

歐盟針對美歐資料隱私架構提出適足性認定草案

戴維萱 編譯

摘要

去(2022)年12月13日,歐盟執委會對美國提出「適足性認定草案」,此舉將促進更為安全的跨大西洋資料流動,並肯認其為自歐洲法院於2020年7月的Schrems II案之裁決中認定「隱私盾協定」無效後,美歐雙方在資料傳輸議題上之一大進展。執委會於「適足性認定草案」中評估美國現行法律架構,其中包括「加強規範美國訊號情報活動之第14086號行政命令」及關於建立資料保護審查法院的新規則,並認為美國提供與歐盟內部法律之保護水準相當的保護措施。然而,仍有論者質疑執委會根據第14086號行政命令作成之適足性認定,恐在日後面臨歐洲法院之挑戰,而目前該草案已交至歐洲資料保護委員會徵求其意見。有鑒於美歐資料傳輸議題之重要性,其後續動向值得我們持續追蹤。

(取材資料: Joseph Duball, *EU-US Draft Adequacy Decision Arrives, EU Process Begins in Earnest*, INT'L ASS'N OF PRIVACY PROF'LS (Dec. 13, 2022), <https://iapp.org/news/a/eu-us-draft-adequacy-decision-arrives-eu-process-begins-in-earnest/>; *Statement on EU Commission Adequacy Decision on US*, NOYB (Dec. 13, 2022), <https://noyb.eu/en/statement-eu-commission-adequacy-decision-us>.)

2020年7月歐洲法院(Court of Justice for European Union, CJEU)在Schrems II案中宣告「隱私盾協定(Privacy Shield)」無效後¹,歐盟執委會與美國進行多次協商,以尋求該協定之替代方案²。

美歐雙方於去(2022)年3月達成一原則性協議,同意以新「美歐資料隱私架構(US-EU Data Privacy Framework, DPF)」取代「隱私盾協定」³。接著,美國總統拜登(Joe Biden)於去年10月7日頒布「加強規範美國訊號情報活動之

¹ Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems*, ECLI:EU:C:2020:559, § 203 (July 16, 2020).

² European Commission, *Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo* (Mar. 25, 2021).

³ European Commission Press Release IP/22/2087, *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework* (Mar. 25, 2022).

第 14086 號行政命令 (Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities)」（以下簡稱第 14086 號行政命令）⁴。美國司法部長梅里克·加蘭 (Merrick Garland) 亦於同日發布關於建立資料保護審查法院 (Data Protection Review Court, DPRC) 的新規則，將美歐雙方所達成之原則性協議的承諾內容落實於美國法律中⁵。

上述兩項文件更加完善了 DPF，故執委會於去年 12 月 13 日發布適足性認定 (adequacy decision) 草案，肯認美國於該些規範中，對符合 DPF 規定傳輸的個人資料之保護水準，實質等同 (essential equivalence) 於歐盟內部法律⁶。執委會此舉有助於完成 DPF 之最終版本及達成美歐間暢行無阻的資料傳輸目標。

本文先簡述歐盟對於第三國資料保護適足性之認定標準與要件，並以此為基礎，分析執委會於本次適足性認定草案中，如何評估 DPF 下美國情報機關對傳輸自歐盟的個人資料之相關規範，進而認定其已達與歐盟內部法律實質等同之保護水準。最後說明外界對該草案之評論與未來發展，作一結論。

壹、資料保護適足性之認定標準與要件

針對資料保護適足性之判斷標準，執委會引述過去歐洲法院於 Schrems 案中之見解，亦即：第三國採取的作法得與歐盟內部採用的作法不同，惟其須在實踐中證明其有效並實質等同於歐盟內部法律的保護水準⁷。

執委會亦指出歐盟資料保護委員會 (European Data Protection Board, EDPB) 之 WP/254 號文件為適足性認定之參考指引⁸。據此，基於國家安全或執法目的

⁴ Exec. Order No. 14,086, 87 Fed. Reg. 62,283 [hereinafter EO 14086]. 訊號情報 (Signal Intelligence) 係指自外國標的使用之電子信號及系統中獲取之情報，例如通訊系統、雷達與武器系統，並將其提供給本國政府之資深文職官員及軍職官員。訊號情報活動可供本國了解外國對手的能力、行動與意圖且有助達成重要國家目標。Signal Intelligence (SIGINT) Overview, NATIONAL SECURITY AGENCY, <https://www.nsa.gov/Signals-Intelligence/Overview/> (last visited Dec. 5, 2022).

⁵ Redress in the Data Protection Review Court, U.S. DEP'T OF JUST., <https://www.justice.gov/opcl/redress-data-protection-review-court> (last updated Dec. 28, 2022); 28 C.F.R. § 201.1 (2022).

⁶ European Commission, Commission Implementing Decision of XXX Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework, recital 7, https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf [hereinafter Draft Decision].

