國立政治大學國際貿易與經營學系研究所

碩士學位論文

歐盟與美國有關雲端運算產業從事跨境資料傳輸法制之比較研究

A Comparative Study on EU and US Data Protection Laws Governing Transatlantic Data Flow Services by Cloud Computing Industry

指導教授：楊培侃 博士

研究生：紀珮宜 撰

中 華 民 國 107 年 7 月

DOI:10.6814/THE.NCCU.IB.015.2018.F06

謝辭

終於完成碩士論文，也代表我在政大六年的日子正式結束了。真的很感謝一路上陪伴我，幫助過我的人。能順利完成論文，首先要感謝指導教授楊培侃老師耐心的陪我討論，並給我很多寫作上的建議，使此篇論文得以順利如期完成。另外，也要謝謝楊光華老師、施文真老師和薛景文老師在這兩年來的指導和教誨，並給予我不僅是課業上，甚至是未來工作與待人處世的寶貴建議。接著謝謝一直陪我待在法學中心，一起努力撐過兩年研究所生活的同學—旺達、俞慶、明億、筑羽、郁淳、芸昕，還有從德國交換回來後加入我們的詩晴。認識你們，並和你們一起渡過研究所的生涯是我莫大的幸運，希望你們一切順利。能夠順利完成學業也必須要感謝一路支持我、給予我很多自由選擇空間的家人，你們的關心和鼓勵一直都是我積極努力的動力。最後，謝謝在政大遇到的一切，法組的學長姐、國貿所其他三組的同學、國貿系香瑩、玉如、柳沫和盈君助教、外交系的教授和同學、國際發展書院的夥伴、財政系徐麗振老師、洪德欽老師、讀書會的同學等，謝謝你們成為我在政大六年生活中不可或缺的一部分，謝謝你們讓我的求學生活更美好。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

摘要

近年來，雲端運算科技快速發展，對企業的營運模式帶來巨大改變，快速成長的歐盟市場則成為美國大型雲端業者積極爭取進入的目標。對雲端運算產業而言，資料的自由傳輸為服務提供的必要條件，但資料傳輸的過程中涉及個人資料及隱私之保護，歐盟和美國在此議題上立場與看法的差異成為雲端運算業者市場進入的主要障礙。另外，在 2018 年歐盟通過更為嚴格的資料保護規則，將雲端運算業者納入規範範圍，增加企業保護資料之義務，使得雲端運算業者成本增加。而針對跨大西洋的資料跨境傳輸，根據歐盟之規範，僅有達到與其相同保護水準之第三國得以將資料跨境傳輸到該國。而傳統美國公司所使用的傳輸途徑包含資料主體同意、標準化契約條款及企業內部約束規則皆未能有效提供雲端產業在進行大量且重複性的資料傳輸時所需要的法律依據。因此多數雲端業者皆使用歐盟與美國為跨大西洋資料傳輸所共同發展出來的跨境傳輸協議──隱私屏障協議作為跨境傳輸的基礎。

鑑此，本文透過分析歐美隱私屏障協議之內容，認為協議較先前的安全港協議對擁有資料並進行處理的企業要求更多的義務，同時也賦予資料主體更多權利可以確保隱私。然即便如此，本文認為該協議仍不足以符合歐盟對於資料隱私保護水準之要求，故建議歐美雙方應針對防止個人隱私因大規模情報蒐集受侵害，以及提供受損害之個人有效救濟途徑的問題進行重新談判，以避免未來隱私屏障協議面臨被判決無效之法律風險。

關鍵字：資料保護規範、隱私屏障協議、隱私權、跨境資料傳輸

DOI:10.6814/THE.NCCU.IB.015.2018.F06

Abstract

In recent years, Cloud Computing has developed rapidly, and has brought big changes in the management model of enterprises. The fast-growing European market becomes the battlefield that all the American large cloud-computing providers aggressively try to get in. For the cloud computing, transferring data without limit is the essential condition in providing services; however, inevitably, the transferring process involves the issue of personal data and privacy protection. The EU and America hold different opinions over this issue, and the differences are the main barriers that prevent cloud-computing providers from entering the European market. In addition, the EU passed a more stringent rule, the Data Protection Regulation, in 2018, and covered the cloud-computing providers by imposing the obligation of protecting data on the enterprises. As for the transatlantic-data flow, according to the EU law, only the country who has the same level of personal data protection is allowed to transfer the data across the border. In this case, the majority of cloud-computing providers adopt the EU-US Privacy Shield Framework, a cross-border data transfers agreement specifically designed for the transatlantic-data flow by the EU and America, as their key foundation. In view of this, this thesis analyzed the content of EU-US Privacy Shield Framework, and concluded that this agreement requires more obligations for the enterprises, which are handling data, than the previous Safe Harbor Framework agreement, while it also gives the data subject more rights to ensure privacy. Nevertheless, this thesis believes that this agreement is still insufficient to meet the EU's standard of data privacy protection. Therefore, it is suggested that both parties, the EU and America, should renegotiate the approaches that prevent personal privacy from being compromised by mass surveillance and data collection and provide affected individual with effective legal resorts to remedy damage, with the aim of avoiding the legal risk of EU-US Privacy Shield Framework being determined invalid in the future.

Keywords: data protection regulation, Privacy Shield Framework, right to privacy, cross-border data flow

DOI:10.6814/THE.NCCU.IB.015.2018.F06

目次

DOI:10.6814/THE.NCCU.IB.015.2018.F06

DOI:10.6814/THE.NCCU.IB.015.2018.F06

圖次

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第一章 緒論

雲端運算（Cloud computing）市場近年來隨著科技的進展而快速成長。根據統計，2018 年全球將會有半數以上的企業使用公共的雲端平台提供服務，且雲端的應用、平台和服務將會持續快速地改變企業營運的模式[1]。所謂的雲端運算可以被認為是透過網路，利用遠端或外部伺服器進行資料處理的方法[2]。此種因應科技發展所興起的產業為各國帶來鉅額的經濟效益，卻也帶來同等的風險，尤其是科技快速發展通常伴隨對現有法規制度的挑戰。對於雲端運算產業而言，大量使用個人資料作為服務提供之基礎，引發各國對於侵害個人資料隱私權的疑慮。而各國對於個人隱私權的看法和保護手段的差異，使得雲端產業所面臨的法規挑戰更為複雜，尤其是歐盟和美國之間更是如此。歐盟將隱私權視為公民之基本權利不得侵犯，且透過資料保護指令提供歐洲公民許多資料保護的權利，但相反的，美國的法律體系在個人資料的保護上較為鬆散，使得作為雲端運算產業主要服務提供者的美國業者，在進入歐盟市場時遇到莫大的阻礙。法律關於隱私權的規範可能是雲端運算產業發展，以及各國雲端運算市場連結之最大阻礙，且美國雲端業者提供服務予歐盟市場所涉及資料跨大西洋的傳輸，更是引起歐盟內部許多個人與隱私保護倡議組織的疑慮，故詳細檢視歐盟和美國資料保護之規則以及雲端業者進行跨境資料傳輸之行為對於隱私權的影響有其必要。

第一節 研究動機與目的

[1] Forrester, *Predictions 2018: Cloud Computing Accelerates Enterprise Transformation Everywhere*, Nov. 7, 2017, https://www.forrester.com/report/Predictions+2018+Cloud+Computing+Accelerates+Enterprise+Transformation+Everywhere/-/E-RES139611.

[2] Kommerskollegium, *Swedish National Board of Trade. How Borderless is the Cloud？: An Introduction to cloud computing and international trade*. Sep., 2012, at 3, *available at* https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/how_borderless_cloud_e.pdf

DOI:10.6814/THE.NCCU.IB.015.2018.F06

近年來，尤其是在美國前中央情報局官員史諾登（Edward Snowden）揭露美國對於外國人大規模無差別的情報監控後，各國對於個人資料隱私越來越重視。不只美國修改其國內關於情報蒐集的政策與法案，歐盟也加快改革資料保護規則的腳步，以確保對於隱私權最高水準的保護。然而對於現今網路普及的數位世代，資料的傳輸和使用為許多新興產業不可或缺的重要基礎，尤其是在全球化市場中，資料的跨境傳輸更是常見。但目前國際上缺乏統一的隱私保護規範，使得各國法律規範程度的落差形成產業發展的障礙。作為雲端產業主要服務提供者的美國，以及主要市場之一的歐盟，就個人資料保護的爭議更是長期存在。美國業者在進入歐盟市場提供服務時，在符合歐盟跨大西洋資料傳輸規範的議題上遇到許多阻礙，失去進入歐盟市場的機會將使美國雲端業者蒙受鉅額經濟損失。在此一背景下，如何確保美國業者取得合法且有效的跨大西洋資料傳輸方法，實為重要且必須優先解決的議題。因此，本文將會首先說明大西洋兩岸的法規落差，接著檢視現況下的制度是否得以提供美國雲端業者克服法規障礙的方法，確保跨大西洋資料傳輸的穩定性。

另外，在 2015 年前，多數美國業者都是以歐盟執委會與美國商務部共同發展之「安全港框架協議（Safe Harbor Framework）」作為跨大西洋資料傳輸的法律基礎，然而該協議在 2015 被法院宣告無效。取而代之的是 2016 年通過的歐美「隱私屏障協議（Privacy Shield Framework）」，此協議加強了安全港協議中的規範，目前是多數雲端服務業者跨大西洋資料傳輸的法律依據。因此，本文亦試圖分析隱私屏障協議施行後，是否得以確實作為有效的跨大西洋資料傳輸的基礎，協助美國業者在透過使用資料獲利的同時，也得確保歐盟公民的隱私權受到完善的保護。

第二節 研究架構

因本文通篇將以雲端運算產業為基礎，了解該產業在現況的隱私保護制度

DOI:10.6814/THE.NCCU.IB.015.2018.F06

下，所遇到關於跨境資料傳輸之困境，故將在第二章將先針對「雲端運算產業」之定義、產業型態與使用雲端運算之利益與風險進行完整的說明，同時也會介紹目前雲端運算產業的現況，以解釋進入歐盟市場對於美國雲端業者之重要性，並突顯法規落差造成之阻礙的影響。接著本文將於第三章分析歐盟與美國兩個法律制度對於資料隱私權的規範落差。歐盟在 2018 開始施行改革後的新資料保護規則，因此第三章之分析也會包含新的資料保護的規範內容。並著重在保護目的、保護手段、提供予個人之權利與賦予業者的義務和法律的執行等各個面向的分析，進行異同比較。對於雲端運算產業而言，資料跨境傳輸為不可或缺的要件，因此，本文將於第四章說明在歐盟新舊資料保護規範下對於跨境資料傳輸的法規差異，以及目前業者履行這些規範義務以進行跨境資料傳輸的方法，並分析雲端運算產業是否因其產業特性而遇到更多阻礙。如前所述，雲端運算業者最廣泛使用的跨境傳輸途徑為隱私屏障協議，該協議之有效性以及未來可能會遇到的風險為本文第五章之重點。最後將完整的分析於第六章作一結論。本文希望可以透過對於資料保護規範之通盤介紹與分析，以及對於現行資料跨境傳輸途徑之檢討，了解美國雲端產業進入歐盟市場的阻礙以及得改善之方向。

第三節 研究方法

為了解雲端運算產業、歐美資料保護規範落差與跨大西洋資料傳輸的現況，本文主要透過文獻回顧法整理相關文獻，以及透過比較法的方式分析歐美規範以及歐盟新舊規範之異同。在雲端運算產業的部份，該產業發展快速涉及之範圍廣大，許多國際組織、各國政府和學者都分別對此議題進行探討，故此部分將以歸納國內外新聞，產業、國際組織和研究機構之報告為主，並輔以調查數據以了解該產業之發展與現況。另外，針對歐盟與美國資料保護規範以及雙方簽訂之協議，本文透過相關條文介紹與比較的方式審視規範之異同，並整

DOI:10.6814/THE.NCCU.IB.015.2018.F06

理學者與該領域之官方專家小組的意見（如歐盟資料保護指令第二十九條工作小組意見書）試圖釐清雲端運算產業在進行資料傳輸時所面臨之歐美法規落的具體落差與障礙，及各方之看法與建議[3]。最後在隱私屏障協議規範探討的部份，以歐美對於隱私屏障協議第一次共同審查之報告為主要分析框架，分別說明該規範對於解決舊有跨境資料傳輸協議之問題是否有效，以及未來可能發生的法律風險[4]。

[3] Opinion 05/2012 on Cloud Computing, July 1, 2012, WP196, 01037/12/EN; Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, Apr. 13, 2016, WP238, 16/EN.
[4] EU – U.S. Privacy Shield – First annual Joint Review, Nov. 28, 2017, WP255, 17/EN.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第二章 雲端運算服務產業發展與個人資料隱私保護

隨著雲端運算產業的快速發展，許多關於雲端運算所帶來的效益與問題隨即引發許多討論。觀察目前的市場，大型的美國公司仍是雲端運算產業的主要服務提供者，而歐盟則是這些公司極欲拓展的海外市場。對於歐盟境內的個人、企業或任何組織而言，是否要採用雲端運算服務必須要進行效益與風險的分析，就效益面而言減少成本、刺激創新是雲端運算服務可以帶來的主要好處；反之，雲端運算所帶來的風險則包含伺服器安全風險、失去對於 IT 技術的控制等。尤其是因為雲端運算科技必然會牽涉到跨境資料的儲存、取得和處理，跨境的資料傳輸便成為該產業不可或缺的要件。目前各國政府皆採行不同的方式保護個人資料的隱私，故服務提供者在進入海外市場時，個人資料的保護的法律規範成為首要解決的問題[5]。本章將先介紹整個雲端運算產業，包含雲端運算的定義、特性、服務提供模式與市場現況，並說明雲端運算對於服務使用者所帶來之具體利益與可能造成的問題。最後說明歐美之間對於資料隱私保護的規範落差是美國雲端業者進入歐盟市場的最大阻礙。

第一節 雲端運算服務之定義與市場現況

近年來雲端運算產業快速成長，使得許多資訊科技的廠商都爭相進入該產業，「雲」或是「雲端運算」等詞彙近年來也十分受歡迎並被廣泛使用。然而目前對於雲端運算並沒有統一和絕對的定義，不同國家、組織甚至公司都有其對於雲端運算定義的闡述，會產生多重定義同時存在的現象，主要是因為「雲端運算」指的並非一項特定的科技，而是一個同時涵蓋多項科技的概念[6]。根據經

[5] Forrester, *supra* note 1

[6] OECD, *Cloud Computing: The Concept, Impacts and the Role of Government Policy*, at 8, OECD Doc. DSTI/ICCP(2011)19/FINAL, (Aug. 19, 2014), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2011)19/FINAL&docLanguage=En.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）在 2014 年所發布關於雲端運算概念、影響和政策的報告，目前有兩個組織對於雲端運算的定義較具代表性，分別為美國國家技術標準局（National Institute of Standards and Technology, NIST）以及美國柏克萊大學 RAD 實驗室（Berkeley RAD Lab）[7]。其中美國 NIST 所作之定義更是被許多學者公認最具權威性而被廣泛引用[8]。美國 NIST 所定義的雲端運算是：「使用無所不在（ubiquitous）、便利（convenient）及隨需應變（on-demand）的網路，共享廣大運算資源（如：網路、伺服器、儲存、應用程式與服務）的模式。該模式可以透過最少的管理資源或和服務提供者的互動，快速的提供各項服務。」[9]。而柏克萊大學 RAD 實驗室的定義則是：「雲端運算指的是透過網路進行服務的應用程式以及在資料中心（data center）提供該些服務的硬體（hardware）與系統軟體（systems software）[10]」。NIST 的定義著重在雲端運算的目的，而柏克萊大學 RAD 實驗室的定義則著重在具體構成雲端運算的要件[11]。簡單來說，所謂的雲端運算可以被理解為「使用者可以透過網路連接至伺服器，並依其需求隨時隨地大量存取共享的運算資源和使用各種應用程式的服務。」

雲端運算服務有下列幾項重要的特性，這些雲端運算的特性使得雲端科技的使用具有特有的優勢和風險，這些特性也會影響各國政府在制定政策與訂立

---

[7] *Id*.

[8] Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 79, WASHINGTON AND LEE LAW REVIEW, 341, 356 (2013).

[9] Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, Sep,. 2011, *available at*: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf, providing that.''Definition: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models….''.

[10] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica & Matei Zaharia, *Above the Clouds: A Berkeley View of Cloud Computing*, at 8, Feb. 10, 2009, *available at*: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[11] OECD, *supra* note 6.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

規範時的考量，也是企業在決定是否使用雲端運算服務時的依據[12]：

（1） 隨需應變的自助服務（On-demand Self-service）：雲端運算的特性之一是透過網路使用遠端的運算服務，當雲端服務部署完成後消費者可以在任何時候使用服務，而不需要一定要和服務提供者互動。

（2） 廣泛的網路連結（Broad Network Access）：因為網路科技的興起，不論地點雲端運算的使用者都可以透過將終端設備連結到遠端的伺服器取得服務，同時只要網路訊息的傳遞經過標準化的機制，使用者得以自由的使用運算資源。

（3） 資源匯聚（Resource Pooling）：雲端服務提供者的運算資源會被匯集於遠端的伺服器，並根據雲端使用者的需求以多租戶的模式（multi-tenant model）動態的分配運算資源[13]。因此許多雲端運算使用者可以同時且不互相影響的使用運算資源，雲端服務的提供可以很容易的規模化。

（4） 快速且具彈性（Rapid Elasticity）：運算資源得以快速的提供給需要的雲端使用者，且供應的規模具有彈性，意即使用者可以在任何時候取得不限規模的運算資源。因此使用資源的規模大小得由使用者決定，可以配合使用者不同時期的需求調整。

（5） 可計算的服務（Measured Service）：運算資源可依其所提供的服務特性被自動控管及最佳化。同時這些運算資源的使用可以被監督、控制和回報，以提供雲端服務提供者和使用者資源使用的透明性。這些資料通常亦是服務計費的基礎[14]。

---

[12] 美國 NIST，The NIST Definition of Cloud Computing, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdfdomanm/csci411/Handouts/NIST.pdf.

