

試析歐盟資料保護委員會「匿名化指引」之重點與影響

謝竣博 編譯

指導老師 楊培侃

摘要

歐盟資料保護委員會於今 (2026) 年 7 月 7 日通過「匿名化指引」，回應近年歐盟法院判例及科技發展所帶來的挑戰，並進一步釐清匿名化之認定標準。指引強調，匿名性並非絕對，應依資料所處之具體情境、相關主體所掌握之資訊及其再識別能力進行判斷，並提出兩種匿名化評估方法，以及無法單獨識別、無法連結及無法推論三項判斷標準。此外，考量科技及再識別技術持續發展，匿名化亦非一次性之作業，而有持續評估並再識別風險之必要。

(取材資料：Rachel De Souza, *EU: EDPB Publishes Draft Guidelines on Anonymisation*, DLA PIPER (Aug. 13, 2026), <https://privacymatters.dlapiper.com/2026/08/eu-edpb-publishes-draft-guidelines-on-anonymisation/>.)

在數位經濟與人工智慧高速發展的浪潮下，資料的流通與再利用已成為企業推動創新與決策的核心引擎。然而，資料控制者在追求資料價值的同時，也面臨著歐盟「一般資料保護規則 (General Data Protection Regulation, GDPR)」極其嚴格的法令遵循挑戰¹。長久以來，產業界一直試圖透過技術手段在資料利用與個資保護之間取得平衡。雖然「假名化 (pseudonymisation)」被廣泛視為降低風險的有效工具，但從法條本身來看，假名化資料只要能透過「附加資訊」加以對照，其本質上仍屬於個人資料²，企業依然必須肩負龐大的法令遵循責任。

這進一步引發實務運作上的重大疑慮：一份資料究竟在什麼情況下，才能真正脫離 GDPR 的範疇，進而使資料被更廣泛的運用？根據歐盟法院 (Court of

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), 2016 O.J. (L 119) 1 [hereinafter GDPR].

² *Id.* art. 4(5) (“[P]seudonymisation’ 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;”).

Justice of the European Union, CJEU) 近年在 *Breyer* 案與 *EDPS v. SRB* 案等指標性判例的解釋³，判斷資料是否構成個資，關鍵在於相關主體是否擁有「合理可能使用方法」來重新識別資料主體⁴。然而，這種基於風險的判斷標準在現實中卻帶來了顯著的法律不確定性。法院要求評估再識別風險是否「微不足道 (insignificant)」，卻未能提供具體且可量化的衡量指標，導致企業難以劃定明確的法遵界限⁵。更棘手的是，隨著人工智慧與高階運算技術的突破，AI 強大的推論能力甚至能從看似非個人或去識別化的資料中重新勾勒出個人剖析，使得原先被視為微小的再識別風險動態劇增。再加上資料傳輸給不同第三方時，接收方與控制者之間資訊不對稱所產生的視角差異，讓「可識別性」的判斷變得極度複雜。

因此，歐盟資料保護委員會 (European Data Protection Board, EDPB) 於今 (2026) 年 7 月 7 日通過「匿名化指引 (Guidelines 02/2026 on Anonymisation)」(下稱「指引」)⁶。指引釐清了資料在何種情況下始得真正構成 GDPR 所稱之匿名資料，並更新第 29 條工作小組 (Article 29 Working Party, WP29) 於 2014 年發布之匿名化意見⁷，以回應近年歐盟在法律與科技上之重大發展。本文首先簡要比較 2014 年匿名化意見與 2026 年匿名化指引之異同，其後進一步分析指引之重要內容，最後探討其可能產生之影響與意義，並作成結論。

壹、匿名化指引之背景起源

歐盟層級之資料保護規範可追溯至 1995 年。時年歐盟通過「資料保護指令 (Directive 95/46/EC)」，旨在建立會員國間統一的個人資料保護標準，並確保個人資料得在歐盟單一市場內自由流通⁸。其後，WP29 於 2014 年發布匿名化技術意見⁹，進一步闡明匿名化之概念及相關技術。意見書中指出，匿名化乃「對

³ Case C-582/14, *Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779 (Oct. 19, 2016); Case C-413/23 P, *European Data Protection Supervisor v. Single Resolution Board*, ECLI:EU:C:2025:645 (Sep. 4, 2025).

