

歐盟GDPR保護適足性審核與因應作為



歐盟GDPR保護適足性審核與因應作為

資訊工業策進會科技法律研究所
法律研究員 吳柏凭
2018年04月10日

壹、事件摘要

歐盟於 1995 年頒布個人資料保護指令(95/46/EC)[1]，對歐洲各國甚至全世界個人資料保護法制發展有極大影響力。然隨著資通訊技術發展變化迅速，網際網路與各項應用興起，既有歐盟個人資料保護指令面對這些變化已經難以為繼，歐盟執委會(European Commission) 出新的資料保護規則 (General Data Protection Regulation, GDPR)，於2016年4月27日通過，5月4日公布，正式成為歐盟第2016/679號規則 (Regulation (EU) 2016/679) [2]。由於歐盟原則上禁止個人資料跨境傳輸，只有在被認可具有保護適足性(Adequate level of protection)的國家或地區才能例外許可傳輸，因此如何獲得歐盟保護適足性認可，就成為能否跨境傳輸歐盟個資的關鍵。

貳、重點說明

一、個人資料保護指令保護適足性審查規定

1995年的個人資料保護指令，就有禁止會員國將個人資料跨境傳輸至對資料保護不具有保護適足性之國家[3]。在第25條第2項中，對於保護適足性的審查，包括資料的性質、處理目的和期間、資料的發生地及最終目的地、該國家施行的普通法及特別法規、以及安全措施等，透過個案綜合判斷是否具有保護適足性[4]。而關於具體的判斷標準，則依照第29條規定資料保護工作小組 (Article 29 Data Protection Working Party) 的指導文件[5]，其中對於法律規範審查，除了內容外，更重視個資保護的執行面。

二、GDPR保護適足性審查規定

GDPR延續了個人資料保護指令的規定，原則上禁止資料跨境傳輸至對資料保護不具有適足性之國家[6]。根據第45條第2項規定，適足性的評估包括以下要素：

1. **法治、對人權與基本自由之尊重、一般與部門之相關立法**，包括有關公共安全、防衛、國家安全及刑法、公務機關對個人資料之接近使用權、及該等立法、資料保護規則、專業規則及安全措施之執行。
2. **有一個或以上獨立監管機關之存在及有效運作**，或對象為國際組織時，確保及執行資料保護規則之遵守，包括充足之執行權，以協助及建議資料主體行使其權利，並與會員國之監管機關合作；
3. **個人資料向其他第三國或國際組織進一步移轉**，該其他第三國或國際組織之規則、判例法、及有效且可執行之資料主體權利及個人資料受移轉之資料主體有效之行政與司法救濟；第三國或國際組織所加入之國際協定，或其他因具法律拘束力之合約或辦法、及從其參與多邊或區域體系而生之義務，尤其關於個人資料保護者。

以上規定與個人資料保護指令最大不同在於將保護適足性的判斷標準明文化，同時補充個人資料向第三地再傳輸應注意的規範、具有獨立性監管機關等規定，填補原本個人資料保護指令的漏洞。

三、保護適足性認可程序與現況

保護適足性認可的程序^[7]為：

1. 來自歐盟執委會的提案。
2. 得到由歐盟各國資料保護機關組成之作業會議(European Data Protection Board)的意見。
3. 得到歐盟各國代表的承認。
4. 歐盟執委會合意認可。

縱然取得認可，之後也會每四年檢驗一次^[8]，如果被判定不具保護適足性，則仍會取消原本的認可^[9]。

現階段已通過保護適足性審核的國家地區包括：安道爾、阿根廷、加拿大（民間機構）、法羅群島、根西島、以色列、馬恩島、澤西島、紐西蘭、瑞士及烏拉圭，另有美國限於「隱私盾」框架(Privacy Shield framework)方可傳輸。

參、事件評析

（一）保護適足性認可的效益

除了取得適足性認可外，個別企業可以透過1.標準契約條款(Standard Contractual Clauses, SCC)；2.拘束企業準則(Binding Corporate Rules, BCR)；或3.取得同意方式進行跨境傳輸^[10]。但是取得適足性認可不但可以節省企業在個資跨境傳輸的成本，減輕企業負擔，同時也有助於整體產業突破歐盟貿易壁壘。

（二）通過保護適足性審核的困難

雖然現行通過適足性審核的國家地區有11個，惟需注意的是，根西島、馬恩島、以及澤西島都是英國屬地，法羅群島是丹麥屬地，而安道爾和瑞士都是在歐洲境內，這些國家地區的法規範本來就與歐盟差距不大，加上美國及加拿大國家本身不被認可具適足性，實際上不屬於歐盟法體系而通過適足性審核的國家地區非常有限。而且包括以色列、烏拉圭或紐西蘭在申請認可都花超過三年的時間，因此也不能作為短期的因應措施。

