試析歐盟法上假名化資料是否屬個人資料之認定標準

巫承運

摘要

隨著數位經濟之興起，如何在資料流通與個資保護間取得平衡，已成當代核心議題，而假名化技術即為其關鍵解方。惟現行 GDPR 針對「附加資訊」之定義及「合理可能使用方法」之標準，仍有模糊空間。本文旨在透過分析歐盟最新「假名化指引」及歐盟法院指標性判例填補此一解釋缺漏。本文發現，判定是否構成「合理可能使用方法」，關鍵在於再識別風險，或者審視各方當事人間之關係，例如持有假名化資料者，是否具備透過法律途徑向第三方取得附加資訊之能力。然而，該標準本身缺乏特定或可量化指標，將導致法律上不確定性，也因為人工智慧等科技發展導致個人資料認定愈加複雜，因此本文認為未來歐盟應發布更具體之標準，亦應依照技術發展之狀況定期檢視個資之認定。

隨著現代數位科技的高速發展，資料的流通與處理已成為現代數位經濟的核心議題，而在歐盟境內嚴格的資料保護架構下，資料控制者（Data Controller[1]）在利用個人資料時，必須同時符合歐盟資料保護相關規則之要求。為尋求資料利用與資料保護之間的平衡點，假名化（Pseudonymisation）技術成為達成平衡之潛在關鍵。

根據歐盟「一般資料保護規則（General Data Protection Regulation, GDPR）」第 4 條第 5 項之定義，假名化係指對個人資料進行處理，使其在沒有「附加資訊（additional information）」的情況下，無法再將個人資料歸屬於特定資料主體，且此附加資訊必須被單獨保存並採取技術與組織措施，以確保個人資料不會被歸屬於已被識別或可被識別的自然人[2]。

其與「匿名化（anonymization）」不同，匿名化是指經處理之資料與原始資料及個人完全分離，沒辦法再回溯辨識，也因此匿名化資訊之使用不會受到歐盟資料保護架構的約束[3]。而假名化處理除了保有資訊回溯之可能，由於其

[1] Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4 (7), 2016 O.J. (L 119) 1, 33[hereinafter GDPR].
[2] *Id*. art. 4(5) ("pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person").
[3] *Id*. recital 26.

有假名之輔助，不需要透過「附加資訊」也可以透過相同之假名將同一個人的不同份資料連結在一起[4]，進而在資料運用上比匿名化的做法更加靈活。

然而，GDPR 也表示：所有能夠指向特定個人的資訊，無論是直接還是間接，都必須受到資料保護法規的保障。因此即使把一個人的資料做了假名化處理，但只要有辦法透過任何「合理可能使用方法（all the means reasonably likely to be used）」來取得額外資訊並解碼，重新找出這個人，那麼這份資料就仍然算是「個人資料」而必須被保護[5]。因此，從 GDPR 之規定觀察，假名化處理僅是將個人資訊被辨識的風險降低，仍舊不改變其作為「個人資訊」的本質。其與將資料從個人完全割裂，進而使資料不再可能回溯的「匿名化資料」有本質上的不同。

雖然 GDPR 定義了假名化資料對有「合理可能使用方法」取得附加資訊者而言，仍屬於個人資料。然而，GDPR 對於「何為附加資訊」以及「合理可能使用方法之內涵」並無過多著墨。另外，GDPR 也並未明確說明假名化資訊對於「沒有合理可能使用方法」獲取「附加資訊」之第三人而言，是否仍屬個人資訊之問題。以上皆有待後續實務發展之填補，也是本文欲探討之問題。

為解答以上問題，本文首先將由歐盟個人資料保護委員會（European Data Protection Board, EDPB）於今（2025）年 1 月推出的「假名化指引（Guidelines 01/2025 on Pseudonymisation）」進行分析，檢視歐盟官方機構對於「附加資訊」之詮釋。接著再透過分析歐洲法院在個人資料認定之議題所作的重要案例：*Breyer* 案[6]，以及今年 9 月甫作成之判決：*EDPS v. SRB* 案[7]，來檢視「合理可能使用之方法」之內涵與適用，並最後做一結論。

壹、歐盟假名化指引對附加資訊之解釋

根據歐盟假名化指引，假名化應該經過三道步驟才算完成[8]：首先，資料控制人或處理人應先修改或轉換資料，將可直接識別資料主體的符號置換成假名；其次，將用來辨識資料主體的「附加資訊」與假名化資料分別存放，最後透過「技術措施與組織措施（technical and organisational measures）」確保個人資料不被回溯到資料主體[9]。

