第 1 章

「誰」的「何種行為」將受規範

——立法管轄權範圍之界定

目 次

關鍵概念：

- GDPR 的立法管轄權範圍擴及適用於設立於歐盟境外的資料管控者之 1. 基於提供商品或服務所需，或 2. 基於監控所需，針對歐盟境內人民所為之個資蒐用行為。
- GDPR 不規範蒐用目的非為建立個人資料檔案系統之非自動化個資蒐用行為。
- GDPR 不規範自然人純粹的個人或家庭活動所為與職業或商業活動無關的個資蒐用行為。

壹、歐盟 GDPR 的立法管轄權界定

一、GDPR 規範「誰」的行為

過往的個資保護規範方式，不夠契合數位網路時代下跨國境個資流通的保護需求，例如 Google 和 Facebook 等網路科技巨擘即曾不斷地爭執他們不受歐盟各國的個資保護法律規範，理由是他們並未在當地設立公司，儘管他們的確在當地蒐用其產品或服務使用者之個資。[1]此次 GDPR 擴張適用範圍的變革，反映了解決此類歐盟立法管轄權爭議的想法。GDPR 的規範對象除了考量資料管控者的「設立地域」觀點外，亦合併考量個資被蒐用者（或網路使用者）之「使用

1 Court of Justice of the European Union, Judgement in Case C-131/12, Google Spain SL vs Mario Costeja González, 13 May 2014, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065; Reuters, Facebook wins privacy case against Belgian data protection authority, June 2016, https://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV.

者」的觀點。由保護歐盟境內人民的個資觀點來看，縱使蒐用歐盟境內人民個資的公司係設立在歐盟境外，該個資蒐用行為仍應有受規範之需求。

承上思考，GDPR 第 3 條乃根據第 1 項之「據點」標準(“establishment” criterion)及第 2 項之「目標」標準(“targeting” criterion)以決定 GDPR 所適用之個資蒐用活動地域範圍。[2]

（一）規範「設立在歐盟境內」的資料管控者──「據點」標準(“establishment” criterion)

GDPR 規範設立在歐盟境內進行個資蒐用活動的資料管控者，不論該個資蒐用活動是否發生於歐盟境內。[3]按照 GDPR 前言第 22 點說明：所謂「設立於歐盟境內」的要求，乃以資料管控者是否透過穩定的安排，有效且確實地開展活動；至於「安排」的法律形式，無論是通過分支機構（分公司）或是具有法人資格的子公司，都不是判斷此點的決定性因素。[4]

（二）規範「設立於歐盟境外」的資料管控者之可能──「目標」標準(“targeting” criterion)（GDPR 的域外效力）

依 GDPR 第 3 條第 2 項規定，GDPR 除了規範設立在歐盟境內進行個資蒐用活動的資料管控者外，亦可能在下列兩種情形下，擴及規範設立於歐盟境外的資料管控者：

---

2 EDPB, Guidelines on the territorial scope of the GDPR (2019), at 4.

3 GDPR, Art. 3(1).

4 GDPR, Recital 22. EDPB 嘗建議一種「三重方法(a threefold approach)」來決定個資之蒐用行為是否屬於 GDPR 第 3 條第 1 項之適用範圍，請參閱 EDPB, Guidelines on the territorial scope of the GDPR (2019), at 5-13.

1. 基於提供商品或服務所需，針對歐盟境內之資料主體進行個資蒐用行為

設立於歐盟境外的資料管控者，基於提供商品或服務所需（無論資料主體是否需要付款購買此商品或服務[5]），針對資料主體進行個資蒐用行為，仍須受到 GDPR 規範。[6]至於應如何判斷資料管控者的個資蒐用行為係為提供歐盟境內的該資料主體商品或服務所需，按 GDPR 前言第 23 點所述，應該要確認是否可以「明顯」看到資料管控者欲向一個或多個歐盟會員國內之資料主體提供服務；而得賴以判斷的因素，例如資料管控者是否提供一種或多種歐盟會員國通常使用的語言或貨幣之使用以訂購商品和服務的可能性，或提供之內容提及居住於歐盟境內的客戶或用戶之情形，皆可能構成該「明顯性」之判斷。[7]