[13] 所謂的多租戶模式指的是一種軟體架構的技術，用於探討與實作如何於多用戶的環境下共用相同的系統或程式元件，並且仍可確保各用戶間資料的隔離性。定義參考：工研院，「商品履歷追蹤先導驗測計畫方案規劃」，2011 年，第 47 頁，網址：https://www.bsmi.gov.tw/wSite/public/Data/f1459144012515.pdf。

[14] 雲端運算服務的計價方式通常為「每次使用付費（ pay-per-use 或 charge-per-use）」。Peter Mell, *supra* note 9.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

此外，根據柏克萊大學 RAD 實驗室對於雲端運算的定義，雲端運算涵蓋了非常廣泛的服務，包含軟體、平台和基礎設施，雲端運算服務也因提供的服務不同而有不同的分類。這些服務的模式主要可以被分為下列 3 類：

首先，是雲端服務業者提供軟體─軟體即是服務（Software as a Service, SaaS）， 在 SaaS 模式下，雲端使用者所使用的是服務提供者在雲端基礎設備上所部署的應用程式（application），使用者並不管理作業平台、系統、硬體和資訊基礎設備，對於雲端使用者而言是較為便利的服務模式，例如：微軟公司提供的 Office 365。第二，雲端服業提供者所提供的是可以部署軟體的平台─平台即是服務（Platform as a Service, PaaS），在 PaaS 的模式中，雲端使用者可以使用這些平台（如作業系統平台、系統開發平台）部署及撰寫自己的應用程式。意即雲端使用者可以直接在平台上撰寫其所需之應用程式。使用者同樣不需要管理和控制雲端的基礎設備，相較於 SaaS 雖然因為需要自行撰寫應用程式，便利性較低，但更具有使用的彈性，例如：Google 提供的 App Engine。最後是由雲端運算業者提供雲端科技的基礎設備─基礎設備即是服務（Infrastructure as a Service, IaaS），在此模式下服務提供者提供雲端使用者運算的原始資源（例如：程式語言、儲存空間等）和硬體環境（伺服器）等。服務提供者允許使用者直接取得原始的運算資源（網路元件），相較於 SaaS 和 PaaS，雲端服務使用者擁有更多彈性，例如：IBM 提供的 SoftLayer[15]。不同的服務模式，雲端使用者和服務提供者所得之利益不同，同時也會面對不同的政策和法規上的挑戰[16]。

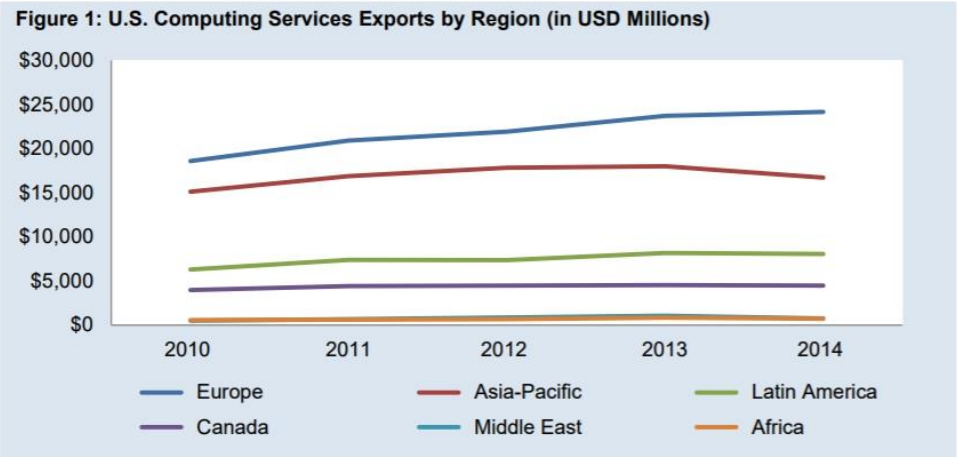
---

[15] NIST, *supra* note 12.

[16] 除此之外，雲端運算在服務的對象以及提供運算資源的組織上也有不同的分類，有些雲端運算服務僅有特定組織成員才得取得，其他雲端服務則可讓一般大眾使用，美國 NIST 同樣針對使用的對象有 4 種不同類型的定義。私有雲（Private Cloud）：所有雲端的系統、應用程式和資料都只屬於企業內部和提供資訊設備的廠商，意即「內部雲（internal cloud）」；社群雲（Community Cloud）：雲端運算的服務主要是提供給特定社群的消費者，而這些使用者通常有共同利益，或關注的議題相仿（例如：醫療產業的資訊交流），管理和營運可由一個或多個組織執行。例如：IBM 的智慧社群雲；公用雲（Public Cloud）：雲端的基礎設備由服務提供者擁有，但其服務的對象是大眾，公共雲的主要獲利來自於使用費用和廣告，例如：Google Apps；

DOI:10.6814/THE.NCCU.IB.015.2018.F06

目前全球雲端運算的市場狀況根據國際研究暨顧問機構 Gartner 2017 年的報告指出，2017 年全球公共雲端運算服務市場的規模將增加至 2,468 億美元，相較於 2016 年成長了 18%[17]。在 2013 年，美國的研究中心也針對網際網路和美國人的生活進行了一項調查計畫，結果指出在 2013 年已經有大約 69%的美國人在使用網路信箱、其他網路的軟體或是網路資料的儲存空間，而使用者也將會持續增加[18]。雲端運算產業被認為是極具發展潛力的市場，而在此市場中，美國的大型企業占據領先的地位，為三項雲端服務型態之主要的服務提供者，目前市占率前三名的公司分別為亞馬遜網路服務公司（Amazon Web Services）、微軟（Microsoft）和 Google[19]。而美國主要的雲端服務出口市場排名，第一大出口市場為加拿大，接著是日本和英國。但若以地區為基礎，歐洲（歐盟國家）仍為最重要的出口市場（如圖一）[20]。



圖一 美國雲端服務出口市場（以地區畫分）

混合雲（Hybrid Cloud）：兩種或多種不同的雲端部署模式混合而成。*Id.*

[17] Gartner 是全球最大的高科技產業分析及資訊科技與應用研究公司。Louis Colunbus, *Roundup Of Cloud Computing Forecasts, 2017*, FORBES (Apr. 29, 2017), https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#5135867031e8.

[18] See John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RES. CTR. (Sept. 12, 2008), http://pewresearch.org/pubs/948/cloud-computing-gains-incurrency.

[19] Barb Darrow, *Amazon Still Leads Cloud Rankings, But Competition Is Coming On Strong*, FORTUNE (June 15, 2017) http://fortune.com/2017/06/15/gartner-cloud-rankings/.

[20] ITA, *2016 Top Markets Report Cloud Computing*, at 3, Apr., 2016, https://www.trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

資料來源：美國商務部國際貿易局，

https://www.trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf

第二節 雲端運算服務之優勢與限制

雲端運算科技的應用對公、私部門的組織帶來許多利益，而這些利益主要可以分為兩個層面，一方面是讓使用的企業降低成本並促進企業發展；另一方面則是降低資料運算產業的市場進入障礙，增加新創公司進入市場，和既有公司擴張業務的機會，然而也因為雲端產業的特殊性質，也會造成不同於一般產業的挑戰和疑慮。本節將分別敘述使用雲端科技所帶來的利益與限制。

第一目 雲端運算服務之優勢

首先，企業使用雲端運算減少的成本可分為下列數個方面：

1. 減少資訊與通訊科技（Information and Communication technology, ICT）的成本支出

對於企業而言最直接的好處就是可以降低企業直接的 IT 成本支出，企業相較以往在取得運算資源上更快速且有彈性，組織不需要耗費時間和金錢去更新基礎設備，而可以透過雲端快速的購買所需的運算資源[21]。而且雲端服務的使用也可以改善企業普遍投入過多 IT 設備支出的問題，過去許多公司或政府單位為了因應未來可能對於 IT 設備的需求，會購買比實際需求更多的 IT 設備，這些設備通常都未能被充分利用而造成成本的浪費[22]。

[21] OECD, *supra* note 6, at 12; Deloitte, *Measuring the economic impact of cloud computing in Europe*, at 56, Jan.10, 2017 https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe. 根據歐盟的市場分析報告，使用雲端運算服務，歐盟整體而言可以降低 20%-50%的 IT 支出，而且在 2010 年到 2015 年間，光是英國、德國、法國、義大利和西班牙的 IT 成本就節省了共 140 億 7400 萬歐元。

[22] OECD, *supra* note 6, at 12; Sean Marston, *Cloud Computing—Business Perspective*, 51, DECISION SUPPORT SYSTEMS, 176, 181 (Apr., 2011). 根據統計，在 2000 年，超過 45%的資本設備運算被使

DOI:10.6814/THE.NCCU.IB.015.2018.F06

2. 將 IT 支出從原本的資本支出（Capital expenditure）轉為營運費用（Operating expenses）

相較於傳統上把 IT 系統作為資本投資，使用雲端服務的企業會視 IT 為營運支出（operational expense），節省下來的成本可以作為他用。甚至透過雲端的技術，服務者所提供的基礎設備可以同時供不同的使用者使用，個別使用者相互獨立不互相影響。而且當越來越多使用者使用雲端運算服務，會使得該項服務因為需求增加而達到規模經濟的效果，使用雲端服務的費用和成本也可以逐漸減少[23]。讓企業進一步擁有更多資本進行其他投資以提升未來的生產力與成長[24]。

3. 規模化（Scalability）和可適應性（adaptability）

雲端運算的技術讓雲端服務使用者可以有規模大小上的彈性，意即雲端運算讓企業有能力，也更容易根據消費者的需求擴大或縮小其服務規模，並隨時增加和移除 IT 的運算能力或儲存空間。這對於工作量變化大（如面對季節淡旺季的差異）的公司而言是一項優勢，也因為可以隨需求調整 IT 服務，企業有能力可以應付未預期的成長或暫時性的需求變化[25]。此外，雲端運算也讓企業得以最小化或甚至免除掉預期與非預期的停機時間（downtime），促進使用者服務的品質和企業運作的持續性[26]。

而就降低資料運算產業的市場進入障礙的部分，雲端運算科技可以帶來下列優勢：

用在 IT 系統上，然而這些設備平均只有 6%的產能被利用。雲端運算可以幫助減少 IT 設備支出的浪費以及維護這些設備的支出。

[23] *Id*. at 178.

[24] Deloitte, *supra* note21, at 56. 根據歐盟的調查報告，英國、德國、法國、義大利和西班牙透過雲端運算服務的使用，在 2010-2015 年間亦省下 1 億 3000 萬歐元的 IT 營運費用。

[25] *Id*.

[26] 所謂的停機時間指的是設備因為維護或失效而不能運作或生產的時間。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

1. 降低市場進入成本，縮短產品部署的週期以加快上市速度

雲端科技提供企業現有的硬體可以提供服務，企業不需要在進入市場的前期投入大量資本建立 IT 系統，可以更快速的進入市場。新創公司也因需要的資本投入減少而增加，中小企業亦獲得更多機會可以參與市場的運作[27]。此外原本 IT 基礎設施不足的第三世界國家也有更多機會可以透過雲端平台拓展 IT 服務[28]。另一方面，雲端運算的使用大幅縮短 IT 產品或服務的生命週期，應用程式或軟體的部署速度大幅加快，增加產品和服務的可得性（availability），資源的利用也極大化。

2. 刺激產業創新與新形態服務型態的出現

使用雲端運算服務同時也可以省去自行管理 IT 系統的時間和資本花費，企業的經營者可以將心力移轉到創新和研發，亦有利企業的整體發展[29]。雲端運算也可以降低企業創新的 IT 障礙。例如近年來 Facebook 和 Youtube 的出現及為例證[30]。同時雲端運算也促成過去未能想像的新型態服務和應用程式出現。例如：移動式的互動程式（Mobile interactive application）、大數據分析等[31]。因此可以說雲端科技對於雲端服務使用者不只帶來成本降低的好處，亦促使新創及中小企業更容易進入市場，也刺激創新的服務型態出現。

雲端運算服務分別也為美國和歐盟帶來不同的經濟效益，並使美歐政府皆制定相關政策以促進該科技於其市場內發展。在 2011 年美國歐巴馬政府即發布「聯邦雲端運算策略（Federal Cloud Computing Strategy）」也是所謂的「雲端第一（Cloud First）」政策，該政策的主要目的是希望透過使用雲端運算來降低資源的浪費以改善美國政府的行政效率[32]。另外，根據歐盟官方所支持的研究報

[27] OECD, *supra* note 6, at 12.
[28] Sean Marston, *supra* note 22, at 178.
[29] Deloitte, *supra* note21, at 56.
[30] Sean Marston, *supra* note 22, at 178.
[31] *Id*.
[32] Vivek Kundra, *Federal Cloud Computing Strategy*, at 7, Feb. 8, 2011,

DOI:10.6814/THE.NCCU.IB.015.2018.F06

告結果顯示，大規模的使用雲端運算科技亦對歐盟帶來巨幅的經濟利益[33]。該報告指出，雲端運算服務的運用在 2015 年到 2020 年間將為歐盟帶來總共 4,490 億歐元的利益[34]。歐盟執委會也早在 2012 年就為了促進雲端產業於歐盟境內的發展而提出「發揮歐洲雲端運算潛力（Unleashing the Potential of Cloud Computing in Europe）」的策略，並以此為基礎發展出一系列政策計畫[35]。

由此可知，雲端運算服務對於使用者、服務提供者和整體社會而言都有所助益，甚至歐盟的產業報告指出，雲端運算服務對於歐洲境內使用該服務的個別組織（包含企業和政府）所帶來的正面效益大於對歐盟服務提供者與整體社會所帶來的效益[36]。但即使如此，並非所有企業、組織，甚至是個人都願意使用各種型態的雲端服務，本文將於第三節探討雲端使用者在選擇是否將資料上傳到雲端時的主要疑慮。

第二目 雲端運算服務之限制

雲端運算科技的應用的確對公、私部門的組織帶來許多利益，然而因為雲端產業的特性，可能也會造成不同於一般產業的挑戰和疑慮，本節將針對使用雲端運算科技所會面臨的問題進行說明，以分析雲端運算使用者在選擇是否接

https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.; Darrell M. West, *Saving Money Through Cloud Computing*, at 5-10, Apr. 7, 2010, https://www.brookings.edu/wp-content/uploads/2016/06/0407_cloud_computing_west.pdf. 美國智庫布魯金斯研究院（Brookings Institution） 於 2010 年針對此議題進行研究，該研究係以美國部分政府單位為基礎，評估這些單位將部分應用程式轉移到雲端與遠端的伺服器後，是否得以減少成本的支出。這項研究最後作出的結論指出在這些美國聯邦與州政府單位將部分敏感性較低的資料移轉到雲端後，平均減少了約 25%至 50%的成本。,

[33] Deloitte, *supra* note 21.

[34] *Id*. 根據估計，在 2008 年到 2020 年間，雲端運算服務總共可以為歐盟各會員國帶來 160 萬的工作機會，同時也預期會有 30,3000 家新的公司企業成立，特別是中小企業。

[35] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final (Sept. 27, 2012).