⁷ Id. recital 4; see also Case C-362-14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, §§ 73, 74 (Oct. 6, 2015).

⁸ Article 29 Data Protection Working Party, Adequacy Referential, WP254 rev.01 (Feb. 6, 2018), <https://ec.europa.eu/newsroom/article29/items/614108/en> [hereinafter WP/254]; see also Article 29 Data Protection Working Party, Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection Through Surveillance Measures when Transferring Personal Data (European Essential Guarantees), WP237 (Apr. 13, 2016),

取得個人資料之第三國，若欲取得適足性認定資格，應遵循下列四項實質保障要件：第一，是否存在處理個人資料之法律依據；第二，資料之取得是否具達成正當目的之必要性（necessity）與相稱性（proportionality）；第三，個人資料之處理應受獨立監督；最後，應提供當事人有效救濟手段⁹。

執委會認定美國對從歐盟傳輸至 DFP 認證的公司之個人資料所採的措施，符合「一般資料保護規則（General Data Protection Regulations, GDPR）」第 45 條規範之適當保護水準，以下分析美國所採前開命令規定是否滿足歐盟所訂適足性各項實質保護要件¹⁰。

貳、歐盟對美國第 14086 號行政命令之適足性認定

一、法律依據

執委會於草案中首先檢視美國現行情報機關蒐集個人資料之法律架構。如以國家安全為目的者，美國情報機關經合法授權即可根據「外國情報監控法（Foreign Intelligence Surveillance Act）」蒐集傳輸至美國當地公司之個人資料。而對於境外的個人資料，包括在歐盟及美國間傳輸的個人資料，美國情報機構亦可根據總統發布的第 12333 號行政命令（EO 12333），針對境外公司進行此等個人資料之蒐集¹¹。

此外，2014 年 1 月 17 日時任美國總統歐巴馬發布「總統第 28 號指令（Presidential Policy Directive 28, PPD-28）」¹²，對美國情報機關對境外人士之「訊號情報」活動設下限制。然於 Schrems II 案中，歐洲法院因該指令未能有效規範「大規模且無差別之資料蒐集（bulk collection）」之行為等理由，宣告其未能提供歐盟人民適當保護。

因此，新發布之第 14086 號行政命令在很大程度上取代 PPD-28。新行政命令強化對所有訊號情報活動所設的條件、限制及保護措施，並建立一種新的救濟機制，使個人能夠訴諸及執行該些保護制度¹³。因該經總統發布之行政命令對整個情報體系具有拘束力，這些新要求將進一步透過情報機關之政策與程序轉化為

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

⁹ WP/254, *supra* note 8, ch. 4.

¹⁰ Draft Decision, *supra* note 6, recital 195; Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 45, 2016 O.J. (L 119)1, 87 [hereinafter GDPR].

¹¹ Draft Decision, *supra* note 6, recitals 115, 117, 118.

¹² *Id.* recital 119; see also Case C-311/18, § 138; *Presidential Policy Directive -- Signals Intelligence Activities*, THE WHITE HOUSE (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

¹³ Draft Decision, *supra* note 6, recital 119; EO 14086, *supra* note 4, sec. 5(h).

行政規則，以便作為其在日常實施之具體指引¹⁴。

美國透過訂定上述規範以實踐美國與歐盟之談判結果——即解決「隱私盾協定」無效後所留下之問題¹⁵。鑒此，在執委會於草案中評估美國現行法律架構時，該行政命令為特別重要之元素¹⁶。

二、限制與規範

第 14086 號行政命令就訊號情報活動（如資料之蒐集、使用與散播等）設立諸多原則，例如：此類活動必須基於法規或總統之授權且須符合美國現行法律、無論被蒐集個人資料的對象之國籍或居住國為何，需考慮到其等的隱私及公民自由等¹⁷。

為驗證訊號情報活動對於個人權利之侵犯，係為追求合法目的所必要（necessary）及相稱（proportionate），該些活動需符合多種限制及條件¹⁸。其中，第 14086 號行政命令列出進行訊號情報活動之 12 個合法目的及 5 個禁止目的¹⁹，且情報機構需經專門程序驗證此類活動具有優先性（priority），以證明該訊號情報活動係屬合理，且該活動之執行亦需符合必要性與相稱性標準²⁰。

就訊號情報蒐集之類型及手段，執委會指出於美國境內進行之資料蒐集應具有「特定性」²¹。對此，該行政命令規定訊號情報活動須以經過濾且係對特定目標所進行之「特定性蒐集（targeted collection）」為優先²²；當無法透過該特定性蒐集合理地獲取所需資料時，方可進行「大規模且無差別蒐集（bulk collection）」²³。同樣的，第 14086 號行政命令將該蒐集限於 6 個特定目的之追求，包括防止國際恐怖主義及間諜活動等²⁴。

針對美國情報機關所掌握之資料，行政命令規定其在資料處理上須遵守資料蒐集最小（data minimization）、資料安全與取得（data security and access）等原

¹⁴ *Id.* recital 120.