2. 基於「監控 (monitoring)」歐盟境內自然人行為所需，對資料主體進行個資蒐用行為

設立於歐盟境外的資料管控者，基於監控發生在歐盟境內之自然人行為所需，而針對資料主體進行個資蒐用之行為，仍須受到 GDPR 規範。[8]在判斷該個資蒐用活動是否構成「監控」資料主體之行為時，應確認：該自然人是否在網路上被追蹤，包括利用資料處理技術對於個資的潛在後續使用，例如包括「描繪（建檔）(profiling)」自然人特徵。[9]依 GDPR 第 4 條 (4) 之定義說明，所謂「描繪」行為，乃指對個資所為任何形式之自動化處理，包括使用個資來評估與該資料主體有關之個人特徵，特別是用來分析或預測有關資料主體之工作表

5 無須對價要求的設計，乃規範假設居住於歐盟境內人民甲使用設立於美國境內之 Google 公司所提供的免費 Gmail 服務，Google 藉此蒐用甲之個資的行為。

6 GDPR, Art. 3(2)(a).

7 GDPR, Recital 23.

8 GDPR, Art. 3(2)(b).

9 GDPR, Recital 24.

現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵。[10]

3. 進行個資蒐用行為的資料管控者雖非設立於歐盟境內，但所設立之處依據國際公法適用歐盟會員國法律，亦適用 GDPR。[11]

（三）中小型企業仍須適用 GDPR

適用 GDPR 規範之企業並不區分規模大小。亦即，GDPR 並未排除中小型企業(a small and medium-sized enterprise, "SME")的適用。不過，SME 在符合兩項要件——1. 個資蒐用行為並非企業營運之核心部分；2. 企業活動並未對個人的自由權利形成具體威脅（例如監控個人或蒐用敏感個資）——下，得減輕其所負擔之 GDPR 規範義務。例如，公司可以不用設置「資料保護長(Data Protection Officer, "DPO")，或有譯為『資料保護專員』」；[12]員工人數少於 250 人的公司不需要保存其個資蒐用活動的紀錄，除非蒐用個資乃公司的日常運作、對個人的自由權利構成威脅，或者涉及敏感個資或犯罪紀錄。[13]

10 GDPR, Art. 4(4).

11 GDPR, Art. 3(3).

12 European Commission, *Does my company/organisation need to have a Data Protection Officer (DPO)?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_en.

13 European Commission, *Who does the data protection law apply to?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.

二、GDPR 規範「何種」行為

（一）原則性規定

GDPR 所規範的個資蒐用行為，乃指：

1. 全部或部分以「自動化方式(automated means)」所為的個資蒐用行為；
2. 雖「非以自動化方式」所為的個資蒐用行為，但蒐用之目的乃為形成或意圖形成資料「檔案系統(a filing system)」的一部分。[14]

依據 GDPR 第 4 條定義性規定之第 6 款，所謂「檔案系統」乃指：可以使用「特定條件」存取的「結構化之個資集合（資料庫）」，無論是集中式、非集中式，或以功能或地域為由的分散式資料庫。[15] 此檔案系統定義的規範重點乃「得以一定方式檢索使用的個資集合」。故倘若以非自動化方式蒐集了一堆個資，但未經系統化處理，係雜亂無章而無從依循特定條件檢索使用者，縱使是大量的個資集合，亦不構成 GDPR 所稱之資料檔案系統。

（二）除外適用規定

依據 GDPR 第 2 條第 2 項規定，下列個資蒐用行為不適用 GDPR 規範：

- 非屬歐盟法規範範圍內之個資蒐用活動(a)；
- 歐盟會員國在開展屬於歐洲聯盟條約(Treaty on European Union, TEU)第 5 篇第 2 章範圍的活動時(b)；
- 自然人因純粹的個人或家庭活動所為與職業或商業活動無關的

