於去識別化技術之規範：英國在匿名化與假名化之區別上，主要仍依循歐盟 GDPR 之概念，匿名化之資料原則上不受個資之規範，但是需要刪除個人資料中足夠多的元素，以達到無法再識別個人之程度；而假名化之個人資料需藉由適當的技術或處理措施增加識別特定個人的難度，以達到降低隱私風險之個資保護目的，惟因仍可透過其他附加資訊加以識別特定自然人，故仍應受相關個資規範之控管。
2. 歐盟對於去識別化技術之規範：歐盟 GDPR 前言第 26 點闡明資料去識別化的相關重點：「個人資料保護原則應適用於有關識別或可得識別當事人之任何資訊。已假名化之個人資料，可透過使用額外資訊而識別出當事人身分，應被認為屬於可得識別之當事人的資訊。為決定當事人是否可被識別，應考慮到所有可合理使用之方法，例如：由控管者自己或透過他人指認以直接或間接地識別該當事人。為確認何為可合理使用作為識別當事人之方法，應考慮所有客觀因素，例如：識別所需之成本與時間，並考慮到資料處理當時現有之技術及科技發展。因此，資料保護原則不適用於匿名化資訊，即非已識別或可識別當事人之資訊，或以使資料主體不可或不再可識別之方式而成為匿名化之個人資料。因此，本規則無涉於此類匿名化資訊之處理，包括為統計或研究目的所為之者。」同時，GDPR 對於假名化及匿名化資訊(anonymous information)有明確之區分，「假名化」係指處理個人資料之方式，使該個人資料在不使用額外資訊時，不再能夠識別出特定之資料主體，且該額外資訊已被分開存放，並以技術及組織措施確保該個人資料無法或無可識別出當事人。換言之，經假名化之資料仍可能透過使用額外資訊加以識別出當事人身分，故仍為應受保護之個人資料；反之，經匿名化之資訊則無法再行識別，因而不受 GDPR 之拘束。
3. 新加坡對於去識別化技術之規範：新加坡個資保護委員會(Personal Data Protection Commission, PDPC)於 2013 年 9 月公布「針對特定主題之個人

資料保護法諮詢指引(Advisory Guidelines on the Personal Data Protection Act for Selected Topics)」，就 PDPC 本身之解釋而言，去識別化(de-identification)與匿名化並不相同。經過去識別化之資料，雖已去除直接識別資料，但仍能夠簡單地透過其他資料再識別特定個人；而經匿名化之資料，則原則上無法再識別特定個人。因此僅有經匿名化之資料不適用個人資料保護法(Personal Data Protection Act)相關規定。

4. 日本對於去識別化技術之規範：2015 年原個情法創設「匿名加工資料(匿名加工情報)」制度，通過對資料進行一定程度的匿名化處理，可以將其作為大數據加以利用，惟針對匿名加工資料須達到「經過處理後無法識別特定個人且無法恢復個人資料之資料」。施行後，企業多反應因匿名加工所要求之加工程度非常高，加工程序很困難；且所謂「無法恢復個人資料」幾乎不存在，致企業無法安心利用此制度。相較於匿名加工資料，2020 年修法增訂「假名加工資料」制度，「假名加工資料(仮名加工情報)」以企業內部自用為前提，對個資採低度去識別化加工，對處理技術的要求也較低。假名加工資料係指加工於特定個資後，只要其未與其他資料為組合、比對，即無法識別出特定個人之加工資料。假名加工資料僅限於企業內部提供給市場拓展、產品開發上研究之用，不能將之提供給第三人，與匿名加工資料有不同之限制規範。