¹⁵ *See* Case C-311/18, §§ 185-188. 歐盟法院宣告美歐「隱私盾協定」無效之理由為：1. 美國法中並未將美國情報當局之權力限制在必要且相稱的範圍內；2. 歐盟公民在美國法院未有充分的救濟方式，以挑戰美國情報機關的監視活動。另參見：張書芳，愛爾蘭資訊保護委員會與臉書間跨境資料運輸爭議之發展，政治大學國際經貿組織暨法律研究中心經貿法訊，272 期，頁 19-25，<http://www.tradelaw.nccu.edu.tw/epaper/no272/4.pdf>（最後瀏覽日：2022 年 1 月 10 日）。

¹⁶ Draft Decision, *supra* note 6, recital 119.

¹⁷ *Id.* recitals 121-126; EO 14086, *supra* note 4, sec. 2(a)(i), (ii)(B).

¹⁸ Draft Decision, *supra* note 6, recital 127.

¹⁹ EO 14086, *supra* note 4, sec. 2(b)(i), (ii).

²⁰ *Id.* sec. 2 (a)(ii)(B), (b)(iii)(A).

²¹ Draft Decision, *supra* note 6, recital 134.

²² EO 14086, *supra* note 4, sec. 2(c)(ii)(A).

²³ *Id.*

²⁴ *Id.* sec. 2(c)(ii)(B).

則，以防止情報機關之濫用²⁵。

三、監督

第 14086 號行政命令要求每個情報機關需有資深的法律、監督及法遵官員，以確保其遵守現行美國法律，特別是其須定期監督訊號情報活動，並確保若有違反規範之情形，權利受損之個人仍可得到救濟²⁶。此一監督職能係由被指派之法遵官員、公民自由保護辦公室 (Civil Liberties Protection Office, CLPO) 官員及監察長履行²⁷。

四、救濟

執委會指出美國提供許多救濟途徑，使資料所有者更可能在獨立、公正且具有約束力之法庭提起法律行動。美國允許個人有其資料之取得權、允許個人提出審查政府取得該些資料之合法性的要求；且若發現違法行為，個人可透過更正或消除其個人資料，以作為救濟²⁸。

第 14086 號行政命令建立一具體的救濟機制，以處理及解決個人對與美國訊號情報活動有關的投訴。任何來自歐盟的個人如認為該訊號情報活動可能違反現行美國法律，而對其隱私和公民自由權利產生不利影響，皆有權經該救濟機制提交投訴²⁹。

在第一階段審查，來自歐盟之個人可向位於美國情報體系 (US Intelligence Community) 下的 CLPO 提出申訴，該單位將進行初始調查，以確定美國情報機關是否違反該行政命令之保障措施或是其他現行的美國法律³⁰；一旦確定其違反前述規定，將進一步認定個人可採之適當救濟方式³¹。CLPO 的決定將對情報體系產生約束力，使其接受第二階段審查³²。此外，第 14086 號行政命令亦明文保障 CLPO 審查之獨立性³³。

在第二階段審查，個人將有機會於新成立之 DPRC 對 CLPO 之決定進行上訴。DPRC 的法官將由美國政府以外之人士，且需具個人資料隱私及國家安全領

²⁵ *Id.* sec. 2(c)(iii). 「資料蒐集最小原則」之意涵與 GDPR 第 5 條相似，即個人資料之蒐集必須適當、相關且限於處理目的所必要。而第 14086 號行政命令規定訊號情報活動機關需制定政策與程序，以盡量減少其所蒐集之個人資料的傳播及留存。See also GDPR, art. 5.1(c).

²⁶ EO 14086, *supra* note 4, sec. 2 (d)(i)(A), (B).

²⁷ *Id.* sec. 2 (d)(i)(A); Draft Decision, *supra* note 6, recitals 154, 155.

²⁸ Draft Decision, *supra* note 6, recital 167.

²⁹ *Id.* recital 168.

³⁰ EO 14086, *supra* note 4, sec. 2(a)(i), 3(a).

³¹ *Id.* sec. 3(c)(i).

³² *Id.* sec. 3(c)(ii).

³³ *Id.* sec. 3(c)(iv).