[36] Deloitte, *supra* note 21. 根據估計，在 2020 年，歐盟境內雲端使用者平均使用雲端運算服務的支出為 350 億歐元，但其可得之平均年淨利高達 1080 億歐元。歐盟境內服務提供者所得之平均年淨利則是 28 億歐元。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

受服務提供者之服務時的主要顧慮。

1. 雲端使用者失去對資訊科技的控制（Loss of IT-control）

雲端使用者把 IT 基礎設備和服務移到雲端伺服器，會喪失一定程度對於資訊科技的控制權。服務提供者對於軟、硬體和基礎設備的更新（update）和發表（release）會有技術上的控制權，舉例而言，服務提供者可以決定使用者使用其軟體和應用程式的方式。甚至在資料上傳到雲端後，雲端使用者與資料的當事人將無法辨認個人資料的具體位置。為了讓使用者願意使用經由雲端所提供的服務，服務提供者必須要建立和使用者之間的信任[37]。

2. 安全（Security）及風險管理（Risk management）

電腦安全議題的討論主要和避免資料在未授權的情況下被使用或擷取相關。電腦安全並非全新的議題，只是在雲端運算科技出現後，許多使用者會將資料大量的上傳到遠端的伺服器，將資料上傳到雲端的公司或個人將喪失對於該些資料的直接控制，只能依賴第三方代理以確保這些資料的安全，因此通常對於資料的安全有所疑慮[38]。但 Gartner 的報告指出，根據統計，實際上雲端服務提供者目前遭遇電腦安全受到侵害的問題比例非常小，多數的安全問題還是發生在企業自己部屬的資料儲存空間（on-premise）[39]。另一方面，許多中小型企業並沒有資源或是專家可以提供高程度安全保護，但是雲端服務提供者有更多資本和能力去招募相關專家，以部屬更高端的安全防護措施，避免資料的安全受到危害[40]。

[37] OECD, *supra* note 6, at 18.
[38] Ron Davies, *Cloud Computing : An Overview of economic and policy issues*, at 15, May 2016, http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf.
[39] *Id.* at 14.
[40] *Id.*近期「雲端安全聯盟（Cloud Security Alliance, CSA）」的調查也顯示，69%的 IT 管理者與相關人員認為雲端服務反而對於資料來說更為安全。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

3. 供應商鎖定（Vendor Lock-in）

供應商鎖定被認為是雲端運算產業中使用者是否願意採納雲端運算的重要指標。雲端運算產業供應商鎖定的情況主要指的是使用者依賴單一雲端服務提供者所提供的科技和服務，且在改變服務的提供者時，會面臨大量的成本支出、法規限制或者是技術上不相容（Technical Incompatibilities）的問題[41]。此問題的產生源自於現況下，個別雲端服務提供者（供應商）之間提供服務所使用的科技或軟硬體並不相容（non-compatible），且標準不一致─即具有專屬性（proprietary）[42]。實際上，雲端服務提供者通常提供使用者獨有的解決方式，以及具有專屬性的應用程式介面，甚至是資料格式，讓使用者以這些方式和介面取得服務和資源。這個現象會讓雲端使用者在更換服務提供者時面臨要轉換不同應用程式、科技和使用介面的困境，成本也因而增加，因此消費者通常會固定依賴單一或特定的雲端服務提供者。而供應商鎖定的問題也擴及到不同雲端空間之間的互通性（interoperability）以及資料的可攜帶性（portability）[43]。目前這個問題尚未解決的主要原因是因為國際之間還缺乏適當的標準化格式（standardized format），以確保雲端空間之間的互通性和資料的可攜帶性。供應商鎖定會使得原本雲端服務可以為使用者帶來的優勢減少，使用者不能依照對其自身最有利的成本和資源分配方式去選擇適當的服務提供者，甚至有些使用者會基於商業考量或是安全、機密等因素，希望將部分特定資料留存在公司內部的儲存空間，但在資料的格式、介面上缺乏統一標準可能會進一步減少使用者接受雲端服務的意願[44]。最後，這個現象也會影響在市場中服務提供者之間的競爭關係，一旦消費者無法自由更換服務提供者，初始的雲端服務提供者就

[41] Justice Opara-Martins, Reza Sahandi & Feng Tian, *Critical Analysis of Vendor Lock-in and Its Impact on Cloud Computing Migration: A Business Perspective*, JOURNAL OF CLOUD COMPUTING ADVANCES, SYSTEMS AND APPLICATIONS, 1 (Apr. 15, 2016).
[42] *Id.*
[43] 資料的可攜帶性（portability）意指消費者可以在不同的雲端之間移轉資料。
[44] Justice Opara-Martins, *supra* note 41, at 2.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

享有優勢地位，反而不利於整個產業發展[45]。目前各國政府甚至是國際組織皆積極合作，希望可以訂定技術上的統一標準，以避免供應商鎖定所帶來的負面影響。例如：歐盟執委會和「歐洲電信標準學會（European Telecommunications Standards Institute, ETSI）」在 2012 年一同發布了一項「雲端標準化調和倡議（Cloud Standardization Coordination initiative, CSC）」，以建立雲端技術的標準化方法，並促進安全、互通性資料可攜帶性標準化等目標[46]。

4. 雲端契約條款（Terms and Conditions）訂定

雲端使用者在使用雲端服務時，為了確保服務品質，並約定雙方的權利義務事項，會簽訂正式的「雲端服務合約（Cloud Service Agreements, CSAs）」以及「服務水準契約（Service Level Agreement, SLA）」。SLA 的內容包含服務品質的定義、權利義務的歸屬、服務水準目標 （Service Level Objective，SLO）以及雙方的預期和責任定義[47]。SLA 主要是用來保障使用者使用服務後的權利，也做為服務提供者服務收費的依據。但目前的契約並非以雲端使用者為中心，許多服務提供者並未在其標準化契約中承諾在服務不符合標準時，服務提供者有義務採取何種特定措施，以及使用者有何救濟方式，甚至僅願意提供非常微薄的補償[48]。尤其是現在雲端運算產業服務的提供者規模都較使用者大（例如：Amazon、Google 等），其在訂定契約時決定內容的權力較大。目前國際上已經有很多組織和政府就契約條款的標準化，以及對使用者的保護進行討論，並希望可以訂立相同的標準[49]。

---

45 *Id.*

46 European Telecommunications Standards Institute, *Cloud Standards in the Digital Single Market*, CLOUD STANDARD COORDINATION, (Jan. 28, 2016) http://csc.etsi.org/.

47 Cloud Standards Customer Council, *Public Cloud Service Agreements: What to Expect and What to Negotiate Version 2.0.1.*, at 4, Aug. 2016, http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf.

48 *Id*. at 5.

49 Ron Davies, *supra* note 38, at 16.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

5. 個人資料隱私保障（Privacy Protection）

觀察雲端運算產業的服務特性和提供服務的模式，雲端運算服務是透過分散及去中心化的電腦網路完成，而這些電腦的所在地，與使用者的終端設備的所在地通常也不會為在同一國家境內，因此，資料的跨境傳輸即為雲端運算產業存在的重要核心[50]。OECD 在 2013 年所修正的「隱私保護及個人資料之國傳輸指導指引（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）」也指出，隨著資料處理科技的進步，資料處理者可以在短時間內大規模的將個人資料進行跨境傳輸，因此必須要考量對於個人資料的隱私保護[51]。另外，一個雲端運算服務通常會涉及多個服務供者所提供之服務來完成，中間涉及的隱私問題更為複雜[52]。

第三節 歐美跨境資料傳輸與個人資料保護之衝突

目前全球的雲端市場中，無論 Saas、Iaas 或 Paas 的服務型態，主要的服務提供者皆為美國公司。對於這些大型雲端服務提供者，歐盟整體而言為其最大且最有潛力的海外市場。但歐盟境內的雲端服務使用者（無論是個人、企業抑或是政府組織）在選擇是否採用美國業者所提供的雲端運算服務時，會衡量雲端運算服務所帶來的利益與可造成的風險。對於使用雲端運算服務的企業而言，使用雲端服務固然可減少大量 IT 成本，並提供企業更多投入科技創新或新的業務以提升企業整體表現的機會，然而雲端運算產業的特性在於利用遠端的處理設備與技術匯集大量資料，依照個別使用者的需求動態分配資料處理的資源，以增加處理效率。因此想要透過雲端科技更有效率的完成個人資料的處理

[50] Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593 (2010).
[51] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (last visited: June 1, 2018).
[52] 有時候更會有基礎設施、平台提供和應用程式分別由不同服務提供者提供的狀況。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

必然涉及資料在使用者與雲端服務提供者之間的傳輸，而此傳輸的過程引發對於個人資料隱私保護的疑慮。而且在現在的雲端產業中，如果由美國雲端業者提供資料伺服器和處理服務，個人資料必然要進行跨大西洋的傳輸，此現象也引起歐美之間資料保護法要求保護程度不同的疑慮。尤其是一直以來歐盟被認為對於隱私重視的程度較其他國家高，為了使用美國雲端業者所提供的遠端雲端服務，隱私保護成為最主要的法律障礙[53]。另外，不同於傳統資料的保護問題，儲存在雲端的個人資料的法律權利歸屬也引發疑慮。哪些組織及個人有權利及在何種情況之下得取得與使用該些資料，這個議題也涵蓋政府基於國家安全和法律執行的目的取得資料的爭議，而且儲存在位在美國伺服器內的資料，其資料隱私的保護是否要適用歐盟的法律亦具爭議[54]。此外如上所述，通常為了完成更有效率的資料處理服務，雲端業者可能會將一項雲端的資料處理切割成不同部份分別外包給不同的雲端服務提供者。以最簡單的情況為例，一個APP 開發的新創公司（SaaS）可能僅提供雲端的軟體服務，其所使用的平台（PaaS）和平台（IaaS）還是由其他雲端業者提供。基於這些特性雲端運算服務對於隱私保護造成的威脅被廣泛認為是最複雜的問題。歐盟和美國採用完全不同的方法對個人資料進行保護，讓在美國業者進入歐盟市場時的隱私保護衝突和疑慮最為嚴重，如果美國的雲端運算服務提供業者想要將其在歐洲蒐集到的資料傳送到美國，除非美國可以提供和歐盟法律相同程度的保護，否則將會被禁止進行跨境傳輸行為[55]。因為不能達到歐盟對於資料保護要求而導致「禁止資料傳輸」的後果，可能直接影響雲端運算服務存在的可能性。以歐盟境內使用者的角度觀之，美國公司如果不能確定可以符合歐盟對於隱私保護的要求，即使該服務對其有成本減少、刺激創新等正面效益，這些雲端運算服務都是不可得的。本文認為美國雲端服務提供業者所需承擔的法律成本為歐盟境內

[53] OECD, *supra* note 6, at 19.
[54] *Id.*
[55] Konstantinos K. Stylianou, *supra* note 50, at 597.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

使用者是否採用雲端運算服務的決定性因素。第三章將分析美國和歐盟對於個人資料隱私保護規範的具體落差，並說明法規落差對於業者而言的問題為何，以及雲端運算業者是否因其產業特性而遭遇更多挑戰。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第三章 歐美資料保護規範之比較分析

雲端運算服務要順利進行，資料的跨境傳輸為重要關鍵，而資料的跨境傳輸則會因為各國隱私保護規範的不一致形成傳輸上的障礙。雖然國際上曾經想要發展共同的資料保護和隱私規範，但並未有具體成果，故目前關於跨境資料傳輸以及隱私保護的規範仍由各國政府各自決定，也因此產生許多規範方法和法規要求程度上的落差[56]。特別是歐美之間的法規落差更是明顯，此法規落差不僅體現在法規訂定的方式、適用範圍、要求的實體權利義務和法律執行上，甚至法規訂定的目的本身就有根本上的差異。而這些差異都會造成美國雲端業者在提供服務時的巨大阻礙，甚至影響雲端產業透過大量蒐集資料，並於遠端處理的服務提供模式。一旦資料被禁止進行跨境傳輸，則雲端科技所帶來的效率將難以被達成。不僅如此，雲端運算服務為近年興起的產業，歐盟在訂定最初的保護規範時並未考量到此種資料密集產業的快速發展，故法規的訂定也未考量到雲端運算服務的產業特性，因此反而讓雲端服務提供者在適用指令時面臨到挑戰[57]。為了確保對個人資料的高度保護，執委會於 2012 年提出「一般資料保護規則（General Data Protection Regulation, GDPR）[58]」，以彌補 1995 年「涉及個人資料處理予自由流動之個人保護指令（Directive 95/46/EC），以下簡稱 DPD」的不足[59]。該規範提高對個人資料隱私的保護水準，使得歐美之間資

[56] CHRISTOPHER KUNER, INTERNATIONAL REGULATION OF TRANSBORDER DATA FLOWS 26 (2016). 如：第 25 屆「個人資料保護與隱私專員國際論壇（ International Conference of Data Protection and Privacy Commissioners）」發表了「蒙特勒宣言（Montreux Declaration）」呼籲聯合國可以建立具有拘束力的規範，清楚地建立有關資料保護和隱私的規範細節。

[57] 歐盟境內發展雲端運算產業遇到的困難之一，即是各會員國之間在落實指令時法規仍有落差，使得資料的跨境傳輸遇到阻礙，這也是歐盟改革保護規範的原因之一，希望透過「規則」的訂定達成會員國間法規的一致性。

[58] 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. 44, 2016 O.J. (L 119) 1, 60; 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. 45, 2016 O.J. (L 119) 1, 61 [hereinafter GDPR].

[59] 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, 1995 O.J. (L281/31); Paul M. Schwartz, *European Data Protection Law and Restrictions on*

DOI:10.6814/THE.NCCU.IB.015.2018.F06

料保護規範之落差更大。本章將以分析歐盟與美國之間隱私保護規範的具體差異為核心，分別說明歐盟和美國在規範的目的與宗旨、規範手段、適用範圍、實體權利義務和法律的執行層面上有何規範上的落差，藉以了解美國雲端服務提供者在進入歐盟市場時會遇到什麼樣隱私法規上的挑戰。

第一節 歐盟與美國資料保護法律規範體系之比較分析

歐盟和美國長期以來對於個人隱私權和資料保護的觀點與立場不同，態度的歧異也體現在歐美的資料保護規範的各個面向，本節將先詳述歐盟 1995 年資料保護指令、美國資料保護規範具體內容差異，藉以作為後續討論的立論基礎。

第一目 保護目的與宗旨

一直以來，各方都認為歐盟對於隱私的保護水準較美國高，而其實不僅是對權利的保護水準有所差異，雙方之間對於「隱私權」的看法亦有根本性的差異，下述將說明歐盟和美國個別對於隱私權的看法。

1. 歐盟──保護公民一般基本人權

歐洲國家長久以來都十分重視個人隱私的保護，在 1981 年，由歐洲國家成立的「歐洲理事會（Council of Europe）」通過了第一個也是當時唯一一個具有拘束力的資料保護國際協定─「歐洲理事會關於資料保護的第 108 號公約（Council of Europe Convention 108）」[60]。該公約的內容是要求各會員國在其國家法律內納入對資料保護的規範[61]。如公約第 5 條第 1 項規定資料保護法的基

International Data Flows, 80 IOWA LAW REVIEW, 471 (1995).

[60] Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data, Council of Europe, Jan. 28, 1981, ETS 108 (1981).

[61] *Id.* art. 3.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

本原則，要求自動處理（automatic process）的個人資料應該以公平且合法的方式取得和處理[62]。公約主要約束的對象是歐盟會員國，因此並未直接為個人創設權利，也未適用於任何私部門的實體[63]。但即便如此，此公約仍被視為歐洲各國將資料隱私作為基本權利的重要發展歷程[64]。

在歐盟，隱私被視為是個人的「基本權利（fundamental right）」，因此保護個人資料的隱私也被視為是保護歐盟公民的基本權利。這個概念體現在歐盟不同的法律條文中，例如「歐洲聯盟基本權利憲章（Charter of Fundamental Rights of the European Union）」第 8 條明文將個人資料的保護認定為個人的基本權利：人人均有權享有個人資訊之保護；此等資訊應僅得於特定明確的目的，於資訊所有人同意或其他法律規定的正當依據下，公平地被處理；人人均有權了解其個人資訊，並有權要求銷毀其個人資訊；應由獨立之主管機關監督這些原則被確實遵守[65]。同樣地，「歐盟基本權利憲章（ EU Charter of Fundamental Rights）」第 16 條第 1 項也指出：人人均有權保護與其相關的個人資料[66]。由此可知，個人資料隱私的保護被視為最根本的權利，而保護公民的基本權利係歐盟法律的一般原則，其他所有規範都必須遵守此原則，若有違反則必須負擔損害賠償責任[67]。

基於此一觀點，歐盟執委會於 1995 通過最具影響力的資料保護指令。歐盟執委會從 1973 年開始針對跨境資料流通進行研究，研究結果顯示歐洲共同體會員國之間對於資料保護的程度不同，會影響會員國之間跨境資料的自由流通，因此執委會認為有必要統合各國的標準，不僅得以促進區域內資料自由流通的

62 *Id.*art. 5.
63 Council of Europe Convention 108, Explanatory Report, para. 38.
64 Christopher Kuner, *supra* note 56, at 37.
65 Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364/1) [hereinafter Charter].
66 Consolidated version of the Treaty on the Functioning of the European Union art. 16(1), May 9, 2008, 2008 O.J. (C 115), providing that: ‘‘Everyone has the right to the protection of personal data concerning them’’ [hereinafter TFEU].
67 Christopher Kuner, *supra* note 56, at 62.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

程度，亦可確保對歐體公民一致的隱私保護水準[68]。根據 1995 年指令第 1 條第 1 項，會員國應保護自然人的基本權利和自由，尤其是和個人資料處理有關的隱私權（right to privacy）[69]。除此之外，1995 年指令第 5 條要求各會員國應該要進一步精確地定義在何種情況之下，可以合法處理個人資料[70]。任何實體要將歐盟公民的個人資料傳出歐盟境外時，也必須要確定該資料接受國對於資料保護的水準係為「充足（adequate）」[71]。藉由這些條文的觀察可得知，歐盟對於歐盟公民的個人資料保護的核心原則是「只有在確定合法、擁有正當的法律基礎的情況下才得以進行資料的處理」，意即原則上禁止，除非在會員國境內（因適用歐盟指令的規範）或在有充足保護的國家才得進行。可見在歐盟，「隱私權」為個人核心且不可被侵犯的重要權利。

2. 美國──保護消費者權益

美國對於隱私保護的意涵與目的與歐盟不同。在美國，隱私保護主要是透過各州的法律，與針對特定部門的聯邦法律來規範以保護消費者的權益，而美國憲法中關於資料隱私的保護，僅限於防止政府對於人民隱私的侵害[72]。不同於歐盟訂立一套涵蓋所有資料類型一體適用的保護指令，美國僅針對特定的資料類型，與特定的資料處理活動訂定特別的規範[73]。整體而言，美國隱私保護體系的法律可以分為 3 種，第一、用來保護較為敏感或風險較高之資料，以資料的類型作為規範的基礎，例如聯邦針對金融、保險機構資料的保護規範─「金融服務業現代化法案（Financial Services Modernization Act of 1999），亦稱

[68] Christopher Kuner, *supra* note 56, at 40.
[69] Directive 95/46/EC art. 1(1), providing that: 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.
[70] Directive 95/46/EC art. 5.
[71] Directive 95/46/EC art. 25.
[72] PAUL M. SCHWARTZ AND DANIEL SOLOVE, PRIVACY LAW FUNDAMENTALS 2-7 (2011).
[73] THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 365 (Alan Charles Raul et al. 4th ed. 2017).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

（Gramm-Leach-Bliley Act, GLBA）」[74]、針對孩童和學生資料的保護規範─「兒童網路隱私保護法（Children's Online Privacy Protection Act of. 1998, COPPA）」[75]。第二、用來規範特定行為，以確保個人資料隱私不因這些行為而受到侵害，以特定行為為基礎─例如「1974 聯邦隱私法（the Federal Privacy Act of 1974）」用以規範聯邦政府機構如何蒐集和使用個人紀錄，避免政府以不正當的手段侵犯人民隱私[76]。加州則要求如果個人的資料被洩漏，或隱私被侵犯，則企業有義務進行通知[77]。最後則是用於確保消費者資料與權益的保護，若是不屬於聯邦或州政府特別法規所涵蓋的資料，則適用美國一般的消費者保護法─「聯邦貿易委員會法（Federal Trade Commission Act, FTC Act）」，此法禁止企業不公平或是詐欺的商業行為（unfair and deceptive acts and practices）[78]。