---

[4] EUROPEAN DATA PROTECTION BOARD, GUIDELINES 01/2025 ON PSEUDONYMISATION 11 (adopted Jan. 16, 2025) [hereinafter GUIDELINES].
[5] GDPR, recital 26.
[6] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779 (Oct. 19, 2016).
[7] Case C-413/23, European Data Protection Supervisor (EDPS) v. Single Resolution Board (SRB), ECLI:EU:C:2025:645 (Sep. 4, 2025).
[8] GUIDELINES, *supra* note 4, at 7.
[9] 技術措施具體包含：網路分段（Network segmentation）、在硬體安全模組（Hardware Security Modules）中儲存秘密金鑰、應用程式介面身份驗證（Secure authentication for API access）與日誌記錄（logging）。組織措施則包含：僱用經過審查與特別授權的人員來操作用於執行假名化轉換與儲存假名化密鑰的系統，並提供所有會與資料主體互動與存取假名化資料之人員適當培訓。*See id*. at 24-25.

而所謂「附加資訊」係指在假名化過程中產生，並可用於將假名化資料回溯到個人之資訊[10]，也就是為了未來能夠將假名化資料還原成原始資料而保留下來之資訊，其中可能包含將假名（pseudonyms）與它們所替代的識別屬性（identifying attributes）進行匹配的表格或者加密密鑰等[11]。

依照上述說明，理論上對於實際經手個人資料之資料控制人或資料處理人而言，其擁有能將假名化資料還原成原始個資的附加資訊，因此對此類實際經手處理個人資料者而言，假名化資料應仍為個人資料。然而，附加資訊不一定由資料控制人或資料處理人持有，而可能是由第三方持有，甚至是存在於網路論壇等公共空間[12]。當這種處於資料處理人及控制人掌握以外的附加資訊存在時，若有第三人能將假名化資訊與附加資訊透過「合理可能使用方法」結合，則該資訊對該第三人而言亦屬於個人資料[13]。

綜上所述，鑑於「附加資訊」乃是回溯或識別資料主體之關鍵，其自應被視為「合理可能使用方法」的核心要素。準此，由何人持有該附加資訊，或何人具備透過「合理可能使用方法」取得該資訊並將其與假名化數據結合之能力，便成為認定該數據對特定當事人而言是否仍屬「個人資料」之決定性因素。惟「假名化指引」對於「合理可能使用方法」之具體內涵與定義，似未有詳盡之闡釋。有鑑於此，本文將於次節透過歐盟法院之相關判例，針對此一議題進行更深入之實務分析。

貳、歐盟法院對於「合理可能使用方法」之解釋

在解釋「合理可能使用方法」時，究竟何人可以合理的取得回溯或再識別個人的方法，乃是最重要的問題。對此，歐洲法院的 *Breyer* 案以及 *EDPS v. SRB* 案提供了極具參考性的實務見解。

在 *Breyer* 案中，當事人參訪德國公家機關網站，發現網站會為了防止網路攻擊與盜版等目的，而將當事人參訪之頁面、檔案、輸入之關鍵字與使用者 IP 位址等資訊儲存在網站伺服器[14]。但單憑這些資訊，網站經營者並不能識別使用者，其唯有在網路服務供應商提供使用者身分資訊之後，始能識別出當事人[15]。

此處所謂「與使用者身分相關之資訊」，即相當於前述概念中的「附加資訊」。因此，本案之核心爭點在於：當附加資訊掌握於第三方（即網路服務供應商）手中時，網站經營者是否可能將 IP 位址與該附加資訊結合以辨識資料主體，此種結合之可能性是否已構成所謂「合理可能使用方法」[16]？

[10] *Id*. at 9.
[11] *Id*.
[12] *Id*.
[13] *Id*. at 1.
[14] Case C-582/14, paras. 13-14.
[15] *Id*. para. 24.
[16] *Id*. para. 45.

對此，法院認為，鑑於網站經營者在遭受網路攻擊時，具備透過「法律途徑（legal channels）」請求主管機關介入，進而向網路服務供應商取得相關資訊之可能性。故認定網站經營者有可能取得附加資訊，確實擁有「合理可能使用方法」，可以取得附加資訊以辨識 IP 位址背後之資料主體[17]。

而在 *EDPS v. SRB* 案中，歐洲法院在認定「合理可能使用方法」時採取與 *Breyer* 案相同的標準，並且對其做了更深入的詮釋。歐洲法院認為，在考量是否存在「合理可能使用方法」時必須考量在現實中，再識別資料主體的風險是否「微不足道（insignificant）」。換言之，若這些再識別的方法本身係被法律所禁止，或者在實務上不可行（比方需耗費完全不成比例的時間、成本及勞力才有可能做到），進而應判斷該方法在客觀上「不可能使用」[18]。