域相關經驗、以及獨立審查案件之能力者擔任³⁴；另外，該職位可享有免受撤職之保護³⁵。而關於情報機關所進行之訊號情報活動是否違反現行美國法律，以及經認定違反後其將就受影響之個人實施何種救濟措施，DPRC 的裁決將具有法律約束力³⁶。

綜上所述，美國執法機關及國家安全機關取得屬本草案認定範圍內之個人資料時，將受美國現行法律架構之約束。進一步地說，該架構列出可取得個人資料的條件，及確保該些資料的後續使用僅限於追求公共利益目的所必要及相稱的範圍內；而具有有效救濟權之個人皆可訴諸以上保護措施³⁷。

參、外界評論與未來發展

Schrems 案的原告 Max Schrems 認為美國目前與美歐間個人資料傳輸有關之法律整體變動似乎相當微小。第 14086 號行政命令雖有些許修正（如引入比例原則或建立 DPRC），不過仔細探究後可發現該行政命令對於非美國公民之保護係誇大其詞且表現不彰。因此，美國任何基於第 14086 號行政命令而作成之符合歐盟適足性的認定，都可能無法滿足歐洲法院的要求³⁸。

儘管在草案中可見執委會努力解釋美國對於比例原則的處理及成果，有論者認為草案仍缺乏更深入的細節，以說明美國所採之措施如何與歐盟就個人資料之保護水準相當³⁹。

誠然，美國試圖與歐盟接觸並表明希望解決歐洲法院所認定的缺失，以繼續使資料得於美歐間傳輸⁴⁰；而執委會亦透過通盤考量美國現行法律體系，以及試圖了解美國何以在其現行法律架構下解決這些缺失，以衡量雙方的資料傳輸可否

³⁴ *Id.* sec. 3(d)(i)(A).

³⁵ *Id.* sec. 3(d)(iv).

³⁶ *Id.* sec. 3(d)(ii).

³⁷ Draft Decision, *supra* note 6, recital 192.

³⁸ Max Schrems 曾對第 14086 號行政命令提出批評，其主張：第一，美歐雙方可能對「必要性」與「相稱性」等用字上採不同的解釋，進而產生不同的保護效果。此外，Schrems 表示該行政命令仍允許「大規模且無差別審查（bulk surveillance）」，因目前所列之措施可追求的目的相當廣泛，故美國的監視活動是否能符合「歐洲基本權利憲章」第 52 條意義下之相稱性（或稱比例原則），值得深思。第二，新設的 DPRC 並非「歐盟基本權利憲章」第 47 條所規定之司法救濟管道，因其實為美國政府下之一行政部門，而非「法院」。See also *New US Executive Order Unlikely to Satisfy EU Law*, NYOB (Oct. 7, 2022), <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

³⁹ See Joseph Duball, *EU-US Draft Adequacy Decision Arrives, EU Process Begins in Earnest*, INT'L ASS'N OF PRIVACY PROF'LS (Dec. 13, 2022), <https://iapp.org/news/a/eu-us-draft-adequacy-decision-arrives-eu-process-begins-in-earnest/>.

⁴⁰ FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, THE WHITE HOUSE (Oct. 7, 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/>.

繼續。

該草案現正交由 EDPB 及歐盟成員國審查，不過即使 EDPB 及成員國對該草案持負面意見，然此等意見未能對執委會產生拘束力。因此，一旦該草案定案且公布，位於歐盟的公司即可據此傳輸資料至美國⁴¹。目前，執委會預計最快於 2023 年 7 月前作成最終決定，屆時用戶可以透過國內法院及歐洲法院對該決定提出異議⁴²。

肆、結論

自 2020 年 7 月歐洲法院於 Schrems II 案中裁定「隱私盾協定」無效以來，歐盟乃至全球企業在資料傳輸議題上，即面臨著重大的法律不確定性。第 14086 號行政命令經執委會審視且評估，確認其中規範美國情報機關為執法及國家安全目的所進行之資料蒐集僅限於實現合法目的所必要，且為保障歐盟公民權利及防止公權力之濫用，該命令亦訂定若干監督及救濟措施。基於上述理由，執委會認定美國已確保對自歐盟傳輸至美國境內公司的個人資料提供充分保護水準。儘管面對諸多批評，本次適足性草案之推出，無疑是美歐間於資料傳輸議題上的之一大進展。該草案現已公布並正在徵求 EDPB 之意見，最快將於 2023 年上半年完成定案，其後續動向仍值持續追蹤。

⁴¹ European Commission Press Release IP/22/7631, Data protection: Commission Starts Process to Adopt Adequacy Decision for Safe Data Flows with the US (Dec. 13, 2022).

⁴² Duball, *supra* note 39; Draft Decision, *supra* note 6, recital 199. 根據 GDPR 條第 58 條第 (5) 款及歐洲法院在 Schrems 案判決中之解釋，若一國資料保護主管機關質疑執委會作成的適足性認定與個人隱私及資料保護之基本權利有所衝突，該國必須提供其法律上之補救措施，以便將此些反對意見提交至該國法院，其或將作為歐洲法院初步裁決之參考。GDPR, *supra* note 10, art. 58(5); Case C-362-14, § 65.