由上述可知，美國沒有一部規範個人資料蒐集和使用的一般資料保護法律，原則上並不禁止企業進行個人資料的處理，除非是特別規範的資料類型與處理行為。在確保符合對於消費者基本權益的保護，並且不構成不公平與詐欺的商業行為即可[79]。針對跨境資料的傳輸亦同，美國同樣沒有關於跨國資料傳輸的法律限制[80]。基於這些觀察可以得知，美國與歐盟的規範邏輯不同，歐盟規定資料只有在有正當法律基礎時才得以進行處理和傳輸，而美國則是基本上允許處理和傳輸資料，僅有在特定情況下有所限制。

第二目 規範手段

歐盟採用的是綜合性立法的方式（omnibus approach）訂定資料保護指令，

[74] The Financial Services Modernization Act of 1999
[75] Alan Charles Raul et al., *supra* note 73. 聯邦的資料保護規範主要是針對敏感性的資料：個人健康資料、信用報告、從網路上蒐集之 13 歲以下孩童的個人資料、精確的地點資料和可以用來辨認偷竊和詐欺身分的資料。因規範數量龐大且類別繁雜，無法一一羅列。
[76] Jay P. Kesan, *supra* note 8, at 398.
[77] California Civil Code §1798.82.
[78] 15 U.S.C. §§41-58
[79] Alan Charles Raul et al., *supra* note 73, 377.
[80] *Id*.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

該指令所涵蓋的範圍不僅涵蓋歐盟境內所有公民的個人資料，甚至擴及 3 個「歐洲經濟區（ European Economic Area, EEA）」的國家──冰島、挪威和列支敦斯登[81]。在其規範的領域範圍內，會員國必須要訂定國內法以符合指令上的要求，保護所有類型之 EEA 公民的個人資料。因此所有個人資料，無論敏感與否都受到相同的保護水準，也因此在 EEA 境內個人資料得以自由流通[82]。

美國則是由聯邦與州政府個別針對不同部門訂定特定規範的方式進行資料的隱私保護立法（sector by sector approach），甚至對於公部門和私部門的規範也有所差異[83]。如同上述，美國資料保護法主要分為 3 種─針對敏感資料的隱私要求、針對特定資料處理行為的要求，以及消費者資料的保護規則。基於這三項目的，聯邦和州政府訂定一系列不同的規範以確保目的的達成，故美國的資料保護方法又被認為是「拼湊物（patchwork）」。除此之外，美國在個人資料隱私保護上有許多企業自願遵守的自願性規範（self-regulation），然而因為該些規範為自願性，與歐盟的強制一體適用的規範仍有極大落差[84]。

第三目 適用範圍

歐盟 DPD 的適用範圍廣，包含全部或部分透過自動化方式（automatic means）處理；以及以自動化方法以外的其他方式處理並成為檔案系統（filing system）一部分的個人資料[85]。換句話說，不管個人資料處理的方式是電腦自動處理，或是持有資料者所為，只要最後歸檔的個人資料，無論種類都涵蓋在指令規範的範圍內。但根據指令第 3 條第 2 項也有明文規定，在下列的情況下，

---

81 *Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement*, 2000 O.J. (L296/41).
82 Directive 95/46/EC art. 1.
83 Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, BERKELEY LAW 1974 (May 2013).
84 Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 Mich. St. Int'l L. Rev. 1095 (2013).
85 Directive 95/46/EC art. 3(1).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

DPD 並不適用於個人資料的處理：不屬於歐洲共同體法所規範的活動，例如歐洲聯盟條約（Treaty on European Union）第五、六章中會員國「共同外交及安全政策」與「司法及內政合作」所涉及的個人資料處理[86]；和公共利益、國防、國家安全有關，以及會員國內刑法所規定的活動[87]。整體而言，歐盟隱私指令所涵蓋的內容係除了明文規定的例外，包含所有實體以各種方法蒐集之所有類型的個人資料。

美國的個人資料保護相關法律所涵蓋的範圍較小，且因為美國法不如歐盟的指令，係以單一規範一體適用，不同的法律所規範的範圍亦不相同，甚至不同規範因為目的不同，用以定義涵蓋範圍的標準也不相同。例如美國 GLB 法案規範的即是參與金融活動的金融機構，如銀行、證券公司和保險公司，如果非金融機構的公司從金融機構取得非公開的個人資料，亦須受到 GLB 法案的管轄[88]。另外，除了以持有資料的公司（data holder）作為劃定規範範圍的基礎外，資料的性質亦是標準之一，例如：HIPAA 適用於該法涵蓋實體所持有之個人可辨識的健康和醫療資料[89]。由此可知，美國所規範的範圍並非「所有資料」，也並非所有「處理或傳送個人資料者」，必須要視個別法律的目的和適用範圍而定，廠商也依照其所蒐集的資料類別，與其本身的企業特性去符合不同的法律要求。此外，美國的各級法律中並未限制「自動化的資料處理」—直接由電腦進行的資料處理，也無相關要求。歐盟指令與美國法律體系在適用範圍上，最大的差異即是歐盟指令除了明文規定的特定例外，適用於「所有類型資料」、「所有類型資料持有者」，以及「各種資料蒐集方法」；但相反的美國整體而言沒有一般化的要求，但如果屬於特殊規範所涵蓋的資料類型或資料持有者，則需符合該規範的規定。

[86] 第五章及第六章規範共同外交及安全政策與司法及內政合作
[87] Directive 95/46/EC art. 3.(2)
[88] GLBA, *supra* note 7474.
[89] The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第四目 實體權利義務

歐盟和美國個人資料保護法中賦予資料主體的權利亦不相同。1970 年代國際上在發展「隱私權」以及「保護個人隱私」的概念時，美國與歐盟的政府與學者都認同應該要以「公平的資訊行為（Fair Information Practices, FIPs）」原則為中心，立法保護資料主體的隱私權。所謂的 FIP 原則是由美國當年的「衛生、教育及福利部（Department of Health, Education, and Welfare, HEW）」提出[90]。內容主要涵蓋 5 個原則：1. 不得有秘密對於個人資料紀錄留存的系統；2. 需提供個人得知個人資料被紀錄及該資料如何被使用的方法；3. 需提供防止個人資料在取得資料處理同意之前被用於和原本蒐集不同的目的的方法；4. 需提供個人更正或修改個人資料紀錄的方法；5. 產生、維持、使用或散播可辨識個人資料的組織，必須要擔保其欲使用之資料的可靠性，以及必須要採取必要措施以預防資料的誤用[91]。但雖然歐盟和美國的個人隱私法都是基於 FIP 原則進行延伸訂定，但賦予資料主體的權利與對資料控制者課予之義務卻仍有差異。

1. 資料主體的權利

歐盟 DPD 中，賦予資料主體的權利是以 5 項 FIP 原則為基礎訂定，主要可以歸類為 2 個面向：（1）透明化原則：資料主體必須被告知資料處理之目的，以及第三國資料持有人的身分、相關其他資訊以確保雙方的公平[92]。（2）個人資料之資料主體有權存取、修改以及要求禁用個人資料：資料主體有權取得關

[90] 美國當年的「衛生、教育及福利部（Department of Health, Education, and Welfare, HEW）」現改為「美國衛生與公眾服務部（US Department of Health and Human Services, HHS）」

[91] United States Department of Health, Education and Welfare Fair Information Practice Principles (1973) https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[92] Directive 95/46/EC art. 10. 資料控制者以必要提供資料主體下列之訊息，除非資料主體已經持有相關資訊：(a) 資料控制者，或其代表之身分；(b) 資料處理的目的；(c) 其他資訊，如：資料接受者或接受者的類別；資料主體對於資料有接近權和修改的權利等。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

於其個人資料之副本[93]，並得在該資料不精確時要求修正[94]。且在特定的情況下，可以限制資料處理活動，或甚至拒絕個人資料的相關處理[95]。

美國雖然也以 FIP 原則為訂定資料保護法之基礎，但不同的法律規範中仍存有差異，而且部分歐盟指令所賦予資料主體的權利，在美國的資料保護法中並不能找到相對應的保護規定。如：美國 FTC 法案和大多數美國的隱私法（如 HIPAA 和加州的法律）並未提供資料主體資料接近權，僅有針對部分特定資料有例外規定[96]。此外，目前美國聯邦的立法亦未授予資料主體要求刪除資料的權利，例如：在 HIPAA 中，資料主體可以提出修改不精確或不完整資訊的要求，但被要求的涵蓋實體並未有修正該資料的義務（資料持有者得拒絕該要求）[97]。由此可知，歐盟指令較美國整體的法律規範賦予資料主體更多直接且明確的權利。

2. 資料控制者與處理者之義務

首先，歐盟 DPD 在規範實質義務前，先對負擔義務的實體進行定義，其中「資料控制者（data controller）」指的是任何單獨或與他人共同決定個人資料處理目地與方法的自然人、法人、行政機關和其他機構[98]。另外，所謂「資料處理者（data processor）」指的則是為控制者處理資料的任何自然人、法人、行政機關和其他機構[99]。此定義將影響後續被課予義務之實體的範圍。相反的美國

[93] Directive 95/46/EC, art 12 (a). 資料主體有資料接近權，得確認與其相關的資料是否進行處理、處理的目的、資料的種類、資料的接受者（recipient）、接受者的類別；該資料被揭露的對象等。而資料主體所要求的資料，資料控制者必須以清楚容易理解的形式給予資料。
[94] Directive 95/46/EC, art 12(b). 資料主體在資料控制者處理資料的目地和條件與指令不符，尤其是資料不完整或不正確時，有權要求修正（ratification）、刪除（erase）及阻絕（block）。
[95] Directive 95/46/EC art. 14. 資料主體得於任何期間得根據重大合法的理由，反對資料控制者處理其資料的權利。當資料主體提出之理由正當，資料控制者不得在其處理的過程中涉及該資料。
[96] 例如：孩童的隱私保護法同意父母可以瀏覽其孩童在網路被蒐集的資料，並且可以刪除和更正資料。
[97] HIPAA, *supra* note 89, § 164.526.
[98] Directive 95/46/EC art. 2(d).
[99] Directive 95/46/EC art. 2(e).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

的法律體系中沒有明顯對「資料控制者」和「資料處理者」加以區分。歐盟 DPD 要求資料控制者或其代表在進行個人資料處理時必須符合幾項義務：

（1） 確保資料品質和相稱性：資料控制者或其代表必須確保資料的處理公平且合法，以及資料的內容為精確，如果有必要應隨時更新，資料也必須要與其傳輸或處理之目的有充分關聯[100]。

（2） 確保個人資料的安全和保密：個人資料控制者在持有資料的期間必須要採用適當的系統性及技術性安全措施，以保護個人資料在處理過程中可能造成的風險。任何資料控制者授權之使用，包含執行處理者個人資料者，在沒有控制者提供的指導時，不得處理資料[101]。同時，在必要時也要對個人資料進行保密[102]。

（3） 通知義務：除了特定的例外，處理個人資料必須要通知主管機關，如果是自動化處理，則控制者需要將處理的邏輯進行通知[103]。

（4） 確保後續傳輸接受者保護程度：個人資料之原始接受者只得在該資料後續傳輸接受者亦處於具有充足保護水準規範的情況下，才得將資料進行傳輸。除了這些特定的義務外，因為歐盟指令的規範原則是只有在有正當且合法基礎時，才得以進行個人資料處理，因此整體而言，資料控制者還負有確保其資料處理係基於正當合法基礎的義務[104]。

美國整體而言，對於資料控制者（或持有者）的義務著重在當資料主體的個人資料受到侵害，其有義務要進行通知[105]。美國 FTC 法案第 5 條則是要求企業必須要遵守其所公布的隱私政策，該法案的目的在於禁止企業進行「不公平

[100] Directive 95/46/EC art. 6.
[101] Directive 95/46/EC art. 17. 資料控制者和其所揭露的第三方，有義務要採取安全措施避免個人資料被不合法的處理、遺失或是未經授權的被揭露和使用。
[102] Directive 95/46/EC art. 16.
[103] Directive 95/46/EC art. 18.
[104] Directive 95/46/EC art. 7.合法資料處理的標準包含：資料主體的同意、契約、契約、遵守法律義務之必要、保護資料主體的重要利益之必要、維護公共利益為必要、資料控制者或第三方尋求正當利益之必要。
[105] Paul M. Schwartz, *supra* note 83, at 1976.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

或詐欺」的商業行為以損害消費者權益，因此雖然 FTC 法案中並未明文要求企業必須要訂定隱私政策，但一旦公布了就必須要遵守[106]。此外，美國大多數的法律也都有要求資料控制者要採用安全措施，保護個人資料，但是因為美國的個人資料保護法並不適用於所有資料，因此僅限個別法律所涵蓋的範圍。美國在義務方面，最主要是以「受損害的實體」為基礎，確定其損害得以或得救濟和補償，許多歐盟 DPD 所要求之義務並未出現在美國的個人資料保護法中。

由上述的討論可以了解，就實質的規範義務上，歐盟和美國雖然都係以 FIP 原則為基礎，但歐盟相較於美國的權利義務都較為明確及完整。甚至有許多權利義務是不存在於美國的法律體系內，因此可見歐盟 DPD 的規範較美國而言保護水準較高。

第五目 法律的執行──主管機關

歐盟 DPD 中，要求各會員國指定一個或多個主管機關，專門負責與個人資料隱私與保護的相關事務，並監督和執行其領域內為符合指令而訂定的國內法[107]。同時，指令中更成立關於個人資料處理之個人權益保障工作小組─即所謂「第 29 條資料保護工作小組（Article 29 Data Protection Working Party, WP29）」，此工作小組由各會員國境內之主管機關組成，負責審視會員國執行隱私指令的成效，以及向執委會遞交第三國個人資料保護的情況，也會對指令執行的情況提出意見[108]。

相對於歐盟的規範，美國的法規則並未指定一個獨立的資料保護主管機關對個人資料的隱私和保護進行監督[109]。通常是由「聯邦貿易委員會（Federal Trade Commission, FTC）」負責，FTC 於 1914 年成立，主要負責消費者保護和

[106] Federal Trade Commission Act Section 5
[107] Directive 95/46/EC art.28.
[108] Directive 95/46/EC art.29.
[109] Paul M. Schwartz, *supra* note 83, at 1977.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

建立公平商業行為，目前美國境內的隱私相關事件由其處理[110]。從 1996 年以來，FTC 已經處理超過 300 項與隱私相關的規範執行[111]。作為資料隱私的保護者與管制者，FTC 可以處理的活動範圍有限，FTC 並未有所有企業的管轄權，且其主要著重的議題為「通知與消費者的選擇」，並不涵蓋所有美國法律下關於 FIP 的執行範圍。故兩相比較之下，可以得知在隱私法的執法機關上，兩個法律體系有所差異，歐盟境內存有一全歐盟的工作小組，各會員國亦指定特定機關作為主管機關，專責隱私保護事務，而美國則是以消費者保護為出發點，主要由 FTC 負責。

第二節 資料保護規範（GDPR）體系介紹

2012 年歐盟執委會宣布要重新審視歐盟境內之資料保護法案，並提出全新的資料保護規則（GDPR），以確保得以在充分保護個人資料隱私的情況下促進資料的自由流通，GDPR 於 2016 年通過，並於 2018 年 5 月 25 日生效[112]。此規則為歐盟促進單一數位市場策略的一部份[113]，旨在使歐盟法規更符合現代數位時代的需求，並且調和各會員國之國內法規，避免法規落差造成的爭議與對雲端產業發展的阻礙[114]。本節將簡述 GDPR 規範與 1995 年指令的差異，以了解在新規範下雲端服務業者可能需要負擔哪些義務。

第一目 擴大適用範圍

GDPR 規範所適用的資料處理行為與 1995 年指令相同，不論是電腦自動處

110 *Id*.
111 *Id*.
112 *GDPR Portal: Site Overview*, EU GDPR INFORMATION PORTAL, https://www.eugdpr.org/ (last visited June. 1, 2018)
113 「單一數位市場策略（Digital Single Market）」由歐盟執委會於 2015 年提出，旨在促進歐盟會員國間數位市場的整合與法規環境的調和。改善個人資料與隱私保護規範亦於 2015 年納入該策略。European Commission, *Right environment for digital networks and services*, May 16, 2017, https://ec.europa.eu/digital-single-market/en/environment-digital-single-market.
114 European Commission, *Reform of EU data protection rules*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

理，或是持有資料者所為，只要最後歸檔的個人資料，無論種類都涵蓋在指令規範的範圍內[115]。然而 GDPR 擴大領域適用的範圍（territorial scope），先前根據指令，領域的適用範圍主要是以資料控制者的「設立處（establishment）」為標準[116]，但 GDPR 將規範適用的範圍擴大到所有處理位於歐盟境內資料主體個人資料的公司，不論公司的位置以及其設立的地點[117]。根據 GDPR 第 3 條的規範，下列情況的資料控制者或處理者屬於規則的適用範圍：歐盟境內的控制者與處理者，不論該資料處理的行為是否發生於歐盟境內[118]；資料控制者與處理者設立於歐盟境外，但處理位在歐盟境內資料主體之個人資料，而這些處理活動和提供貨品和服務給歐盟公民相關，或者是對其與監督歐盟境內公民之行為相關[119]。

由此可知，GDPR 的適用範圍較指令大，適用於指令的企業必然與歐盟有一定程度的連結，特別是以設立點為基準，然而 GDPR 係要求所有處理歐盟境內公民資料的企業，無論其與歐盟是否有一定程度的連結，都必須要符合對於個人資料隱私的規範。這對於原本非指令適用範圍的企業而言將形成額外的法規遵循成本。