14 GDPR, Art. 2(1).
15 GDPR, Art. 4(6).

個資蒐用行為(c)；[16]

- 主管機關基於預防、調查、偵查或起訴刑事犯罪或執行刑事處罰（包括保護和防止對公共安全的威脅）之目的所為的個資蒐用行為(d)：

  由於此類型的個資蒐用行為通常會對當事人自由與權利造成較大威脅，故此款排除 GDPR 適用規定，當然並非意指此類個資不應受保護，而只是因為此類個資蒐用行為之目的係為了保護特定的重大公益，因此對於蒐用行為的規範應另外量身訂作更符合規範需求的特別法。[17]

16 依據 GDPR 前言第 18 點說明，此款規定的解釋適用須加上「不得與職業或商業活動有關」的要件限制。*See* GDPR, Recital 18. 此外，就與 GDPR 第 2 條第 2 項第 c 款相似規定之 95 指令第 3 條第 2 項規定之解釋適用，歐盟法院曾於 *Ryneš* Case 主張：既然對 95 指令規定的解釋，必須符合歐盟基本權利憲章所保障之基本權利，那麼 95 指令第 3 條第 2 項規定所指出的例外不適用 95 指令之情形，也必須從嚴解釋為：僅限於個人資料運用發生於「純粹(purely)」的個人或家庭活動，而非「只是(simply)」個人或家庭行動。 *See* Case C-212/13, Frantisek Ryneš v. Urad pro ochranu osobnich udaju, paras. 29-31, Dec. 11, 2014, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62013CJ0212&from=EN. 關於此判決之進一步說明，參閱張陳弘，《「GDPR 施行兩周年評估報告之分析及相關議題研析」委託研究計畫結案報告》，委託單位：國家發展委員會，2021 年 1 月，89-91 頁，資料下載點：https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvNTc0NC8zNDkxOS9hZjQyZGE1MC1kZWYxLTRmODQtYWM0MC1mZGM3NTc3MWY4MTcucGRm&n=57WQ5qGI5aCx5ZGKLnBkZg%3D%3D&icon=..pdf.

17 *See* GDPR, Recital 19.

貳、臺灣個資法之比較說明

一、資料管控者於臺灣「境外」蒐用臺灣境內人民個資之規範──個資法第 51 條第 2 項

按個資法第 51 條第 2 項規定：「公務機關及非公務機關[18]在臺灣領域外對臺灣人民個人資料蒐集、處理或利用者，亦適用本法。」公務機關理當指「臺灣」之公務機關。若此，則依論理解釋，非公務機關亦應指設立於臺灣之非公務機關或臺灣國民。循此，則個資法得發生境外效力之情形乃指：規範設立於我國或具備我國籍之資料管控者，於臺灣境外蒐用臺灣國民個資之行為。此項規定乃延續傳統立法常見就「境外效力」的規範思維──以「國籍」作為臺灣法發生境外效力的聯繫因素。

相較而言，GDPR 為因應網路科技無國界的規範需求，以及資料蒐用科技的無國籍差別運用特性，在「域外效力」發生的聯繫因素設計上，不使用「國籍」標準：即在境外為蒐用行為之資料管控者不需具備歐盟會員國國籍，在歐盟境內被蒐用個資之資料主體也無須具備會員國國籍；而改以個資蒐用行為是否為提供歐盟境內人民商品或服務所需，或基於監控歐盟境內人民之目的所為，來決定 GDPR 是否適用於在境外進行蒐用行為的資料管控者。亦即，資料管控者或資料主體各自是否具備歐盟公民身分，並非 GDPR 域外效力發生與否的決定因素。[19]

---

18 按個資法第 2 條第 7 款與第 8 款規定，公務機關乃指依法行使公權力之中央或地方機關或行政法人；非公務機關乃指公務機關以外之自然人、法人或其他團體。

19 按 GDPR 前言第 2 點說明，個資蒐用的保護原則或規範，乃基於基本權利和自由之保護，尤其是個資保護的權利，並不問被保護人的國籍或住居所。*See* GDPR, Recital 2.