試論「一般資料保護規則」與「歐盟資料法」於混合資料之適用

林立

摘要

「一般資料保護規則」針對個人資料規範，以自然人基本權保障為核心，透過廣泛之個人資料定義，對資料蒐集、傳輸與揭露設定嚴格要求。而「歐盟資料法」則針對非個人資料使用設下規則，其以公平取用與使用資料的市場治理為導向，賦予使用者取用資料並得請求提供予第三方之權利。二者看似相互獨立，然在物聯網連網設備所產出之混合資料，則有交錯適用的空間。本文指出，資料法雖建立資料提供機制，但涉及個人資料時仍須先符合「一般資料保護規則」之合法性、目的限制與資料最小化等要求。因此，混合資料持有者履行資料法下義務之重點不是單純的提供資料與否的二元選擇，而在於如何在界線內具體化提供範圍與方式。

在數位技術深度滲透日常生活的背景下，智慧車輛、穿戴式設備與智慧家電等連網設備持續生成大量行為與操作資料，形成反映個人活動模式的資料軌跡[1]。此類資料具高度經濟與社會價值，多由設備製造商或服務提供者掌握，長期導致資料取得不易與再利用受限之問題。資料分享亦受到缺乏誘因、權利義務不明確等障礙，致使資料無法有效流通[2]。為回應此一現象，歐盟逐步建構旨在兼顧資料保護與資料流通的法制架構。

其中，「一般資料保護規則（General Data Protection Regulation, GDPR）」奠定歐盟個人資料保護的制度基礎[3]，其適用客體限縮於「個人資料」，以保障

[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), recital 30, 2016 O.J. (L 119) 1, 6 [hereinafter GDPR] ("[O]nline identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers.").

[2] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), recital 2, 2023 O.J. (L series) 1 [hereinafter Data Act] ("Barriers to data sharing prevent an optimal allocation of data for the benefit of society. These barriers include a lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, the costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, creating bottlenecks for data access, lacking common data sharing practices and the abuse of contractual imbalances with regard to data access and use.").

[3] GDPR, art. 1(1) ("This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.").

「自然人」之基本權利為核心[4]。相對地，「歐盟資料法（EU Data Act）」（以下簡稱資料法）旨在促進資料經濟之流通[5]，其標的涵蓋個人與非個人資料，並賦予使用者（含法人）資料存取與分享之權利[6]。

具體而言，實務上最大的挑戰在於物聯網產生的資料往往屬於混合資料[7]：同一組資料流中，既包含純粹的機器運作參數，亦參雜與使用者行為高度相關之個人資料[8]。在網路傳輸的過程中，資料持有者會透過遠端連線，持續蒐集並控制這些混合資料。這意味著，資料持有者在技術上不可避免地會接觸並處理到資料主體的個人資訊[9]。此種混合資料之難題，不僅限於物聯網裝置，亦普遍存在於數位經濟中的雲端運算與資料處理服務中，成為法規遵循的共通挑戰[10]。

此時，問題隨之產生：當資料法要求這些資料持有者必須將資料開放給第三方使用時，他們將面臨兩難的困境[11]。一方面，其負有促進資料流通的法定義務；另一方面，作為掌控混合資料的實體，其又受限於 GDPR 嚴格的個資保護限制[12]。本文將透過比較兩法之規範架構，分析混合資料所引發之合規難題，並試圖為實務運作提出可行的解釋。

壹、一般資料保護規則與歐盟資料法之規範價值與內容歧異

混合資料之所以引發合規兩難，根源在於 GDPR 與資料法的價值取向與規則結構不同。GDPR 以自然人基本權保障為核心，先規定抽象的基本原則以設定底線[13]，例如目的限制（GDPR 第五條第一項 b 款）與資料最小化（同條第一項 c 款），並以可問責性要求控制者對合規負舉證責任（同條第二項）。此外，