第二目 增加資料主體之實體權利

GDPR 中不僅加強現有指令中資料主體的權利，同時也賦予資料主體新的權利，以確保在現今數位科技的發展下，資料主體的個人資料隱私得以受到完善的保護。首先，GDPR 擴大原本透明化原則下資料主體應被告知的資訊內容，包含：其個人資料將被儲存的時間[120]；資料主體得以要求刪除、修正、限

115 GDPR art. 2.1
116 Directive 95/46/EC art. 4.
117 *GDPR Key Changes*, EU GDPR INFORMATION PORTAL, https://www.eugdpr.org/key-changes.html (last visited June. 1, 2018).
118 GDPR art. 3.1.
119 GDPR art. 3.2.
120 GDPR art. 15.1(d).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

制處理範圍的權利[121]；資料主體得以向 DPA 提起控訴的權利等[122]，藉以加強資料主體對其個人資料的控制。

另外，GDPR 擴大資料主體要求刪除、限制和拒絕資料處理的權利。就刪除權（Right to erasure）的部分，GDPR 進一步將歐盟境內討論已久的「被遺忘權（Right to be forgotten）」納入條文之中，被遺忘權的主要內涵係資料主體在條文規範的情況下，得以要求資料控制者刪除其個人資料，不得有不合理的延遲[123]。且如果資料控制者已經公開資料主體之個人資料，在考慮技術和成本後，必須要採取合理的程序通知進行資料處理的第三方資料主體要求刪除任何個人資料的連結（links）、複本（copy）或是再製（replication）[124]。此條文不僅加強資料主體的權利，同時提高對資料控制者的義務，要求其不但要告知第三方資料當事人對於刪除個人資料的要求，同時亦須確保該項個人資料被刪除，另外也要告知資料當事人第三方採取了哪些相關的措施[125]。而就限制或拒絕資料處理的部分，GDPR 條文中更明確的在規範中說明特定情況下，資料主體有「限制資料處理的權利（ Right to restrict processing）」，包含：對資料的精確度有質疑時[126]；資料的處理不合法[127]；或是對於原本蒐集資料的目的而言，資料處理已非必要等，在這些情況下，如果資料主體認為不需要要求資料控制者刪除資料，則可要求其限制處理範圍[128]。

121 GDPR art. 15.1(e).
122 GDPR art. 15.1(f).
123 GDPR art. 17.1. 條文中列出 6 種得要求其資料被刪除的情況：1. 其個人資料對蒐集或處理該資料的目的已非必要時；2. 當事人撤回下列情況下做出對資料處理的同意（consent）：資料控制者因為資料當事人的同意才得以合法處理資料，及當事人同意讓資料控制者處理原本依規範不得處理的「特殊類別個人資料」，如：透漏種族、政治傾向和宗教等資料；3.當事人基於個人情況，反對資料當事人繼續處理其個人資料，而資料控制者也未能提出超越資料當事人利益、權利或自由的正當理由時；4. 資料被以非法的方式處理；5. 為了符合規範資料控制者的歐盟或各國的法律，個人資料必須被刪除；6.與兒童有關的資料處理，同意資料處理的資料當事人應至少年滿 16 歲；若孩童未滿 16 歲則需取得其監護人同意才得合法處理其個人資料。
124 GDPR art. 17.2. 另外，17.3 條也規定被遺忘權的例外情況。
125 *Opinion of Advocate-General Jääskinen*, delivered on 25 June 2013, Case C-131/12, ¶¶ 51-65.
126 GDPR art. 18.1(a).
127 GDPR art. 18.1(b).
128 GDPR art. 18.1(c).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

除了擴大既有指令規範的權利外，GDPR 亦賦予資料主體新的權利。最主要的是新增資料可攜帶權（Right of data portability），根據規則，資料主體必須得以在不同的資料控制者之間轉移其個人資料，亦即可以沒有障礙的自由更換進行資料處理的控制者[129]。此權利隱含各資料控制者必須要確保資料的格式必須要得以互通（interoperability）[130]。

第三目 增加資料控制者與處理者之義務

在新的 GDPR 中，對於資料控制者與處理者的定義與指令相同，控制者得以決定資料處理的方式與目的，處理者則是為控制者進行資料處理，且其處理活動不得超過控制者的指示範圍[131]。在 DPD 中，僅對資料控制者規範直接的履行義務，處理者和次級處理者即使違反指令規定，仍由控制者負責，處理者和次級處理者的懲罰和義務則是由與控制者之間的契約決定。然而，新的 GDPR 規範，不僅加強對資料控制者的義務要求，同時亦對處理者與次級處理者課以直接的義務要求[132]。此一部分的改變，對於業者而言影響最大。下述將分別說明控制者與處理者於 GDPR 下的義務。

1. 資料控制者的義務

（1） 資料保護設計（Data protection by design and by default）：

資料控制者必須在提供所有服務或新產品時，於計畫階段和執行階段都將關於個人資料處理的資料保護和適當防衛措施納入考量[133]。同時也必須要遵守人資料蒐集最小化原則（data minimization），僅在絕對必要的範

[129] GDPR art. 20.
[130] Guidelines on the right to data portability, Dec.13, 2016, WP 242 rev., 16/EN, at 13.
[131] GDPR art. 2(d), 2(e).
[132] GDPR art. 3(1).
[133] GDPR art. 25.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

圍內進行資料處理[134]。此義務隱含資料保護的措施不應該是「額外」的措施，而是在 IT 系統建立時就應該將對資料的保護納入考量[135]。

（2） 共同資料控制者（Joint controllers）

在指令中並沒有關於「共同控制者」的直接規定，僅有認定可能會有多個實體共同決定資料處理之目的和方法的情況[136]。但在 GDPR 下，明確規範有共同控制者的情況，並要求共同控制的情況必須要以「約定（arrangement）」的方式分配資料保護的義務，約定的結果必須要告知資料主體[137]。此外，在指令中資料控制者僅需要對與其相關，或其所導致的傷害負責，如果資料控制者可以證明其與對資料主體的傷害無關，即可免責[138]。因此如果有多個實體共同控制資料處理的情況下，受損害的資料主體不一定可以得到完全的補償（full compensation）[139]。但 GDPR 修改相關規定，授權資料主體得以要求任一共同的資料控制者對資料處理造成的損害負全責，藉此取得完全的補償[140]。

（3） 指定歐盟境內代表：

指令中有要求在歐盟外設立的資料控制者必須要指派一境內代表[141]，GDPR 亦有相關規範，但進一步規範該代表必須對控制者不履行義務的行為負責（即各國的 DPA 可能針對境內代表執行相關懲罰措施）[142]。

134 GDPR art. 23.
135 *GDPR Key Changes*, EU GDPR INFORMATION PORTAL, https://www.eugdpr.org/key-changes.html (last visited June. 1, 2018).
136 Directive 95/46/EC art. 2(d).
137 GDPR art. 26.
138 Directive 95/46/EC art. 23(2).
139 Detlev Gabel &Tim Hickman, *Chapter 10: Obligations of controllers – Unlocking the EU General Data Protection Regulation*, WHITE& CASE (Sept. 13, 2017), https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection.
140 GDPR art. 26(3).
141 Directive 95/46/EC art. 4(2).
142 GDPR art. 27.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

（4） 指定資料處理者：

指令中要求資料控制者僅得指定符合指令規範的處理者為其進行資料處理，且處理活動只限在控制者的指令範圍內[143]。在 GDPR 中不僅有和指令相同的要求，甚至進一步要求資料控制者在選擇處理者時，只能從符合下列義務的處理者中選擇：必須要履行保密的義務；遵守和指定次級處理者有關的規則；採行相關措施協助控制者保護資料主體的權利；協助資料控制者在必要情況下取得 DPA 的許可；在與資料控制者的契約關係結束後必須退回或刪除個人資料；提供控制者所有證明其符合 GDPR 規範的必要資料[144]。新的規範中針對資料控制者和資料處理者之間簽訂的契約內容設立許多強制性的要求，使得原本不需要履行義務的資料處理者反而必須要遵循嚴格的契約義務，才能獲得與控制者簽約的機會。嚴格的要求可能會導致境外的處理者不願意採行相關措施，反而導致控制者在尋找處理者時更為困難[145]。

（5） 資料外洩的通知（Reporting data breaches）：

指令中對此沒有特定的要求，僅部分會員國的國內法有相關規定。但 GDPR 中則明確要求控制者原則上必須要在意識到資料外洩的 72 小時內通報 DPA，除非資料外洩的狀況不可能對資料主體造成任何傷害[146]。此外，如果資料外洩的結果對資料主體造成風險，資料控制者也必須要通知受影響的資料主體[147]。根據第三章美國與歐盟資料保護規範的比較中可得知，資料外洩的通知義務原本較受美國法律體系的關注，歐盟的指令中沒有特別的規範。但 GDPR 將此義務明文化後，也更進一步完善歐盟資料保護體

143 Directive 95/46/EC art. 17(2) &17(3).
144 GDPR art. 28.3
145 Detlev Gabel, supra note 139.
146 GDPR art. 33.
147 GDPR art. 34.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

系。

2. 資料處理者的義務

（1） 指定處理者：

如前面資料控制者的義務所述，資料控制者在選擇將部分處理工作外包給資料處理者時，必須要考量比指令規範更多的要件，而資料處理者要符合的規範也增加。此外，GDPR 並不包含任何過渡的條款，故既存的外包契約也可能需要重新協商以符合規範要求[148]。此外，如果資料處理者對於資料的處理超出原本控制者的指示，且自行決定資料處理的目的和方式，則其必須以資料控制者的身分被 GDPR 規範[149]。

（2） 指定次級處理者：

在原本指令的規範體系中，原則上次級處理者同樣只有在符合資料控制者的外包指示時，才得以進行資料處理。但原本的指令並沒有明文規範指定次級處理者需符合的要求[150]。然而，在 GDPR 中明確訂納入選擇次級處理者的規範。首先，在指定次級處理者前必須要先取得控制者的書面同意[151]；而次級處理者必須要確保對個人資料的處理符合資料控制者和處理者之間契約的內容[152]。GDPR 將原本歐盟體系在處理涉及外包服務給次級處理者的作法明文化，要求次級處理者必須要負擔和處理者相同的資料隱私保護義務，以避免在資料處理程序中因為涉及不同處理者而對資料主體

148 Detlev Gabel &Tim Hickman, *Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation*, WHITE& CASE (Jul. 22, 2016), https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection.
149 GDPR art. 30(2).
150 Directive 95/46/EC art.16.
151 GDPR art. 28(2).
152 GDPR art. 28(4).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

的隱私造成風險。

除了上述的新義務外，GDPR 也將許多原本指令中僅要求控制者的規範擴展到處理者，包含：保存資料處理紀錄的義務[153]；與 DPA 合作的義務[154]；採取採行適當的系統性及技術性安全措施，以保護個人資料在處理過程中可能造成的風險[155]；資料外洩後的通報義務[156]。同時也因為資料主體在 GDPR 下必須直接負擔規範義務，故資料主體得以直接對資料處理者提起控訴[157]。

第四目 加強法律執行與制裁

在法規的執行上，GDPR 有兩項重要的改革。首先，雖然各會員國仍需指定一或多個資料保護主管機關（DPA）以執行規則中的要求以及保護個人的權益，但由各國主管機關所共同組成以協調各會員國規範的 WP29 將由「歐盟資料保護委員會（European Data Protection Board, EDPB）」取代[158]。EDPB 仍會提供建議以及法律的解釋。另外，為了確保企業遵守資料保護規範，GDPR 也提高違反義務的罰金上限，從指令中的最多 100 萬歐元的罰金上限，提高到 2000 萬歐元或 1 年全球營業額的 4%的罰款[159]。

第三節 GDPR 義務對雲端運算服務提供者之影響

根據上述的介紹，GDPR 不僅擴大適用範圍、加強資料保護的義務，同時也增加資料主體的權利，可知歐盟立法者希望在新興的數位市場中，確保對於歐盟公民個人資料和隱私最高的保護水準。然而這些權利義務對於現況下的雲

153 GDPR art. 30(2).
154 GDPR art. 31.
155 GDPR art. 28(1), 28(3)(e), 32.
156 GDPR art. 33(2).
157 GDPR art. 82(1), 82(2).
158 GDPR art. 68.
159 GDPR art. 83(5), 83(6).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

端產業造成非常大的影響與衝擊，特別是增加雲端運算服務業者的營運成本，因此本文接下來將會根據對雲端業者造成最大影響的規範內容進行說明。然而因為歐盟資料保護規範體系中對資料控制者和資料處理者課以不同的義務，因此必須要先說明雲端運算業者的角色定位以利後續影響的說明。無論是在 DPD 或是 GDPR 下兩個身分的主要區別標準為：是否得以決定個人資料處理的目的和方法，得決定者為資料控制者，反之則是資料處理者 。

根據 WP29 的意見，雲端服務提供者應被定義為資料處理者，而使用雲端服務的使用者（客戶）則是資料控制者[160]。主要的原因如下：(1) 雲端服務提供者所提供的資料處理服務，被使用者清楚且嚴格的定義在契約當中，因此資料處理的目的是由雲端使用者決定，很難輕易改變；(2) 資料主體是直接授權予雲端使用者得以進行資料處理，而雲端服務提供者則是從使用者取得欲處理的資訊；(3) 通常單一雲端服務提供者所提供的資料處理服務，只是雲端使用者所進行資料處理的一部份，雲端服務提供者對於資料沒有排他的管理權限[161]。據此，原則上雲端運算服務提供者被定義為資料處理者。此外，因為雲端運算產業的特性，服務過程可能會涉及數個資料處理者，原始的資料處理者可能會透過簽訂契約的方式將部分活動外包給次級處理者（sub-processor）。因此一個雲端服務提供者，在不同的服務提供的過程中可能是資料處理者或是次級處理者，但不論是何者都需要遵守資料控制者對於執行資料處理的指示[162]。在確認雲端服務提供者之身分後，接下來針對 GDPR 生效後對雲端運算業者所造成影響進行分析：

首先，在 DPD 下，有義務保護個人資料隱私的是資料控制者，也就是雲端服務產業中的雲端服務使用者，如果其所使用的雲端服務提供者違反隱私保護

[160] Opinion 05/2012 on Cloud Computing, July 1, 2012, WP196, *supra* note 3, at 7.
[161] Mantelero, A, *Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution*, 3 EUROPEAN JOURNAL FOR LAW AND TECHNOLOGY (2012).
[162] Opinion 1/2010 on the concepts of "controller" and "processor", Feb. 16, 2010, WP29, 00264/10/EN.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

的要求，責任還是屬於控制者。因此美國大型的雲端服務提供者即使違反隱私規範，因為雲端服務使用者被要求要確保資料後續傳輸的保護水準，故基本上服務提供者並不會直接受到懲罰。但此現象在 GDPR 規範生效後有很大的改變。原本作為資料處理者的雲端服務業者只需負擔確保資料處理的安全措施有關的少數義務[163]。然而，GDPR 中對資料處理者訂定明確的法規義務，雲端服務提供者必須直接對資料處理的行為負責，個人也有權力直接對資料處理者提起司法救濟和請求賠償這也代表如果業者未能履行法規義務，將面臨被處以巨額罰鍰的風險[164]。

現況下，因為相較於雲端服務使用者，大型的雲端運算公司在契約的談判上佔有主導地位，因此雖然雲端服務使用者必須負擔 DPD 下的義務，但對於資料的控制程度反而不如這些雲端業者[165]。這個現象可能會在 GDPR 將雲端業者直接納入規範範圍中而有所改變，使得雲端業者不能使用其市場的主導力量使個人資料保護面臨風險。此外，履行義務的要求將會根本的改變雲端業者和使用者、資料主體以及 DPA 之間的關係。例如：在 DPD 的規範下，雲端業者和各國的 DPA 之間並沒有直接的互動，但現在 DPA 有調查處理者的權力，得取得所有處理者持有的個人資料。同時，DPA 也可以進到資料處理者的經營場址（到址調查）、發布警告、要求其遵守規範、禁止資料處理或甚至是對資料處理者處以罰鍰。

此外，在指令的規範下，原本僅提供雲端基礎設備（IaaS）或是平台（PaaS）給雲端使用者的業者，原則上不會取得在其設備或平台上處理的個人資料，而且若單純只是提供設備和平台，也不會有誘因要取得該些資料。然

163 Directive 95/46/EC art.16, 17.

164 主要的法規義務如前述包含：維護資料處理活動的相關文件記錄；採行適當的安全標準；執行定期的資料保護影響評估；指派 DPO；遵守跨境資料傳輸的相關規則，並且和會員國的 DPA 合作。

165 Mark Webber, *The GDPR' impact on the cloud service provider as a processor*, 16 PRIVACY & DATA PROTECTION JOURNAL 12, 12 (March, 2016).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

而，根據 GDPR，資料處理者必須了解甚至是紀錄這些個人資料，這些規範明顯對於 IaaS 或 PaaS 的業者並不恰當，原本僅是提供設備的業者被要求要進一步提供資料保護的設備，可能對業者造成不必要的負擔，以及對於契約上責任分配的不確定性[166]。

第三、是對雲端業者提供服務時契約簽訂方式的影響。在現況下，提供雲端運算服務的大型雲端業者（例如：Google, Facebook 和 Apple）皆使用標準化的服務條款，雲端服務的使用者僅能被動接受標準化契約中的條件或是更換服務提供者。然而，根據 GDPR 的規範，明確要求資料控制者和處理者在訂定契約時，必須納入條文所述的特定條款內容[167]。且相較於指令，GDPR 要求需要載入契約的內容增加，包含確保其員工的保密義務；採取適當的安全措施以避免資料的遺失或未經授權被取得或處理；只有在事先取得控制者的同意才得以採用次級處理者等。這項規範將迫使雲端業者改變其訂定契約的方式。