⁴ 更多關於假名化及「合理可能使用方法 (reasonably likely to be used)」之討論，可參：巫承運，試析歐盟法上假名化資料是否屬個人資料之認定標準，經貿法訊，350 期，頁 1-5，2025 年 11 月 25 日，<https://tradelaw.nccu.edu.tw/uploads/epaper/no350/1.pdf>。

⁵ *EDPS*, ECLI:EU:C:2025:645, para. 82.

⁶ EUROPEAN DATA PROTECTION BOARD, GUIDELINES 02/2026 ON ANONYMISATION (adopted July 7, 2026, for public consultation) [hereinafter GUIDELINES].

⁷ ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 05/2014 ON ANONYMISATION TECHNIQUES, WP216 (adopted Apr. 10, 2014) [hereinafter OPINION 05/2014].

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

⁹ WP29 係依據「資料保護指令」第 29 條所成立，旨在就個人資料處理相關之資料主體保護事項提供專業意見，並獨立行使其職權。Id. art. 29.

於個人資料所為之不可逆 (irreversible) 處理¹⁰」，其結果須如同永久刪除般不可還原¹¹。意見書並就當時常見之匿名化技術及其再識別風險進行分析，提出「單一化 (singling out) ¹²」、「可連結性 (linkability) ¹³」及「推論 (inference) ¹⁴」等判斷面向，作為評估匿名化措施有效性之重要基礎。

隨著數位科技快速發展，跨境資料蒐集、處理與傳輸日益頻繁，原有規範逐漸難以因應新興之資料處理模式。為回應數位環境下日益複雜之個人資料保護問題，並進一步統一歐盟境內之資料保護規範，歐盟遂於 2016 年通過 GDPR，取代原有之「資料保護指令」。

根據 GDPR 前言第 26 段，匿名資料係指「與已識別或可識別之自然人無關之資訊」，或原屬個人資料，但經匿名化處理後，使資料主體「無法或不再能被識別」之資訊¹⁵。由於此類資料已無法連結至特定自然人，故不屬於 GDPR 之適用範圍。由此可知，匿名化之核心問題在於：相關資料是否仍可連結至特定自然人而具「可識別性」，以及應從何一主體之角度判斷其可識別性。

CJEU 於 *EDPS v. SRB* 案中，即釐清可識別性之判斷視角。CJEU 指出，可識別性之判斷應結合具體資料處理活動及所涉及之法律義務，以確定應採取何一主體之視角¹⁶。在此基礎上，指引進一步指出，「採取何種判斷視角，取決於該主體本身是否決定資料處理之方式與目的¹⁷」。因此，若某一主體係代表他人處理資料，不論該資料對其而言是否屬於個人資料，均應以決定該資料處理之主體（即控制者）之視角加以判斷¹⁸。換言之，企業以處理者身分代表控制者處理個人資料時，即使其本身無法識別特定個人，該資料對其而言仍屬個人資料。

¹⁰ OPINION 05/2014, *supra* note 7, at 5.

¹¹ *Id.* at 6.

¹² 其係指能夠從資料集中，單獨辨識出部分或全部可識別特定個人之資料紀錄的可能性。*Id.* at 11.

¹³ 其係指至少能夠將涉及同一資料主體或同一群資料主體的兩筆資料紀錄相互連結的能力。*Id.*

¹⁴ 其係指根據一組其他屬性的數值，以相當高的機率推知某一特定屬性數值的可能性。*Id.* at 12.

¹⁵ GDPR, recital 26 (“[A]nonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.”).

¹⁶ Case C-413/23 P, *European Data Protection Supervisor v. Single Resolution Board*, ECLI:EU:C:2025:645, paras. 98–100 (Sep. 4, 2025).

¹⁷ GUIDELINES, *supra* note 6, at 7.

¹⁸ *Id.*

指引亦指出，匿名化可能基於不同目的而為。在某些情況下，企業可能希望資料對任何第三方而言均屬匿名；但在其他情況下，匿名化則可能僅針對特定接收者，原始控制者仍持有足以識別個人之資訊。因此，判斷資料是否已達匿名化程度，必須與資料實際被使用及分享的具體脈絡緊密結合。

貳、指引之重要內容

為判斷資料是否已達匿名化程度、以及所採匿名化措施是否有效，指引分別提出兩種評估方法及三項判斷標準。前者用以確定應如何評估資料主體遭識別之可能性，後者則用以具體檢驗匿名化措施能否有效防止資料主體遭到識別。以下分別說明。