附件三：國際上主要國家運用傳統去識別化技術後遭還原之案例

1. 美國 AOL 案：2006 年美國線上(AOL)曾公開發布 65 萬 7000 名用戶約 2000 萬筆的匿名之搜尋資料，由於 AOL 處理方式是將使用者 id 透過假名化方式以代碼取代，仍被美國紐約時報從匿名搜尋資料中識別出一位居住於喬治亞 62 歲女性，後續又陸續有其它用戶的真實身分被識別出來。最終 AOL 為此以 500 萬美元和解。此一案例足見匿名化處理若未經過謹慎審核即對外發布，將造成個資外洩事件。
2. 美國 Netflix 案：自 2006 年起，影音串流平臺 Netflix 曾舉辦「Netflix Prize」的技術挑戰賽，釋出約 48 萬名用戶針對 1 萬 7 千部電影超過 1 億筆電影評分作為訓練資料，包含用戶 id、評分日期、電影、評分，廣邀技術團隊運用訓練資料開發出可預測用戶對電影評分之準確度。儘管 Netflix 聲稱用戶 id 已經過匿名處理，但後來仍有學術機構結合外部資料(IMDB 電影評分網站)，將用戶真實身分識別出來，而 Netflix 也在 2009 年宣告停止舉辦競賽。
3. 澳洲醫療公開資料案：澳洲健康部(Department of Health)於 2016 年 8 月曾發布上億筆經匿名化之公開資料用於研究用途，如：健保資料(Medicare)與藥品補貼計畫(Pharmaceutical Benefits Scheme, PBS)，涵蓋約 290 萬位使用者資料，紀錄範圍自 1984 年起至 2016 年，而 2017 年墨爾本大學(University of Melbourne)研究團隊從中透過外部資料(如： 信用卡歷史資料)的輔助，比對生產、運動傷害以及手術資料，推論出 43 筆可能還原之個資資料，而其中有 7 筆最終完全比對至真實個資。研究團隊通知有關當局下架資料，當局於 6 週後下架時已有 1,500 次下載數。
4. 歐盟丹麥 Taxa 4x35 案：2019 年位於丹麥的一家計程車公司 Taxa 4x35 遭丹麥資料保護局(Danish Data Protection Agency, Datatilsynet)通報警方有關其未遵守 GDPR 之規範及資料最小化原則等違法行為，並建議裁處 120 萬之罰鍰。該公司聲稱其用於預約及結算計程車服務所蒐集之客戶個資均會於 2 年後進行匿名化措施，惟經丹麥資料保護局檢查發現，該

公司於 2 年期限屆至後所為之匿名化措施僅有刪除客戶之姓名，而仍保留客戶之電話號碼，直到 5 年後始加以刪除，透過該電話號碼即可能識別出特定客戶之相關資訊(該公司於 2018 受檢查時，共發現 8,873,333 筆保留超過 2 年之個資)。雖該公司辯稱所保留之電話號碼僅作為公司資料庫管理及業務發展使用，惟丹麥資料保護局認為此並不構成保留客戶個資之正當理由，該公司於沒有客觀目的之情形下儲存大量客戶個資，違反相關個資保護規範，故建議裁處罰鍰。此案最近一次法院判決為 10 萬丹麥克朗，但檢查官仍可上訴。

5. 歐盟瑞士最高法院案：法院遇到需保密的法律訴訟案，會將參與者進行匿名化處理，然後瑞士蘇黎世大學在 2019 年發布一項研究指出，可以透過結合金融機構的資料進行推論，識別出瑞士最高法院匿名的參與者。研究者在 12 萬件匿名的法院文件中透過它們開發之演算法，在有金融機構真實資料參照的前提下，可還原約 84%的匿名者身分。
6. 美國 Strava 案：運動訓練服務公司 Strava 開發出可以用視覺化方式呈現跑者跑步地理位置的 APP，目前受到使用者歡迎，根據統計，全球約有 9,500 萬名 Strava 用戶，並以 25%的速度持續成長中。該公司為了保護使用者隱私，避免洩漏使用者住家或公司之位置，採用一種「端點隱私區域 (Endpoint Privacy Zone, EPZ) 」的技術，可將起跑與結束的 GPS 路線做模糊化之處理。然而，仍有比利時研究團隊透過推論攻擊(inference attack)的方式，在小範圍的地圖中可以還原被模糊化之區域，準確率達 85%。