第四、一般而言，在雲端運算產業中一項服務的提供都會涉及一系列不同外包商提供的服務。然而，在 GDPR 中要求雲端服務業者在選擇次級處理者（外包廠商）前，必須要先取得控制者的「書面同意」，而且如果在外包服務上有任何改變都必須要通知控制者。此項義務在雲端環境中的可行性仍待商議。此外，根據 GDPR，外包服務予次級處理者雲端業者必須要確保該外包廠商也符合其與控制者之間契約的義務，如果次級處理者違反規範，係由處理者向控制者負責。現況下僅有只有大型的美國雲端業者有能力將違反義務的責任轉給次級的處理者，因為這些業者通常有能力控制整個供應鏈。但小型的 SaaS 服務提供者，很難有能力可以和 Amazon、Google 或 Microsoft 談判，要求這些企業去接受額外的義務，有學者認為可以預測大型的公司將會主導歐盟的雲端市

166 Mark Webber, *supra* note 165.
167 GDPR art. 28.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

場。

第五、GDPR 中的被遺忘權在執行上有一定的困難。GDPR 明確說明如果資料控制者公布了個人資料，在考慮技術和成本後，必須要採取合理的程序通知進行資料處理的第三方，資料主體對於刪除任何個人資料的連結（links）、複本（copy）或是再製（replication）的要求。但 GDPR 並未定義所謂的「合理的程序」，而且基於雲端產業的特性，很難說明特定資料的確切位置，甚至也很難說明誰是最原始的控制者，以及在複雜的雲端環境中，最原始的控制者要如何辨識需要通知哪些控制者或處理者。基於上述的問題，被遺忘權將造成雲端服務提供者非常大的負擔[168]。

最後，資料可攜帶權的要求也對雲端服務提供者造成負擔。這項權利主要是為了解決在雲端中會出現的供應商鎖定的問題，要求資料控制者或處理者必須要確保資料得以切換成可移轉的格式。然而在現況下，多數的雲端服務提供者並未使用標準化的資料格式以及服務介面，以促進不同雲端服務業者之間的可互通性（interoperability）[169]。特別對中小型的企業來說，這項要求可以自由移轉個人資料的權利，將會造成不成比例且巨大的額外負擔，因為可攜帶權實際上要求雲端業者必須要投資新的系統，並且確保移轉資料的進出系統一致[170]。另外，根據歐盟雲端運算契約的專家組織，資料的移轉應該被視為一項雲端業者可以額外收費的服務[171]。但根據 GDPR 的規定，以及 WP29 所發布的關於資料可攜帶權的指導，資料控制者不得對移轉服務收費，也會影響雲端服務業者的營運方式[172]。

---

168 ENISA, T*he Right to Be Forgotten – Between Expectations and Practice*, Oct. 18, 2011, www.enisa.europa.eu/publications/the-right-to-be-forgotten.

169 Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Sept. 22, 2015, WP232, 2588/15/EN, at 12.

170 P Swire and Y Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72(2) MARYLAND LAW REVIEW 335 (2013).

171 *EC Expert Group on Cloud Computing Contracts*, Dec. 2014.

172 Guidelines on the right to data portability, Dec.13, 2016, WP242 rev.01, 16/EN, at 12.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

綜上所述，整體而言 GDPR 不僅是提供統一性的資料保護法規，亦為因應新型態網路科技的發展，增強了規範的強度，對雲端產業造成很大的影響。可以預期雲端服務業者將會大幅改變營運的模式，同時也必須要增加投資以確保得以完全履行 GDPR 下的義務[173]。

第四節 小結

從本節之分析可得知，歐盟 1995 年資料保護指令和美國整體的資料保護法律體系，無論是目地宗旨、保護手段、適用範圍、實體權利義務、法律執行等都具有非常大的落差，此資料保護規範上的落差也成為美國企業在進入歐盟市場時最大的疑慮。另外，歐盟在 2016 年所通過的 GDPR 更近一步擴大適用範圍，將原本僅需要負擔極小義務的資料處理者納入規範內，對於雲端運算業者影響最大，使其必須負擔許多額外的成本來履行義務。另外，GDPR 在賦予資料主體的權利，和加諸在資料控制或處理者身上的義務都較指令更為嚴格，對雲端業者而言也帶來新的負擔，例如：GDPR 中關於資料處理記錄保存的要求，會使得 PaaS 和 IaaS 的業者除了和以往一樣提供平台和設施，還必須要進一步去了解資料處理的內容甚至對此負責；另外 GDPR 也改變雲端產業契約訂定的方式，現況下通常雲端服務業者相較於使用者的談判籌碼較高，傾向採用標準化的契約條款要求資料控制者接受，然而 GDPR 詳細要求控制者與處理者之間契約的內容，可能會實質改變現況的服務提供模式；再者，雲端服務的提供經常涉及將部份的資料處理外包給次級處理者，GDPR 要求在外包服務前必須先取得控制者的書面同意，也必須要要求次級處理者符合一定的義務，這項規範對於基於各種不同目的大量處理資料的雲端運算產業而言，有一定的影

[173] 根據 ICO 關於為符合 GDPR 義務所會增加的成本預期研究，光是英國企業的成本就高達一年 3 億 2000 萬歐元。 London Economics, *Implications of the European Commission's Proposal for a General Data Protection Regulation for Business*, May 2013, https://ico.org.uk/media/1042341/implications-european commissions-proposal-general-data-protection-regulation-for-business.pdf.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

響。整體而言，原本 DPD 對於資料保護的規範要求就較美國嚴格，而 GDPR 進一步提高保護水準，更加擴大跨大西洋兩岸規範的差距。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第四章 歐美對雲端運算產業跨境資料傳輸規範之比較分析

雲端運算服務要順利進行，資料的跨境傳輸為重要關鍵，而資料的跨境傳輸則會因為各國隱私保護規範的不一致形成傳輸上的障礙。根據第三章之各項比較可得知，無論是法律的保護手段、適用範圍、實體權利義務或是法律執行的方式，歐盟和美國的個人資料保護體系都存有巨大差異。甚至歐盟 WP29 也曾在意見書中指出：「美國現在以特定部門的法律和自願規範的拼湊物（patchwork）不能提供歐盟所要求對於個人資料的充足保護」[174]。這些差異都會造成美國雲端業者在提供服務時的巨大阻礙，甚至影響雲端產業透過大量蒐集資料，並於遠端處理的服務提供模式。一旦資料被禁止進行跨境傳輸，則雲端科技所帶來的效率將難以被達成。為了瞭解美國業者在跨境傳輸歐盟公民個人資料時必須符合之要求，本章將以「跨境資料傳輸」之規範為核心，分析美國業者如何在歐美存在巨大法律規範落差的情況下，順利進行跨大西洋資料傳輸。第一節將先說明在 DPD 下對於跨境資料傳輸有何要求，以及美國業者於該些規範下所採用的跨境傳輸途徑，雲端業者是否亦得適用該些途徑。然而，如前述，歐盟新的 GDPR 針對資料保護規範進行改革，故第二節將說明在 GDPR 下跨境傳輸的規範有何改變，是否提供更有效的跨境傳輸途徑。最後針對整體資料跨境傳輸的規範和傳輸途徑作一小結。

第一節 歐盟資料保護指令之跨境傳輸規範

[174] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government, Jan. 26, 1999, WP 15, 5092/98, at 4.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

根據歐盟 1995 年 DPD 第 25 條第 1 項之規定，會員國應該確保任何傳輸至第三國後將欲處理之個人資料的傳輸，僅得在遵循符合本指令之國內法的情況下得以進行，該第三國應該確保對資料的充足保護[175]。意指資料傳輸的目的地國對個人資料應該要有「充足的保護水準（adequate level of protection）」。而所謂充足的保護水準根據歐洲法院（Court of Justice of the European Union , CJEU）的見解，應該依照指令第 25 條第 2 項所有的情況進行權衡[176]。第 25 條第 2 項所羅列應納入考量的相關標準包含資料的性質、資料處理目的、處理期間、資料來源國以及傳輸之目的地國與第三國現行有效之一般法律規定及特別規定等[177]。但資料傳輸的目的地國（第三國）的資料保護水準未必需要和歐盟「完全相同」，但需達到本質上相當（essentially equivalent）的水準[178]。第三國的資料保護法規是否提供資料充足的保護水準是由執委會評估，並做出「適足性的認定（adequacy decision）」來確認。

另外，歐盟 DPD 第 26 條也揭示在特定的情況下，即使不符合充足保護水準仍得進行傳輸，第 26 條第 1 項包含：(a) 資料主體對該傳輸給予明確地同意[179]；(b) 資料的傳輸對履行資料主體與資料控制者之間的契約，或依據資料主體請求執行契約前之措施為必要[180]；(c) 資料的傳輸對資料控制者和其他自然人或法人間簽定或履行，基於資料主體利益之契約為必要[181]；(d) 資料的傳輸是基於重要的公共利益，或該傳輸對於法律主張之建立、行使或防禦為必要[182]；(e) 資料的傳輸是為保護資料主體的重要利益[183]；(f) 資料傳輸是依據歐盟或會員國法律之登記，目的為提供資訊給一般大眾或提出諮詢且具合法利益

[175] Directive 95/46/EC art. 25.
[176] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, Judgement of 6 October 2015, ¶ 70.
[177] Directive 95/46/EC art. 25(2).
[178] *Id*. ¶ 73.
[179] Directive 95/46/EC art. 26(a).
[180] Directive 95/46/EC art. 26(b).
[181] Directive 95/46/EC art. 26(c).
[182] Directive 95/46/EC art. 26(d)
[183] Directive 95/46/EC art. 26(e).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

者，但僅限於滿足該歐盟或會員國法所列之特定條件的情況[184]。第 26 項第 2 條則說明如果控制者得提供適當的保護措施（adequate safeguards），以確保資料隱私、資料主體之基本權利受到保護，則即使傳輸之目的地不符合 25 條的充足保護水準，控制者仍得進行傳輸。

因此任何企業或組織如果欲將資料跨境傳輸到歐盟境外，只得在該目的地國的規範具充足保護水準，或該傳輸行為符合 DPD 所列之特定例外的情況下才得進行。根據此規範原則，本節將介紹在 DPD 的法律制度下，美國業者進行跨境傳輸的主要途徑。另外，因雲端運算產業為近年來快速發展的新興產業，具有特殊之產業型態，故本節最後將分析現況下一般美國企業用以作為跨境資料傳輸之途徑於雲端運算產業是否適用。

第一目 DPD 下之傳輸途徑

首先，雖然美國從未主動要求歐盟執委會對其資料保護法規之進行「適足性」的審查，並做出認定，但歐盟各會員國的共識為美國的隱私法並未達到充足的資料保護水準[185]。因此，美國業者很難以執委會對美國整個資料保護法規之適足性認定作為傳輸的基礎。在此情況下，美國業者解決資料傳輸困境的途徑如下：

1. 資料主體的同意（consent）

依據 DPD 第 26 條第 1 項（a）款，資料主體對於資料跨境傳輸給予清楚地（unambiguously）同意則得例外進行跨境資料傳輸，而這項同意必須由資料主體主動給予（freely given），且必須針對「特定（specific）」的傳輸行為[186]。通常這項方法用於一次性的資料傳輸（specific one-off

[184] Directive 95/46/EC art. 26(f).
[185] Paul M. Schwartz, *supra* note 83, at 1980.
[186] Directive 95/46/EC, art. 26(1)(a)

DOI:10.6814/THE.NCCU.IB.015.2018.F06

transfer），重複且持續進行的跨境資料傳輸要取得資料主體對於特定傳輸行為明確的同意非常困難。

2. 標準化條款（Standard Contractual Clause, SCC）

根據 DPD 第 26 條第 2 項，資料控制者提供適當保護措施亦得做為合法傳輸的依據，據此，歐盟執委會訂定 2 項標準化條款，提供企業作為適當的保護措施。企業或組織在簽定契約時，於契約中納入 SCC，即得認為資料控制者與資料傳輸的接受者願意遵守歐盟指令中關於資料保護的原則，而 SCC 即為進行跨境資料傳輸的法律依據。目前的 SCC 包含一項適用於歐盟境內的資料控制者將資料傳輸到歐盟或 EEA 境外的資料控制者的情況（controller-controller）[187]，另一項則適用於位於歐盟境內之資料控制者將資料傳輸到歐盟或 EEA 境外的資料處理者的情況（controller-processor）[188]。

然而，SCC 是否得以提供跨境資料傳輸有效的隱私保護現階段仍有爭議，其中最受矚目的案件是 *Irish Data Protection Commissioner v. Facebook and Max Schrems* 一案。該案起源於一名奧地利公民 Max Schrems 向愛爾蘭資料保護主管機關（Irish Data Protection Commissioner, 以下簡稱愛爾蘭 DPC）提起控訴，認為美國 Facebook 公司和愛爾蘭 Facebook 公司使用 SCC 作為資料傳輸的法律依據，並不能有效確保其資料受到歐盟指令要求的充足保護。其主張美國政府在 SCC 的規範下仍可以透過大規模的監控來取得個人資料，認為歐盟法律制度賦予個人的基本隱私權利受到侵犯[189]。

---

[187] *Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC*, at 19, O.J. (L 181), July 4, 2001; 2004 年執委會針對 2001 年的 SCC 進行修改。

[188] *Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC*, at 52, O.J. (L 6) (Jan. 10, 2002). .

[189] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, [2016] No. 4809 (H. Ct.) (lr.).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

愛爾蘭 DPC 認為美國政府授權對於從歐盟傳送到美國的個人資料進行電子監控，且在美國的法律制度下受影響的資料主體未有有效的救濟途徑，違反歐洲基本權利憲章第 47 條的規範，同時也違反憲章第 7、8 條賦予人民的基本隱私權[190]。因此愛爾蘭 DPC 主張以歐盟執委會訂定的 SC 作為保護措施也未能有效保護資料隱私。然而 SCC 係由歐盟執委會的決議訂定，故 SCC 是否無效應由歐盟法院裁定，相關的法律程序目前被提交到歐盟法院進行先行裁決。SCC 的法律效力面臨可能會被宣判無效的不確定性。

3. 企業內部約束規則

同樣根據 DPD 第 26 條第 2 項，具拘束力之企業規則（Binding Corporate Rules, BCR）亦是提供適當保護措施的途徑之一。BCR 指的是同一個企業集團內部，在將個人資料轉移到一個或多個 EEA 境外之第三方國家同一集團的資料控制者或處理者時，必須遵守企業針對個人資料保護訂定的內部規範。透過 BCR 的保護，個人資料得以例外被傳輸到歐盟境外。BCR 主要是藉由企業足夠的內部控制來確保個人資料的隱私，但 BCR 必須由各會員國的資料主管機關確認後方得作為跨境資料傳輸的法律基礎。即使目前歐盟內已經有許多關於企業訂定 BCR 的指導[191]，但企業採納 BCR 的狀況卻不理想，主要是因為現在取得主管機關同意的程序冗長又昂貴，很多企業認為訂定 BCR 非常麻煩且費時費力。

4. 歐美跨境資料傳輸協議

[190] 歐洲基本權利憲章第 47 條保障歐盟公民尋求司法救濟和公正裁判的權利。

[191] Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, Apr. 14, 2005, WP108, 05/EN; Recommendation 1/2007 on the Standard Application for the Approval of Binding Corporate Rules for the Transfer of Personal Data, Jan. 10, 2017, WP 133; Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, June 24, 2008, WP153, 18/EN; Working Document Setting up a framework for the structure of Binding Corporate Rules, June 24, 2008, WP154, 1271-00-01/08/EN.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

如前所述，美國的資料保護法規本身未能達到歐盟 DPD 第 25 條規範的「充足保護水準」，故原則上歐盟公民的個人資料被禁止傳送到美國。為了解決法規上的落差，美國商務部（U.S. Department of Commerce, DOC）和歐盟執委會共同發展出「美國—歐盟安全港架構（U.S.-EU Safe Harbor Framework）」。DOC 於 2000 年發布了安全港協議隱私原則[192]，而歐盟執委會對此也做出適足性的認定，同意如果美國企業符合安全港協議之原則及得視為提供適當保護[193]。在安全港協議的原則下，美國企業得以每年自行向 DOC 進行認證，確定其符合安全港協議中關於隱私保護的 7 項基本原則以及其他相關的要求，基於此自我認證，美國企業得被視為符合歐盟隱私保護的標準，並得以以協議作為跨大西洋資料傳輸的法律基礎[194]。但在 2015 年，安全港協議被歐洲 CJEU 認定為無效，CJEU 的裁定的來源源自於一名歐洲公民向愛爾蘭 DPA 提起控訴，認為歐洲 Facebook 公司的用戶資料被傳輸到美國 Facebook 公司時，這些個人資料受到美國政府的監視，美國法律中並未能提供防止美國政府大規模監測歐洲人民個人資料的方法（與 SCC 受到的法律挑戰相似）。愛爾蘭最高法院將此案提交制歐洲法院進行先行裁決。根據 CJEU 的裁決，其認為執委會所承認的安全港協議中的自願認證機制並不足以確保歐洲公民的資料在美國受到保護，CJEU 因

192 U.S. Department of Commerce, *Safe Harbor Privacy Principles and Related Frequently Asked Questions*, July 21, 2000.

193 Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, July 26, 2000, C(2000) 2441, 2000/520/EC.