[4] *Id.* art. 4(1) ("'personal data' means any information relating to an identified or identifiable natural person.").
[5] Data Act, recital 6 ("In order to realise the important economic benefits of data, including by way of data sharing on the basis of voluntary agreements and the development of data-driven value creation by Union enterprises.").
[6] *Id.* recital 5 ("This Regulation ensures that users of a connected product or related service can access.").
[7] Dionysia Kontotasiou, *Non-Personal Data: How to Handle It & the Opportunities for Businesses*, CONVERT (Jan. 10, 2022), https://www.convert.com/blog/privacy/non-personal-data-how-to-handle-it-the-opportunities-for-businesses.
[8] Data Act, recital 6. ("The data generated by the use of a product or related service can be personal data or non-personal data, or a combination of both.").
[9] EUROPEAN DATA PROTECTION BOARD (EDPB), GUIDELINES 1/2020 ON PROCESSING PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY APPLICATIONS 6-7 (2020).
[10] *Response to Draft EDPB Recommendations on Supplementary Measures for Personal Data Transfers*, DIGITALEUROPE (Dec. 21, 2020), https://www.digitaleurope.org/resources/response-to-draft-edpb-recommendations-on-supplementary-measures-for-personal-data-transfers/.
[11] Data Act, art. 5(1) ("The data holder shall make data available to a third party of the user's choice;").
[12] Data Act, art. 1(5).
[13] GDPR, art. 5(1) ("collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.").

個人資料之處理必須具備合法性基礎，包含資料主體已就特定目的同意、履行契約或締約前措施所必要、遵守控制者法定義務所必要；保護資料主體或他人之重大利益所必要；履行公共任務與正當利益所必要（GDPR 第六條第一項第 a 款至第 f 款）[14]，而個人資料主體得透過 GDPR 所定之資料主體權利，對資料控制者之處理活動施加限制，例如其存取權以及要求提供副本之權利[15]。

相對地，資料法以資料可取得性與市場治理為導向，主要處理的是「資料集中」所造成的競爭與創新障礙，因而採取以資料持有者之提供義務搭配使用者之存取權的規制設計[16]。具體而言，資料法要求連網產品與相關服務提供者，在產品與服務設計上即確保使用者得以取得其使用所產生之資料（資料法第三條第一項）[17]，並賦予使用者向資料持有者請求取得資料及提供之權利（資料法第四條），藉此打破製造商或服務提供者對資料主體的單方控制[18]。然而資料法明定其不影響 GDPR 之適用，因此其所創設之存取或提供義務，並不當然構成個人資料處理的合法性基礎；凡取得內容涉及可識別自然人的資訊，仍須回到 GDPR 第六條第一項先行確認是否具備合法性基礎及相應保護措施[19]。由此可見，在混合資料情境下，資料法主要規範「請求與提供」資料之權利義務配置，而 GDPR 則界定「涉及個資時能否提供以及如何合法提供」，兩法因而在同一資料流中併行適用[20]。

貳、混合資料適用一般資料保護規則與歐盟資料法之情形

混合資料含有個資以及非個資，然而不必然在同一處理行為上同時適用 GDPR 與資料法。宜先依資料性質區分，凡得以直接或間接識別自然人之部分，

[14] GDPR, art. 6(1).
[15] GDPR, art. 15(1).
[16] Data Act, recital 1 (“High-quality and interoperable data from different domains increase competitiveness and innovation and ensure sustainable economic growth.”).
[17] Data Act, art. 3(1). (“Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user.”).
[18] Data Act, art. 4(1). (“Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.).
[19] GDPR, art. 6(1).
[20] Elisabeth Dehareng & Helena Engfeldt, *EU Data Act: All Your Threshold Questions Answered*, INT’L ASS’N OF PRIVACY PRO. (Aug. 22, 2024), https://iapp.org/news/a/eu-data-act-all-your-threshold-questions-answered.

屬 GDPR 所稱之個人資料[21]，其蒐集、儲存、傳輸與提供均屬資料處理，須先符合 GDPR 之合法性基礎、目的限制與資料最小化等要求。至於同一資料流中不屬於個人資料部分，仍應依資料法所設之使用者資料取得機制，由資料持有者使該可得資料及其必要中介資料得以供使用者取得並用於解讀與使用[22]。亦即，區分資料的性質分別適用二者，分別適用較為簡單，也不太會產生規範衝突的情況。

