簡介歐盟一般資料保護規則之地域範圍指引草案

張安潔 編譯

摘要

歐盟資料保護委員會於去（2018）年 11 月 23 日公布一般資料保護規則之地域範圍指引草案，並已於今（2019）年 1 月 18 日前開放公開徵詢意見。本指引草案針對一般資料保護規則中，最重要的地域範圍進行解釋，其中包含三大重點：第一，如何認定機構在歐盟境內設有所謂之「據點」，以及可能落入適用範圍之業務行為；第二，機構若未在歐盟境內設有據點，但資料處理行為落入「針對性」要件之情況；以及第三，一般資料保護規則中要求機構需指定「代表人」的相關規範。

（取材自：Gernot Fritz, Digital: *EDPB Publishes Draft Guidelines on Territorial Scope of the GDPR*, FRESHFIELDS BRUCKHAUS DERINGER (Nov. 26, 2018), https://digital.freshfields.com/post/102f6aq/edpb-publishes-draft-guidelines-on-territorial-scope-of-the-gdpr.）

歐盟「一般資料保護規則（General Data Protection Regulation, GDPR）」第 3 條規範：即使是位於歐盟境外的機構，在一定條件下處理歐盟境內當事人個資，也會落入 GDPR 的適用範圍[1]。此舉擴大歐盟資料保護法體系的適用範圍，是 GDPR 帶來的主要改變之一。根據 GDPR 規範內容，若滿足特定條件，非歐盟事業機構也需要肩負 GDPR 的義務，惟相關的條件卻規定得相當模糊，以致於有解釋的必要[2]。歐盟資料保護委員會（European Data Protection Board，以下簡稱委員會）於去（2018）年 11 月 23 日針對這些模糊的條文用語應如何被理解，發布一份指引草案，並已於今（2019）年 1 月 18 日前公開徵詢意見[3]。以下為 Freshfields Bruckhaus Deringer 律師事務所對此指引草案之相關分析，指出該草案雖釐清了不少適用上的問題，但仍存有部分疑義、甚至有些部分可能違反母法規定。該分析見解值得參考，故本文介紹之。

---

[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, art. 3, 2016 O.J. (L 119) 1, 32, 33 [hereinafter GDPR].

[2] *Id.*

[3] European Data Protection Board, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version for Public Consultation, Adopted on16 November 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf [hereinafter Draft Guidelines].

壹、「據點」之認定標準

根據 GDPR 第 3 條第 1 項的規定，不論該資料處理地是否位於歐盟境內，資料控管者（controller）或處理者（processor）在歐盟境內據點（establishment）之業務活動中所進行之個人資料處理，皆落入 GDPR 的適用範圍[4]。委員會針對此項規定，建議一種「三重法（threefold approach）」的步驟，逐案認定各相關資料處理活動是否落入 GDPR 第 3 條的範圍內[5]。

一、歐盟境內必須有據點

所謂據點指透過穩定安排（stable arrangements）有效且實際地執行業務，無關乎其法律型態為何，例如子公司、分公司或辦事處[6]。根據指引草案，在某些情況下，即使在境內的是非歐盟機構的單一員工或代理人，只要其行為具有一定程度的穩定性，即足以建立所謂的穩定安排[7]。故即便負責處理特定資料的非歐盟機構在歐盟沒有分公司或子公司，亦不妨礙其構成 GDPR 定義下的據點[8]。

二、在據點的業務活動中所為之資料處理

即使非歐盟機構於歐盟境內的據點在資料處理中，未實際擔任任何角色，其行為也可能與此等資料處理行為密不可分[9]。根據指引草案，假如是為了使非歐盟機構提供的服務更有利可圖，其歐盟境內據點對歐盟市場執行潛在客戶之開發與行銷活動，就可能屬於此情形[10]。

三、資料處理地並不重要、資料控管者或處理者之據點位置方為關鍵

判定 GDPR 適用的地域範圍時，對於資料控管者或處理者設立的據點本身，或非歐盟的資料控管者或處理者在歐盟境內之商業據點而言，地理所在位置是重要的，但資料處理地卻不然[11]。非歐盟機構對歐盟境內資料處理者之指示，並不會因此使其自動受 GDPR 管制，但歐盟的資料處理者和非歐盟的資料控管者間需簽訂資料處理協議[12]。儘管 GDPR 不及於該非歐盟機構，歐盟的資料處理者仍有義務簽訂此類協議，即使是與歐盟境外的資料控管者[13]。

---

[4] GDPR, art. 3.1.
[5] Draft Guidelines, at 4.
[6] GDPR, recital 22.
[7] Draft Guidelines, at 5.
[8] *Id.*
[9] *Id*. at 6.
[10] *Id.* at 7.
[11] *Id*. at 8, 9.
[12] *Id*. at 10.
[13] *Id*. at 11.