194 安全港協議的 7 項基本原則分別是：1. 通知（Notice）：組織必須要告知個人關於蒐集和使用資料的目地、如果個人有疑問應該如何與組織聯繫以及個人資料將會被揭露給哪些第三方。2. 選擇（Choice）：組織必須提供個人下列事項的選擇權利：(a) 揭露資料給第三方；(b) 將資料用於原本蒐集和後續被授權使用之目的不同的目地。3. 後續的傳輸（Onward transfer）：將資料進一步傳輸給第三方，必須要遵守通知和選擇的原則，而該第三方也要提供相同的隱私保護水準。4. 安全（Security）：組織創造、蒐集、使用或散布個人資料必須要採取適當的預防措施保護個人資料。 5. 資料完整性（Data Integrity）：必須要確保資料被用於原本的使用目的、且資料正確並隨時更新。6. 進取權（Access）：個人必須得以接觸到其個人資料，且必須得以修正、更改或刪除部正確的資料。7. 執行（Enforcement）：有效的隱私保戶必須要包含認證義務履行的機制，同時也要包含救濟措施，以及為履行義務時的制裁。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

此認定安全港協議無效[195]。CJEU 的判決對於美國和歐盟之間的貿易影響重大，因為有將近 4000 家企業是依靠安全港協議進行資料傳輸[196]。雖然這些企業還是得以 SCC 或 BCR 等傳輸途徑進行傳輸，但執委會和 DOC 仍然認為歐美之間需要發展新的隱私保護框架，以確保跨大西洋資料傳輸的法律穩定性。因此雙方於 2016 年 7 月達成新的隱私架構協議的共識──「歐盟─美國隱私屏障框架（EU-US Privacy Shield framework）」[197]。新的協議中加強原本安全港協議規範的程度，並針對美國業者設立新的義務，此協議為許多雲端運算服務業者用以作為正當化依據的途徑，詳細規範內容將於後續章節深入討論。

第二目 美國雲端業者適用 DPD 下傳輸途徑之困境

在 DPD 的規範下，雖然已經存在可以做為跨大西洋資料傳輸法律依據的途徑，但雲端運算服務如前面的介紹所述，為近年興起以資料處理為中心的產業，在服務提供的過程通常涉及資料跨境傳輸，而這些過程必須要符合歐盟 DPD 下各歐盟會員國所採行的法律[198]。然而歐盟在訂定 DPD 時並未考量到此種資料密集產業的快速發展，故法規的訂定也未考量到雲端運算服務的產業特性，這些雲端運算獨有的產業特性也讓雲端服務提供者在適用現有途徑時面臨到許多挑戰。因此接下來將說明在 DPD 的規範下，雲端運算業者在適用跨境傳輸途徑時會遇到的問題。

首先，取得資料主體同意的方式並不可行。同意的方式通常用於特定的一

195 Case C-362/14, *supra* note 176.
196 P. Chase, S. David-Wilp & T. Ridout,*Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies*, 2016, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf.
197 Privacy Shield Framework, https://www.privacyshield.gov/welcome.
198 Judith Rauhofer & Caspar Bowden, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, EDINBURGH SCHOOL OF LAW RESEARCH PAPER (June 21, 2013).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

次性資料傳輸（specific one-off transfer），而非像絕大部分雲端運算所使用的重複以及持續進行的資料交換[199]。對於資料控制者而言，要取得資料主體對於資料控制「精確」的同意是非常困難的，或甚至是不可能[200]。此外以同意作為正當化資料傳輸的方式，必須要在傳輸之前先取得同意，因此所有傳輸的細節必須要在事前就決定好，尤其是傳輸的目的和接受者，並且要告知資料主體，同時資料主體對於傳輸的同意也可以隨時撤回[201]。對於雲端運算這種將定期或是重複的資料傳輸作為企業商業行為一部分的產業，以同意作為資料傳輸的途徑並不可行。最後，DPD 中所規範的「同意」必須取自於資料主體。在雲端運算的情況下，許多雲端服務提供者所處理的資料為雲端使用者的員工、供應商或客戶的資料，因此要直接取得資料主體的同意在雲端產業的運作情況下基本上很難做到[202]。

再者，SCC 除了前面所述的法律訴訟問題外，實際上 SCC 的設計也未能真實反應雲端運算產業的現況。首先，對於雲端運算產業而言 SCC 太不具彈性[203]。原則上為了確保資料控制者的義務得以被完整的履行，SCC 必須完整且沒有修改的被納入雲端服務的契約中[204]。但在現況下，實際上大部分的美國雲端服務提供者的規模和談判的議價能力都比雲端服務使用者大，可能會不願意採用大幅影響其服務提供範圍和選擇外包廠商權利的條款。WP29 也建議，除了 SCC 外，雲端服務提供者可以在不違反 SCC 和資料主體基本權利的前提下，加入基於實務經驗的額外條款[205]。此外，在雲端運算產業中許多資料處理的過程中都涉及次級資料處理者（外包商），而用於處理者與次級處理者之間的 SCC

199 *Id*. at 8.
200 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Nov. 25, 2005, WP114, 2093/05/EN.
201 *Id*. at 12.
202 Judith Rauhofer, *supra* note 198, at 8.
203 WK Hon and C Millard, *Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4*, 9 SCRIPT-ed 23-24 (2012).
204 Judith Rauhofer, *supra* note 198, at 12.
205 Opinion 05/2012 on Cloud Computing, *supra* note 3, at 19.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

是效仿資料控制者和處理者之間的 SCC。在 2010 年執委會修改其通過的決定，允許資料處理者得以在符合其與資料控制者之 SCC 的條件下進一步將資料傳輸到一個或多個次級處理者。

然而如果原始的雲端運算服務是由歐盟的資料控制者和歐盟的資料處理者所簽訂，因為其契約中不會包含 SCC，後續資料處理者要將雲端運算服務外包給其他次級處理者便不能有得作為基礎的 SCC，亦即不能將控制者和處理者間 SCC 的義務進一步適用於資料處理者與次級處理者之間（carry forward）。換言之，如果資料控制者和處理者皆在歐盟境內，而次級處理者位於美國，就會出現無法律基礎得依據的困境，因此使用 SCC 作為跨境資料傳輸的途徑並不能完全符合雲端產業的需求。

最後，BCR 並不能涵蓋所有雲端跨境資料傳輸的情況。BCR 的使用主要是提供跨國公司在進行集團內部跨境資料傳輸時得以證明採取符合 DPD 第 26（2）條規範的「適當防衛措施」[206]。然而對雲端運算服務提供者而言以 BCR 作為跨境傳輸的主要途徑仍不足以確保資料傳輸的持續和穩定。其中最主要的問題是，所謂的 BCR 僅適用於同一個公司集團內部，因此如果雲端服務使用者、雲端服務提供者，以及外包廠商並不屬於同一公司集團，整體雲端產業鏈的運作並不適用此一途徑。而在雲端運算產業中，因為產業的特性，一個服務的提供可能涉及其他次級服務提供者的參與，也通常都包含公司外部的廠商，這樣的外包關係或是服務提供的關係 BCR 即不得適用[207]。

綜上所述，在 DPD 的規範下美國業者通常採用資料主體明確的同意、企業在簽訂契約時納入 SCC，以及企業團體之間的 BCR 作為跨境傳輸的途徑。然而每個途徑各有其缺點以及施行上的問題。此外，因為雲端運算服務的產業型

206 Explanatory Document on the Processor Binding Corporate Rules, Apr. 19, 2013, WP204, 00658/13/EN, at 6.
207 *Id*. at 7.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

態有其特殊性，故雲端運算業者在適用這些途徑上更不可行。而歐美之間跨大西洋資料傳輸協議的適用問題將於本文第五章做詳細的分析。

第二節 GDPR 之跨境傳輸規範改革

2016 年通過的 GDPR 除了提高資料隱私保護的水準外，歐盟的立法者同樣意識到在新興的雲端市場中跨境資料傳輸是必要的要件，且也是雲端運算產業最重要的資料保護議題之一。通常被上傳到雲端的個人資料會在全球不同的管轄領域之間流動，或是儲存在不同國家的伺服器內。為了確保這些在不同國家之間流動的歐盟公民個人資料得受到適當的隱私保護，根據 GDPR 第 44 條，任何經處理或傳出至第三國或國際組織後將欲處理之個人資料之傳輸，僅得於資料控制者或處理者符合本章義務的情況下進行，包含從第三國或國際組織進一步進行資料的傳輸（onward transfers）[208]。由此可知 GDPR 規範的邏輯和 DPD 相同，原則上禁止資料的處理和跨境傳輸，除非符合 GDPR 中的要件。而根據 GDPR 第 45 條之規定，個人資料傳輸到第三國或國際組織時，僅得於執委會認定該第三國、第三國內之領域或特定部門，或國際組織對資料提供充足的保護水準時才得以進行[209]。與 DPD 相同，資料傳輸時，目的地國必須提供充足的保護水準，只是在 GDPR 下，執委會適足性的認定不僅限於國家，亦得針對一國境內的特定領域或特定部門。另外 GDPR 在第 45 條中更進一步加入第三國是否具有有效且獨立的資料保護監管主管機關；及該國的法治是否提供資料主體有效且可執行的行政和司法救濟途徑等標準，作為執委會在做適足性認定時所應納入考量的因素[210]。

GDPR 下也和 DPD 同樣有例外得進行資料傳輸的規定。根據 GDPR 第 46 條，資料控制者或處理者如果能提供適當保護措施，確保資料隱私、資料主體

[208] GDPR art. 44.
[209] GDPR art. 45.
[210] GDPR art. 44, 45.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

之權利並且確保具有有效權利救濟途徑時，得在資料傳輸目的地國不符合充足保護水準的情況下，例外進行跨境資料傳輸[211]。而 GDPR 更進一步在第 46 條第 2 項將 SCC、BCR 明文定義為適當的保護措施[212]。並且在 GDPR 條文內提供更具體的內容，讓企業組織得以更容易使用這兩個途徑作為跨境資料傳輸的法律基礎[213]。同時透過直接規範的方式，也得大幅減少各國 DPA 在核准時解釋和施行的不一致性，降低企業必須要適應不同國家法規落差的成本[214]。另外，GDPR 中也新增幾項得以視為適當保護措施的途徑，分別為：「DPA 條款[215]」與「行為準則[216]和認證[217]（codes of conduct and certification）」。GDPR 第 49 條則和 DPD 第 26 條第 1 項相同，列出得以例外進行傳輸的特定情形[218]。

由上述之條文規範內容可知，基本上 GDPR 的規範和 DPD 相同，禁止資料跨境傳輸到歐盟境外，除非該第三國對於個人資料具有充足的保護水準，但為協助業者取得跨境傳輸的正當法律基礎，GDPR 亦改革現有的資料跨境傳輸途徑，同時新增新的傳輸方法，以求釐清原本指令下各途徑的規範細節，並彌補原本各途徑的不足。

第一目 GDPR 對現有途徑之改革未能解決雲端業者之困境

然而，即便 GDPR 已針對 DPD 下之傳輸途徑進行改革，並且新增新的傳輸選擇，仍不足以提供雲端運算業者有效的法律基礎，以進行跨大西洋的資料傳輸。原因敘述如下：

---

211 GDPR art. 46(1).
212 GDPR art. 46(2)
213 GDPR 提供關於 BCR 明確的要件和程序要求。如果公司集團內部的 BCR 符合 GDPR 中所規範的要求，則有權的 DPA 必須要核准該 BCR 作為公司內部跨境傳輸的基礎。GDPR art. 47.
214 Marina Škrinjar Vidović, *EU Data Protection Reform: Challenges for Cloud Computing*, 12 Croatian Yearbook of European law & Policy 171, 200 (2016).
215 GDPR art. 46(2)(a).
216 GDPR art. 46(2)(e).
217 GDPR art. 46(2)(f).
218 GDPR art. 49.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

首先、為了使業者得以透過更具彈性的途徑取得跨境傳輸的正當性，GDPR 擴大執委會適足性認定的範圍，除了特定國家，亦得針對具有充足的保護水準「特定地區 specific territory」或「特定產業」作出符合標準的決定[219]。然而，由先前就美國資料保護體制的分析可知，美國整體而言資料保護水準仍落後歐盟，再加上 GDPR 加強資料保護規範的義務，因此美國要取得執委會的認可仍有困難。而且針對雲端運算產業，美國也未提供更嚴格的保護規範，即使僅針對雲端運算產業去作適足性的認定應該也難以被認為和歐盟具有本質上相當的保護水準。故此一途徑對跨大西洋資料傳的而言，無論是否是雲端運算產業仍不可行。

第二、以資料主體的同意作為雲端產業跨境傳輸的基礎仍不可行。GDPR 相較於指令更進一步釐清形成有效資料主體同意的條件，詳細訂定指令中所規定的「主動給予（freely given）」和「消費者知情（informed）」的要件[220]。然而雖然 GDPR 提供更明確的規範，但仍然未改變同意僅適用於一次性資料處理的特性。如前所述，雲端運算服務通常涉及非常多的資料主體，且每次資料處理的目的不一定完全相同，同時資料儲存的位置也可能會不斷改變，因此同意的途徑在雲端服務產業依然難以適用。此外，WP29 也提到這項方法通常僅適用於非大量（non-massive）、非重複（non-recurrent）以及非結構性（non-structural）的資料傳輸。所以可見在雲端運算產業中不太可能採用此項方法[221]。

---

[219] GDPR art. 44, 45.

[220] 在新的規範中進一步釐清同意的要件：1. 資料主體不僅要有同意的意思，還必須要以清楚且明確的方式表達，GDPR 明文排除默示同意或被動取得的作法。2. 「主動給予」的部分，資料主體必須有真正自由選擇的權利（genuine and free choice），且資料主體也必須得自由的拒絕或收回該同意。另外，如果資料控制者和資料主體之間有明確的不對等關係（clear imbalance），則同意就會被假設為非主動且自由的給予。而且資料控制者也必須要避免以資料主體的同意做為契約生效的必要要件；3. 知情的部分，GDPR 要求資料控制者必須要以容易理解的方式去告知資料處理的內容、資料控制者的身分、資料處理的目的等。

[221] Opinion 05/2012 on Cloud Computing, *supra* note 3, at 18.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第三、GDPR 將 SCC 和 BCR 正式納入規範範圍，並提供更具體的內容。在 SCC 的部分，現況下的執委會已經通過的 SCC 將得繼續使用，然而 GDPR 並未解決在雲端服務業者於歐盟成立的情況下 SCC 難以適用的問題，且 SCC 所面臨的法律挑戰也尚未有結果，故使用 SCC 仍有其不確定性和不足之處[222]。另外，在 BCR 的部分，GDPR 將 BCR 直接納入條文規範的作法會使得採用 BCR 作為跨境傳輸的依據更為容易，WP29 也承認在同一個集團內的資料控制者要將大量的資料傳輸到次級處理者時，BCR 會是有效率的法律途徑[223]。以此觀點觀之，BCR 可能可以在雲端運算產業中適用[224]。然而，同樣的，BCR 仍然僅能適用於「同一個企業集團內部的外包服務」，而雲端產業中的服務外包的情況複雜，因此僅使用 BCR 並不能滿足確保雲端產業整體跨境資料傳輸穩定性的需求。

由上述之分析可知，雖然 GDPR 的規範有針對現有的傳輸機制進行釐清和改革，但基於雲端預算產業的特性，這些措施個別或是整體都不足以確保美國雲端運算業者得以大量、穩定的進行跨大西洋的資料傳輸。

第二目　雲端業者適用 GDPR 新途徑之挑戰

GDPR 中除了針對現有的資料傳輸途徑進行改革，亦增加新的傳輸途徑，以提供企業組織在選擇如何正當化跨境資料傳輸行為時有更多彈性。這些新的傳輸途徑包含「DPA 條款」與「行為準則和認證（codes of conduct and certification）」。前者雖然被認為是新的途徑，但所謂 DPA 條款和執委會的 SCC 相似，只是改由各國 DPA 自行訂定或是相互合作後訂定以作為跨境傳輸的法律基礎。目前仍未有會員國之 DPA 訂定並發布相關的條款，因此實際使用的情形

222 Opinion 05/2012 on Cloud Computing, *supra* note 3, at 18.
223 Explanatory Document on the Processor Binding Corporate Rules, *supra* note 206.
224 V Reading, *Binding Corporate Rules: Unleashing the Potential of the Digital Single Market and Cloud Computing* (speech held at IAPP Europe Data Protection Congress) Nov. 29, 2011, at 4, file:///C:/Users/lorra/Downloads/SPEECH-11-817_EN.pdf.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

尚未清楚。

另外則是行為準則和認證，所謂的行為準則係由同一產業的聯盟或工會發展出針對特定產業的自願性標準和規範，訂定行為準則的目的以 GDPR 為例，一方面是提供廠商證明符合規則規範的方式，另一方面也是讓消費者得以更容易的透過此透明的標準規範去檢視廠商是否符合規則[225]。目前，歐盟境內的「歐洲雲端基礎設施服務供應商聯盟（Cloud Select Industry Group, C-SIG ）已經發展出針對雲端運算產業的行為規則（EU Data Protection Code of Conduct for Cloud Service Providers）[226]。該行為準則提供雲端服務業者遵守 GDPR 義務的詳細說明和指引，不僅讓雲端運算業者得以更有效的履行義務，同時宣布遵守該行為準則並且經過第三方認證後，企業也可以此作為履行 GDPR 的證明。然而雖然納入這項新的方法的確提供控制者和處理者更多彈性，但作為跨境資料傳輸的正當化基礎仍有疑慮。首先，關於行為準則作為傳輸基礎的條文規定並不夠詳細，適用上也需要更進一步的解釋和執行[227]。另外，觀察目前針對雲端產業訂定的行為準則可以發現，跨境資料傳輸的規範分為兩部分，一是針對同一級集團內的資料傳輸，另一則是針對跨境傳輸到第三國[228]。但除了針對特定名詞和作法有更詳細的說明外，例如：同一集團之資料控制者和處理者的定義，行為準則中仍是再次重申如果要進行跨境傳輸資料控制者或處理者仍必須要採用 BCR、遵守 SCC、取得資料主體的同意或是傳輸到被執委會認定為保護程度充足的第三國[229]。因此雖說行為準則的確是在 GDPR 中才被納入條文規範的方式，但如果仔細觀察行為準則的內容，目前似乎沒有提供雲端業者原本幾項途徑外其他正當化跨境傳輸行為的方式。