然若實務上個人資料與非個人資料在技術上難以有效切割，或即使去除識別欄位後仍存在再識別風險[23]，仍須依資料法第一條第五項，優先適用 GDPR[24]。以車隊管理為例：一家物流公司（法人使用者）為優化運輸效率，依據資料法向車廠請求其租賃車隊的行駛資料[25]。這些資料雖包含車輛油耗與維修參數（非個資），卻同時記錄了卡車司機，亦即資料主體之煞車頻率、行使路徑與修時間（個資）。在此情境下，只要資料內容涉及資料主體（司機），無論請求人具備何種身份，資料持有者皆需要依 GDPR 第六條尋找合法性基礎（例如確認是否取得司機同意或具備正當利益）[26]。即便具備處理個資之合法性基礎，資料持有者仍須在技術層面落實 GDPR 第五條之處理原則。具體操作上，應優先採行「資料最小化」措施，僅釋出達成物流優化目的所嚴格必要之欄位（如油耗數值），而剔除與目的無關之細節（如司機休息時的精確位置）[27]。此外，針對可識別身份之資訊，資料持有者先應採行 GDPR 之「假名化」，以代碼取代司機姓名等直接識別資訊，並將代碼對照等「額外資訊」分離保存且以技術與組織措施嚴格保護；同時，在交付前亦應完成必要性與比例性之權衡，確認

[21] GDPR, art. 4(1) (“‘[P]ersonal data’ means any information relating to an identified or identifiable natural person”).
[22] Data Act, 4(1) (“Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.”).
[23] Helena Wootton et al., *EU Data Act: Interplay with the GDPR*, ADDLESHAW GODDARD (Nov. 12, 2025), https://www.addleshawgoddard.com/en/insights/insights-briefings/2025/data-protection/eu-data-act-interplay-gdpr/.
[24] Data Act, art. 1(5) (“This Regulation is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein.”).
[25] *The Scope of the EU Data Act: What’s In, What’s Out?*, EVERSHEDS SUTHERLAND (Sep. 18, 2025), https://www.eversheds-sutherland.com/en/belgium/insights/the-scope-of-the-eu-data-act-whats-in-whats-out.
[26] GDPR, art. 6.
[27] GDPR, art. 5(1)(c) (“adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization”).

物流效率等商業利益未凌駕司機作為資料主體之利益或基本權利或自由，方能在履行資料法義務的同時，同時維護資料主體之權利保障[28]。

參、實務運用之潛在難題

前述判斷架構固可作為混合資料的操作原則，惟在進入資料提供與第三方使用的實作階段時，仍會遭遇技術與商業利益上的不確定性，構成法規遵循之實質挑戰。特別是當個資保護等限制之因素，與資料流通之要求發生衝突時，資料持有者極易採取過度保守的法遵策略（如拒絕提供），此舉除引發法律爭議外，更讓資料法欲促進資料經濟的目的被削弱[29]。

實際上要將混合資料之切割與去識別化並不容易，資料持有者為履行資料法之提供義務並降低個資風險，往往嘗試將資料去識別化或匿名化，以便以「非個人資料」之形式進行資料處理提供[30]。然而，物聯網資料的分析價值常常仰賴時間戳記、裝置標記或使用者情境等資訊，但此類欄位亦可能成為再識別線索，使得去識別化難以達到可確信排除識別風險的程度。若處理不夠徹底，第三方可能在自認取得非個資的情況下實際取得個資，從而無意間成為 GDPR 下的資料控制者，卻缺乏足以支撐該處理行為的合法性基礎，導致合規責任轉移與侵權風險。此一不確定性將抬高資料分享成本，降低第三方請求意願，並可能反向削弱資料法欲促進資料流通與創新目標[31]。

結論

綜上所述，資料法與 GDPR 之規範目的雖有歧異，前者著重於資料流通與市場治理，後者重在自然人基本權利之保障，但在混合資料情境下須交錯適用。資料法固創設資料取用與提供之制度工具，惟涉及個人資料時仍需先符合 GDPR 之合法性與資料最小化等要求；故「先確認個資處理適法、再履行資料提供」可作為較穩健之處理順序。然而，去識別化門檻、再識別風險，仍是資料共享實作中最易引發爭議之處，後續仍待主管機關與實務判準進一步具體化。

---

[28] Data Act, art. 4(5).
[29] GDPR, recital 26 (“To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out.”).
[30] *See Interaction of the GDPR and the EU Data Act*, TAYLOR WESSING (Oct. 13, 2023), https://www.taylorwessing.com/en/global-data-hub/2025/eu-digital-laws-and-gdpr/gdh---interaction-of-the-gdpr-and-the-eu-data-act.
[31] Data Act, retcital 2 ("Barriers to data sharing prevent an optimal allocation of data for the benefit of society. Those barriers include a lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, the costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and the abuse of contractual imbalances with regard to data access and use.”).