貳、「針對性」之認定標準

未在歐盟境內設有據點的資料控管者或處理者，不必然意謂其得被排除於 GDPR 的地域適用範圍外[14]。GDPR 更進一步規定，非歐盟境內的資料控管者或資料處理者在處理歐盟境內當事人的個資時，只要與下列兩類行為相關，仍適用 GDPR[15]：（1）向當事人提供貨品或服務，無論是否要求當事人支付費用；或者（2）監測當事人在歐盟境內的行為。

一、歐盟境內的當事人

評估當事人是否位於歐盟境內的標準，為相關行為發生的時點，如提供貨品或服務，或其行為被監測的時候，至於提供或監測的時間長短在所不問[16]。此外，無論是提供貨品或服務或監測個人的行為，對歐盟境內的個人一定要具有針對性（targeting）的要素[17]。只要資料處理並非針對歐盟境內特定個人，也非監測其在歐盟境內之行為，則在歐盟外之第三國處理歐盟公民或居民之個資並不適用 GDPR[18]。

二、提供貨品或服務

首先，委員會認為資料處理行為與貨品或服務的提供之間，需要有直接或間接的關聯[19]。其次，委員會也確認僅是其網站得自歐盟進入之事實，本身並未提供充份的證據足以顯示資料控管者或處理者有意對歐盟境內當事人提供貨品或服務[20]。

在判斷上是否對歐盟境內當事人提供貨品或服務，判斷時可考慮以下因素[21]：（一）歐盟或至少一個成員國被指名是貨品或服務可能提供的對象；（二）資料控管者或處理者向搜索引擎營運者支付網路參考服務費用，以便有助於歐盟的消費者訪問其網站；（三）資料控管者或處理者已針對歐盟會員國目標客群發起行銷和廣告活動；（四）業務具有國際性質，例如特定旅遊活動；（五）提及得自歐盟地區聯繫的專用地址或電話號碼；（六）使用不同於資料控管者或處理者所在之第三國的頂級網域名稱，例如「.at」（奧地利的頂級網域名稱）或使用中性頂級網域名稱，例如「.eu」（歐盟的頂級網域名稱）；（七）從一個或多個歐盟成員國到服務提供地之路線指示；（八）提及包含定居於歐盟成員國內的國際客戶，特別是有這些客戶的經驗分享及意見回饋；（九）使用非貿易商所屬國家通常使

[14] *Id*. at 12.
[15] GDPR, art. 3.2.
[16] Draft Guidelines, at 13.
[17] *Id*. at 14.
[18] *Id*.
[19] *Id*. at 15.
[20] *Id*.
[21] *Id*. at 15, 16.

用的語言或貨幣，尤其是使用一個或多個歐盟成員國的語言或貨幣；或（十）提供在歐盟成員國內交付貨物的服務。

三、監測當事人之行為

根據指引草案，使用「監測」一詞意謂資料控管者在蒐集歐盟境內個人行為的相關資料和後續再使用上是有特定目的，因此委員會並不認為任何在網路上蒐集或分析歐盟境內個資之行為都會自動落入「監測」的定義中[22]。根據指引草案，有必要考慮資料控管者處理資料的目的，特別是後續任何涉及該資料的行為分析或特徵側寫技術；不過委員會認為透過使用 cookie 或其他追蹤技術如指紋識別，以及地理定位行為（特別是為了行銷目的），正是屬於這種監測行為[23]。綜上所述，如果網站是歐盟居民可及者，則僅是在網站上使用 cookie 是否一定會落入 GDPR 適用範圍，似乎並不清楚。

參、指定代表人

設在歐盟境外的資料控管者及處理者，只有該當上述「針對性」要件時，才有義務指定其在歐盟境內的代表人（representative）[24]。此代表人可以是自然人、商業機構或非商業機構，且必須設立在其提供服務或貨品，或進行監測行為的歐盟成員國境內[25]。固然非歐盟機構有一定程度的自由得選擇於何歐盟成員國境內設置代表人，但不可或忘的是該代表人必須讓當事人及其他成員國（即非代表人設置地）的監管機關容易聯絡，尤其在聯繫上必須以監管機關和相關當事人使用的一種或多種語言進行[26]。此外，指引草案認為該代表的職能與對外資料保護長（Data Protection Officer）的角色並不相容，因此被指定之代表人不能同時被同一機構指派為資料保護長[27]。

委員會更進一步指出，之所以導入代表人之概念，係意圖使執法者能夠對代表人採取與對資料控管者或處理者相同的執行處分[28]。委員會的看法亦表示這將包括可能對代表施以罰鍰或其他行政罰，並使代表人承擔直接責任[29]。然而這樣的見解無法自 GDPR 的規範推導而得；相反地，GDPR 第 58 條明確規定監督機關可以直接對代表人採取的唯一處分，就是命令該代表人提供機關監督所需的資訊[30]。所有其他相關的執法權力（包括加諸行政罰）及 GDPR 的責任制度皆僅針

[22] *Id*. at 18.
[23] *Id*.
[24] *Id*. at 19.
[25] *Id*. at 20.
[26] *Id*. at 20, 21, 23.
[27] *Id*. at 20, 21.
[28] *Id*. at 23.
[29] *Id*.
[30] GDPR, art. 58.

對資料控管者和（或）處理者[31]。因此，委員會認為能對代表施以罰鍰的可能性和承擔責任的看法在 GDPR 中是沒有依據的。

[31] Draft Guidelines, at 23; GDPR, arts. 83, 84.