此外，在要件方面，規範上雖然我國個資保護規範與GDPR未有極大歧異，但只要存有差異，要取得認可就有極高困難度，這些都需要與歐盟執委會溝通。而在監管機關要求方面，雖然沒有要求單一機關，但對於機關的「獨立性」仍有要求。關於機關的獨立性目前歐盟並沒有明確的標準，但在歐盟法院判決中，有因為德國的州對州層級的資料監管機關進行調查的權力，而被認為不具獨立性^[11]。

（三）通過適足性審核的具體作為

以日本為例，為了取得歐盟適足性認可，在2015年9月就其個人資料保護法（個人情報保護法）進行修正，其中設立個人資料保護委員會（個人情報保護委員會）即是為了符合適足性要求中「獨立監管機關」規定，而第24條跨境傳輸的規定更是重要。

日本個人資料保護委員會在2016年就與歐盟執委會溝通三次^[12]，同時在2017年發出共同聲明^[13]。在不修正法律的狀況下，日本個人資料保護委員會頒布一指導方針來消除差異，並於於2018年2月9日先揭示調適方向^[14]，包括：

1. 將歐盟視為敏感性個人資料而日本未明文規定者，解釋上一律視為敏感性個人資料。
2. 歐盟不管個人資料保管期間，一律可以主張權利，而日本則限保管期間6個月以上方可主張權利。指導方針對於歐盟跨境傳輸的個資，不管保管期限一律許其主張權利。
3. 對歐盟跨境傳輸的個資將要求揭露特定利用目的。
4. 對於歐盟跨境傳輸的個資再移轉，必需要透過契約等規制，確保資料受保護水準。
5. 關於歐盟跨境傳輸的個資，在去識別化一定要確認無法再識別，以與歐盟去識別化資料定義相符。

肆、結語

歐盟GDPR已施行在即，如何因應以突破其跨境傳輸的限制將不只是單純避免業者受罰，更是跨越歐盟貿易壁壘的重要關鍵，而在眾多例外許可跨境傳輸的方法中，又以取得保護適足性認可為最根本因應之道。雖然現在取得認可的難度極高，但仍有許多能努力的空間，目前我國也著手申請適足性認可的準備，未來能得到何種程度的回應，值得後續觀察。

[1] 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.

[2] Reform of EU data protection rules, European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited Apr.10, 2018).

[3] Data Protection Directive, art. 25(1).

[4] Data Protection Directive, art. 25(2).

[5] European Commission, Working Party on Protection of Individuals with regard to the Processing of Personal Data, Working Documents Transfers of personal data to third countries: Applying Articles 25 and 26 of EU data protection directive, July 24, 1998.

[6] General Data Protection Regulation, art. 45.

[7] Adequacy of the protection of personal data in non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (last visited Apr.10, 2018).

[8] General Data Protection Regulation, art. 45(3).

[9] General Data Protection Regulation, art. 45(5).

[10] General Data Protection Regulation, art. 46.

[11] European Commission v. Federal Republic of Germany (C-518/07).

[12] 個人情報保護委員会，個人情報保護委員会の国際的な取組について，https://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai2/siryoku3.pdf (last visited Apr.10, 2018).

[13] JETRO，個人データ保護の「十分性認可」取得の好機に一日EU首脳が共同声明－，<https://www.jetro.go.jp/biznews/2017/07/845f14ec50674c94.html> (last visited Apr.10, 2018).

[14] 個人情報保護委員会，EU 域内から十分性認可により移転を受けた個人データの取扱いに関するガイドラインの方向性について，https://www.ppc.go.jp/files/pdf/300209_siryoku1.pdf (last visited Apr.10, 2018).

■ 関連連結

- [Reform of EU data protection rules, European Commission](#)
- [Adequacy of the protection of personal data in non-EU countries](#)
- [JETRO：個人データ保護の「十分性認可」取得の好機に一日EU首脳が共同声明－](#)

■ 関連附件

- [個人情報保護委員会，個人情報保護委員会の国際的な取組について \[pdf\]](#)
- [個人情報保護委員会，EU 域内から十分性認可により移転を受けた個人データの取扱いに関するガイドラインの方向性について \[pdf\]](#)

你可能会想参加

- 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
- 個人資料保護新思維企業法遵論壇
- 【實體】2024科技研發法制推廣活動—科專個資及反詐騙實務講座
- 【直播】2024科技研發法制推廣活動—科專個資及反詐騙實務講座
- 中部場—商業服務業個資保護工作坊
- 南部場—商業服務業個資保護工作坊
- 北部場—商業服務業個資保護工作坊
- 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會
- 電商零售業法制宣導說明會暨產學研座談會
- 零售業個資保護宣導暨座談會
- 零售業個資保護及資訊安全教育講習
- 零售業個資保護及資訊安全教育講習

吳柏凭

法律研究員 編譯整理

上稿時間：2018年04月

文章標籤

個資去識別化

個資管理制度

個人資料保護與管理

 推薦文章