一、匿名化評估方法

(一) 脈絡性方法 (contextual approach)

此方法反映 GDPR 下之法律判斷標準。依此方法，企業必須考量可能試圖識別個人之第三方實際具備之能力、資訊及資源。此方法承認，不同主體可能取得不同之資料集、技術或法律權限，而此等因素均可能影響個人遭再識別之可能性¹⁹。

例如，假設某控制者欲將一組包含人口統計資料及醫療資訊之資料集進行匿名化。控制者首先發現，單憑資料集內之人口統計資訊尚不足以再識別個人；然而，如將該等資訊與特定之外部醫療資訊相結合，則可能再識別資料主體。若僅考量再識別在理論上是否可能，該資料即可能被認為尚未達匿名化程度；惟依脈絡性方法，控制者尚須進一步確認各相關主體是否實際能夠透過合理可能使用之手段取得該外部醫療資訊²⁰。因此，即使某項再識別方式在理論上可行，若特定主體實際上無法合理取得所需之外部資訊，該資料對該主體而言仍可能被認定為匿名。

(二) 簡化方法 (simplified approach)

此方法不考慮不同主體間之差異，而係假定存在更廣泛的潛在再識別能力。儘管採取此種方法可能導致企業將部分原可被認定為匿名之資料仍視為個

¹⁹ *Id.* at 16.

²⁰ *Id.* at 17.

人資料加以處理，惟 EDPB 指出，此方法提供了一種較為保守、且實務上較容易證明合乎規範之方式²¹。

EDPB 亦指出，將兩種方法結合運用往往有所助益。企業可先以簡化方法對資料進行初步評估，於必要時再進行更細緻之脈絡性分析²²。

二、匿名化有效性之判斷標準

指引的另一個核心內容，係建立一套由三項標準所構成的新判斷架構，供企業評估資料是否已有效匿名化。EDPB 指出，若以下三項標準均獲得滿足，原則上即可將該資料視為匿名資料，進而不再屬於 GDPR 所適用之範圍。

(一) 欠缺可單獨識別之記錄 (No Record Isolation)

第一項標準在於判斷，「是否能夠透過與單一個人相關之屬性值的獨特組合，將特定個人從資料中辨識出來²³。」即使如姓名、身分證字號等直接識別資訊已被移除，若剩餘資料仍足以形成獨特之個人特徵組合，該個人仍可能遭辨識。一筆紀錄所包含之資訊越多、屬性越豐富，其於特定資料中具獨特性之可能就越高。

(二) 無法連結 (No Linkage)

第二項標準則檢視「該資料是否能夠與其他包含同一個人相關資訊的資料集 (dataset) 相互連結²⁴。」EDPB 指出，表面上看似無害、無法識別個人之資訊，在與其他資料來源結合後，仍可能產生識別效果。因此，企業必須考量相關主體可能取得哪些補充資訊，以及各資料集之間相互比對或連結之可能性。

(三) 無法推論 (No Inference)

第三項標準著重於判斷，「是否能夠從資料集中推論出與特定可識別個人有關且具有實質意義之資訊²⁵。」EDPB 說明，推論風險不僅可能來自個別紀錄層級之資料，亦可能存在於彙總資料 (aggregated data) 中，包括統計結果、人工

²¹ *Id.*

²² *Id.*

²³ *Id.*, at 18.

²⁴ *Id.*, at 19.

²⁵ *Id.*, at 21.

智慧模型及合成資料集 (synthetic datasets)。若所作出之推論與特定個人有關，且可能影響其權利或利益，即可能構成匿名化判斷上之問題。

參、結論

相較於 2014 年之匿名化意見，指引為企業評估及記錄匿名化提供了一套更為詳細的架構。然而，企業也因此必須對再識別風險進行更細緻的評估、考量不同利害關係人的視角，並保存足以支持其匿名化判斷的相關證據。

指引亦相當重視再識別技術日益精進所帶來之風險，以及人工智慧可能帶來之影響²⁶。EDPB 並強調，匿名化並非一次性之作業，今日已有效匿名化的資料，未來可能因新資訊得以取得或新分析技術出現，而面臨再識別風險。因此，EDPB 建議企業應定期重新評估已匿名化之資料集，以確保再識別風險隨時間經過仍維持在可忽略之程度。

²⁶ *Id.*, at 26.