此外，歐洲法院認為，不得武斷地認定假名化資料在「所有情境下、對任何人」而言均構成個人資料。若個人資料經假名化處理後，已使除原始資料控制者以外之第三人無法再識別出資料主體，則對該第三人而言，該數據即非屬個人資料[19]。

參、歐洲法院判斷標準分析

有論者認為，歐洲法院在實務上所採用之「合理可能使用方法」，其標準實質上採用一種「基於風險（risk based）」的判斷標準，比方在 *Breyer* 案中，法院認為法律原則上禁止網路服務供應商向網站經營者傳輸附加資訊，但若網路攻擊發生，網站經營者即可向網路服務供應商取得附加資訊。但網路攻擊很可能發生，故本案中附加資訊被取得而導致資料主體被再識別，是一種「合理之風險」，僅因網站經營者得依法取得附加資訊，而被認定有「合理可能使用方法」之標準並非過度嚴苛[20]。同樣的，*EDPS v. SRB* 案也是採用相同標準，以再識別風險作為標準判定[21]。

另有論者認為，判斷是否存在「合理可能使用方法」時，應聚焦於「各方當事人間之關係（relationship between the parties）」，檢視該關係是否賦予資料持有者取得附加資訊以識別資料主體的能力[22]。以 *Breyer* 案為例，法院之所以認定 IP 位址對網路經營者而言構成個資，係因存在一法律途徑允許網站經營者向網路服務供應商取得附加資訊；反之，判決看似也在暗示，若缺乏法律關係，對網站經營者而言，縱使客觀上存在一個持有附加資訊之第三方（如網路服務供應商），單純之 IP 位址並不構成個人資料[23]。

---

[17] *Id*. paras. 47-48.
[18] Case C-413/23, para. 82.
[19] *Id*. para. 86.
[20] Michèle Finck & Frank Pallas, *They Who Must not be Identified—Distinguishing Personal From Non-Personal Data Under the GDPR*, 10(1) INT'L DATA PRIV. L. 11, 18 (2020).
[21] Case C-413/23, *supra* note 18.
[22] Miranda Mourby et al., *Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK*, 34 COMPUT. L. & SEC. REV. 222, 225 (2018).
[23] *Id*. at 226.

本文認為，歐洲法院判準似乎較偏向「基於風險」之認定，然而，歐洲法院採取之標準亦可能帶來些許隱患。首先，所謂的「合理可能使用方法」此一標準欠缺特定或可量化的指標，將導致標準之判定高度仰賴個案判斷[24]。例如法院在 *EDPS v. SRB* 案中所指出之標準，即若該方法本身違法或者所需成本過高進而導致其現實上不可能。然而法院並沒有提供一個清楚的標準去衡量何謂成本過高，這可能會導致法律適用上的不確定性。

其次，科技的進步（特別是人工智慧的發展）將導致未來應如何判定何人擁有「合理可能使用方法」以識別資料主體一事變得更為複雜。由於人工智慧的運算及推理能力非常強大，甚至可能透過使用非個人資料、匿名化資料等等傳統上排除於 GDPR 適用外的資料種類，而便能夠生成與個人相關之推論或個人剖析（profile）[25]，進而使原先可能「微不足道」之風險上升至合理可能之風險，使得原先被認定不屬於個人資料的假名化資料成為個人資料。

肆、結論

由分析歐盟「假名化指引」可知，諸如對照表與加密金鑰等「附加資訊」，不僅係還原假名化資料之關鍵，亦為「合理可能使用方法」中的核心。

另一方面，透過歐洲法院實務見解之梳理，在判斷特定主體是否持有「合理可能使用方法」時，要基於資料主體是否有再識別之風險去認定。若再識別風險本身「微不足道」時，即可認定該假名化資料不屬於個人資料。此見解在當今由資料驅動之經濟體系下，有助於調和個資保護與數據流通之衝突。

然而，此一標準在適用上仍然高度仰賴個案判斷，導致一定的法律上不確定性，也因為人工智慧的高速發展與應用導致再識別個人的風險提高，因此，本文認為歐盟未來在個人資料保護及假名化之規範發展，除了可以提供更具體化的標準外，更應該定期依照科技，特別是人工智慧的發展狀況，檢討個人資料的認定標準。

[24] Patrice Navarro, *Pseudonymized Data After EDPS v SRB*, CLIFFORD CHANCE (Sep. 10, 2025), https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/09/pseudonymized-data-after-edps-v-srb.html..

[25] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019(2) COLUMBIA BUS. L. REV. 494, 575 (2019).