---

[225] *EU Cloud Code of Conduct Version 2.0*, EU CLOUD COC INFORMATION PORTAL, at 4, May, 2018 https://eucoc.cloud/fileadmin/cloud-coc/files/European_Cloud_Code_of_Conduct.pdf.
[226] *Id*.
[227] Marina Škrinjar Vidović, supra note 214.
[228] EU Cloud CoC, supra note 225, at 10-12.
[229] *Id*.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

最後則是認證機制，所謂的認證是用來證明處理者或控制者符合特定標準[230]。雖然根據 GDPR 得以發展認證機制，並以該項認證作為跨境傳輸的基礎，但目前尚未有進展，故是否得以有效作為資料傳輸的基礎仍不確定。

第三節 小結

對於雲端服務供應者而言，跨境資料傳輸為提供服務不可或缺的要件，尤其是美國大型的雲端服務供應者要進入歐盟提供服務，勢必會涉及資料跨大西洋傳輸的問題。根據 DPD 的規範所衍伸出來的跨境資料傳輸途徑，分別為資料主體明確的同意、企業在簽訂契約時納入 SCC、企業團體之間的 BCR 以及歐美之間的隱私屏障協議，這些途徑皆可作為法律基礎正當化資料跨境傳輸到美國的行為，然而每個途徑各有其缺點以及施行上的問題。此外，因為雲端運算服務的產業型態有其特殊性，故雲端運算業者在適用這些途徑上更不可行。歐盟為了適用近年興起的數位經濟與雲端科技，在 2016 年的 GDPR 中亦改革了跨境資料傳輸的規範，不僅將原本既有的指令傳輸途徑規範釐清，包含執委會對於充足保護水準的認定、資料主體的同意，也將業者常用但不在指令規範內的 BCR 和 SCC 明確納入條文範圍。GDPR 中甚至提供新的傳輸途徑，希望廠商在不可避免要進行資料跨境傳輸時，能確保個人的資料隱私被完善的保護。

但從上述的分析可知，GDPR 對現有制度的改革並未真正解決原本各途徑對於雲端運算業者而言適用上的問題。新的傳輸途徑 DPA 條款、行為準則與認證制度目前也被認為不足以解決問題。由此可知，GDPR 即使提供新的選擇，都未能有效解決原本既有方法的不足。雲端運算產業的特性和傳統產業不同，資料跨境傳輸為服務提供的必要條件，尤其是對美國大型雲端運算服務提供者而言，如果未能取得有效進行資料傳輸的方法，進入歐盟市場將會遇到非常大

[230] GDPR art.42, 43.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

的困難。為了解決雲端運算產業大量且持續進行跨大西洋資料傳輸的需求，如前所述，歐盟執委會和美國商務部共同討論發展出新的跨境資料傳輸框架協議──隱私屏障協議，希望得以根本解決跨大西洋資料傳輸的困境，目前約有3000 多家美國業者都以此途徑作為跨大西洋傳輸的途徑，對於歐美兩國之間的業者而言，隱私屏障協議非常重要。但先前有安全港協議被法院判決無效，對於產業造成重大影響的先例，隱私屏障協議是否得真正有效且持續提供跨境傳輸正當的法律基礎，將於下一章進行分析。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第五章 歐美隱私屏障協議作為調和方案之可行性分析

GDPR 生效後，對雲端業者的義務要求增加，要如何確保符合法規上的義務對於美國業者而言是一大考驗。而且 GDPR 中對於現有途徑的改革，以及新增的傳輸途徑仍然不能作為雲端業者有效的法律基礎，故另尋折衷的替代方法有其必要。在 2015 年 CJEU 裁定安全港協議為無效前，許多公司都是依靠歐美之間的跨境資料傳輸協議作為傳輸的途徑，這項協議提供美國業者可以透過自我認證檢視其隱私政策是否符合安全港協議中的七項原則和其他額外要求，若是符合則得被視為符合資料保護要求，得不限數量和頻率，大量將個人資料從歐盟傳輸到該公司。此種型態的傳輸途徑更符合雲端運算產業的需求。然而在 2015 年，安全港協議被 CJEU 裁定無效。為了彌補安全港協議無效後對跨大西洋資料傳輸造成的不確定性，歐盟執委會和美國商務部積極談判新的跨境資料傳輸協議，並於 2016 年發布「歐美隱私屏障協議」。該協議通過後，許多業者便以此作為跨境資料傳輸的法律基礎。然而有了先前安全港協議的前例，隱私屏障是否真的能持續且有效的提供企業跨境資料傳輸的依據，並確保資料符合 GDPR 中高標準的保護規範值得討論。故本章將先介紹隱私屏障的內容，分別就既有原則加強以及全新的義務進行說明；接著分析新的隱私屏障協議是否得以解決原本安全港協議的問題，以及是否因此得提供跨大西洋傳輸之個人資料符合歐盟標準的隱私保護，又或是產生新的問題；最後討論隱私屏障是否得以提供雲端運算業者穩定且有效的傳輸途徑。

第一節 隱私屏障協議原則介紹

歐美隱私屏障協議於 2016 年 7 月 12 日通過，並於同年 8 月 1 日生效[231]。

[231] European Commission, *Guide to the EU-U.S. Privacy Shield*, Aug. 1, 2018,

DOI:10.6814/THE.NCCU.IB.015.2018.F06

該框架協議是為了保護所有基於商業目地，從歐盟跨境傳輸到美國之個人資料的隱私權，同時也提供進行跨大西洋資料傳輸之美國企業明確的法律規範[232]。根據歐盟執委會，該項協議加強取得歐盟個人資料的公司資料保護的義務；防止美國政府監控並取得歐盟公民的個人資料；提供有效的法律救濟和保護予個人；最後也要求歐盟和美國每年都必須要對協議進行共同檢討，以確保並修正協議內容的適用[233]。

在討論隱私屏障之資料保護原則前，希望使用隱私屏障作為跨境傳輸途徑的美國公司必須確保遵守下列基本的要求：必須採行符合隱私屏障要求之資料保護的政策和措施；必須清楚地將其符合規範的隱私政策公開於企業網站；每年都需要進行自我認證（Self-certify）以確保其隱私政策符合義務；提供歐盟公民選擇拒絕將資料傳輸給第三方的權利；確保取得歐盟公民個人資料的第三方也符合隱私屏障之義務；要在 45 天內回應歐盟公民對於隱私相關問題的控訴等。主要都是要求企業要公開隱私政策、對隱私政策進行定期的檢討並且在特定期限內回應控訴。

隱私屏障框架的 7 項基本原則和安全港協議差異不大，但每一項原則下的規範更為嚴格且具體，以達到和歐盟指令本質上相當（essentially equivalent）的資料保護水準[234]。同時隱私屏障協議為了解決原本安全港協議規範不足的部份，也新增了全新的義務[235]。下述以不同的面相介紹隱私屏障協議的規範內容：

---

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en#eu-us-privacy-shield.

232 *Id.*

233 *Id.*

234 *Id*.

235 EU Commission, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and od the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016, O.J. C(2016) 4176 (L 207/1), at Annex II, III.1-16. 共有 16 項由 DOC 發展出來的輔助原則。[hereinafter Privacy Shield adequacy decision].

DOI:10.6814/THE.NCCU.IB.015.2018.F06

1. 加強承諾：美國的公司如果要進行跨大西洋的資料傳輸，必須要遵守更嚴格的規範，主要包含：

（1） 更嚴格的通知義務，安全港協議中的通知，僅要求企業必須要通知個人關於蒐集和使用資料的目地、如果個人有疑問應該如何與組織聯繫、個人資料將會被揭露給哪些第三方，以及其選擇的權利等。但在新的隱私屏障協議中，關於通知的規範更具體，並訂有 13 項具體必須提供的資訊[236]；

（2） 資料保留的限制，安全港協議限制資料使用的目地必須要被限制在資料主體一開始同意蒐集或是後續授權的目地範圍內，而隱私屏障進一步規範企業和實體，即使其中止繼續進行自我認證，但在持續保留個人資料的期間都需要遵守隱私屏障的原則。另外，一旦當初蒐集資料的目地不再存在，就必須要將個人資料刪除[237]；

（3） 對於後續將資料傳遞給第三方遵守更嚴格的義務（stricter controls on onward transfers），並加強可責性，根據隱私屏障，企業必須要和第三方的資料控制者簽訂契約，要求第三方控制者也必須要提供資料相同程度的保護水準，且其對資料的處理必須要被限制在特定的目地範圍內。如果資料的處理必須要透過第三方的機構，則也需要和該機構簽訂符合歐盟基本資料保護原則的協定。此義務的訂定，是為了確保第三方取得個人資料後有一定的條約或契約義務要保護個人資料的隱私，如果第三方違反義務，企業必須對此負責[238]；

（4） 企業有義務要保存處理個人資料之紀錄，如果 FTC 為了調查要求相關資料，企業有義務要提供資料[239]。

---

236 *Id*., at Annex II § II.1.
237 *Id*., at ¶ 23.
238 *Id*., at ¶¶ 27-29; see also *Id*., at Annex II §§ III.3, 7(d).
239 *Id*., at ¶ 44.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

總體而言，以安全港協議 7 項必須遵守的基本原則為基礎，加強義務的範圍和規範的強度。

2. 加強執行：商務部將會加強對於義務執行的監督，包含事前對於隱私政策的驗證，以及事後依其職權針對隱私屏障清單上的企業進行定期的審查（ex officio reviews）[240]。另外，如果有和隱私屏障相關的控訴，將會由 FTC 展開調查，未能履行義務的公司將會面臨制裁或者會失去以隱私屏障作為跨大西洋資料傳輸依據的權利[241]。
3. 明確的防衛措施與透明化義務：美國司法部（Department of Justice）以及國家情報局辦公室（Office of the Director of National Intelligence）以書面的形式作出承諾，將會限制美國政府基於公共利益取得商業資料，和其他美國公司擁有之資料。同時美國和歐盟每年也會針對隱私屏障協議的執行進行共同審查，審查內容包含因為國家安全理由取得資料的議題，以及對於協議運作的定期監督。定期審查除了由歐盟執委會和美國商務部共同執行外，也會邀請美國國家情報相關專家和歐盟資料保護主管機關參與。
4. 透過幾項救濟管道，有效保護歐盟公民的權力：任何歐盟公民認為其資料隱私受到損害，得有幾項尋求救濟的管道：（1） 直接要求公司解決，該公司必須於 45 天內回應[242]；（2） 向歐盟資料保護當局提起控訴。此外，美國國務院（Department of State）也承諾會設置行政監察官（Ombudsperson）給予歐洲人民新的救濟程序，對於和情報活動有關的疑問或是控訴可以尋求此途徑尋求解答或救濟。

歐美跨境資料傳輸協議──隱私屏障在取得歐盟執委會認定為有效的傳輸途徑後，目前為跨大西洋跨境資料傳輸的主要途徑，至今共有約 3000 多家企業採

[240] *Id*., at ¶¶ 36-37.
[241] European Commission, *supra* note 231.
[242] European Commission, *supra* note 235, at ¶ 44.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

用隱私屏障作為跨境傳輸的法律基礎[243]。但隱私屏障協議的內容公布後，同樣受到一些質疑，歐盟 WP29 提出關於協議的意見書，在意見書中，工作小組認同隱私屏障對於修正安全港協議的缺點的努力和進步，但同時也認為仍然有一些疑慮需要被解決。在隱私屏障施行後一年，歐盟和美國在 2017 年 9 月 18 和 19 日針對協議進行第一次的共同審查，WP29、歐盟執委會的委員和其他專家都參與在華盛頓進行的審查[244]。審查報告中針對隱私屏障的施行情況進行檢討，WP29 雖然肯認美國主管機關為建立隱私屏障的行政程序，以使美國企業得以根據隱私屏障進行自我認證（self-certify），並真正受益於此跨境傳輸機制所作的努力，然在最終的審查報告中，WP29 仍對現在隱私屏障是否得以真正提供穩定的傳輸基礎提出幾項質疑。下一節將以第一次共同審查之報告為基礎，再加上各界對於隱私屏障施行一年來的諸多討論，分析隱私屏障協議實際的適用是否真的足以解決跨大西洋資料傳輸缺乏有效法律基礎的問題。

第二節 隱私屏障協議之適用分析

在分析隱私屏障是否得以作為跨大西洋傳輸的法律依據前，必須要先回顧 CJEU 認定安全港協議無效的判決，以了解安全港協議無效的理由，並檢視隱私屏障協議加強義務後，是否得以避免相同的問題。接著再說明除此之外，隱私屏障協議是否有其他不足之處。

第一目 CJEU 對於歐美跨境資料傳輸協議之要求

如同前述，安全港協議為在 2015 年被 CJEU 判決無效前為跨大西洋資料傳輸最主要的途徑，總共有 4,400 家美國的企業組織透過自我宣示、自我認證被

[243] *Privacy shield list*, EU PRIVACY SHIELD INFORMATION PORTAL, https://www.privacyshield.gov/list (last visited May. 30, 2018).
[244] Detlev Gabel, Robert Blamires, Tim Hickman & Matthias Goetz, *EU-US Privacy Shield approved*, WHITE & CASE, July 12, 2016, https://www.whitecase.com/publications/alert/eu-us-privacy-shield-approved.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

納入安全港協議清單，並以安全港協議作為傳輸途徑大量且持續的進行跨大西洋資料跨境傳輸[245]。然而在 2014 年，愛爾蘭國家資料保護主管機關（DPA）請求 CJEU 進行先行裁決，請求的內容為「各國 DPA 是否被要求應該要直接接受執委會的安全港決議，或者 DPA 可以自行針對美國保護機制是否提供適當的保護水準進行調查。」在 2015 年 10 月 6 日，CJEU 對此做出裁決（CJEU Schrems Decision）認為 DPA 並不受到安全港決議的拘束，可以自行進行調查[246]。另外，在此裁決中，CJEU 進一步認定執委會在 2000 年核准安全港協議時，並未做出足以證明安全港協議得提供適當且充足保護水準的調查[247]。且執委會針對安全港協議的決議中並沒有任何企圖限制美國政府干涉歐盟人民基本權利的規範，而實際上安全港協議對於美國政府的干涉也沒有任何有效的法律保護方式。Schrems 所提出侵害隱私權的案件中，所涉及的美國大規模監控計畫為美國國安局的「稜鏡」（PRISM）計畫，此項計畫首次被公開是在 2013 年 7 月的 Snowden 事件[248]。讓 NSA 和 FBI 直接進入網路服務公司的數據中心服務器，獲取音訊、視訊、圖片、電郵、文檔和通訊紀錄。CJEU 認為美國 NSA「大規模且無差別的」資料蒐集行為違反歐盟基本權利憲章中關於資料保護的規範[249]。另外，歐盟公民的隱私權如果在美國受到侵害，美國的法律制度並沒有提供有效的救濟管道，違反歐洲基本權利憲章第 47 條的要求。由上述的說明可知，CJEU 認為安全港協議不能作為跨大西洋傳輸的主要理由有二：1. 美國國防部大規模無差別的蒐集歐盟的個人資料；2. 美國法律下缺乏給予歐盟資料

---

245 *Safe Harbor list*, US DEPARTMENT OF COMMERCE SAFE HARBOR INFORMATION PORTAL, https://safeharbor.export.gov/list.aspx. (last visited Apr. 20 2018).
246 Case C-362/14, *supra* note 176.
247 David Bender, *Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective*, 6 INTERNATIONAL DATA PRIVACY LAW (May 13, 2016).
247 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. 2000 (L 215), at 7.
248 B Gellman and L Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASHINGTON POST (June 7, 2013), https://www.washingtonpost.com/ investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.accessed 20 April 2016.
249 Charter of Fundamental Rights of the European Union, 2012 O.J.(C 326/02), Oct. 26, 2012.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

保護權利受到影響的公民救濟的途徑。

第二目 隱私屏障協議是否符合 CJEU 要求之分析

為了分析歐盟之間的隱私屏障協議是否比安全港協議更「安全」，首先檢視隱私屏障協議是否得以有效阻止美國政府大規模且無差別的蒐集歐盟公民傳輸到美國的個人資料；以及是否提供隱私權受到損害的歐盟公民有效的救濟途徑，藉此了解隱私屏障協議施行後，是否得以解決 CJEU 裁定安全港協議對於隱私保護的不足之處，以分析未來隱私屏障是否可能亦被認定為無效。接著討論隱私屏障協議施行一年後是否產生其他疑慮以及解決此些疑慮的建議，以確保協議確實得作為業者跨大西洋傳輸的法律基礎。

(一)、大規模無差別監控計畫

美國政府在 2013 年史諾登事件後，對其國內情報監控相關法案做出許多修正，主要是為了讓國內關於情報和國家安全的法律架構能更加完善，同時也限制情報單位蒐集資料的行為，並增加監控計畫文件的透明度，以避免侵害個人的資料隱私[250]。其中與歐洲公民個人資料最相關的是「外國情報偵察法（Foreign Intelligence Surveillance Act, FISA）」、「總統第 28 號指令（Presidential Policy Directive 28, PPD28）[251]」，以及「第 12333 號行政命令（Executive Order 12333）[252]」。以下將分別簡述此 3 項文件的內容，並分析修正後的規範是否得以有效避免美國情報單位之監控計畫對歐洲公民隱私權的侵犯。

首先，FISA 主要授權政府在獲得法院許可的前提下，得對外國組織和個人進行一年的監視，而法案中第 702 條款允許美國國家安全局（NSA）收集和分

[250] David Bender, *supra* note 247.
[251] White House Off. of the Press Secretary, *Signals Intelligence Activities*, Pres. Pol. Dir./PPD-28 (Jan. 17 2014).
[252] Exec. Order 12333, 46 Fed. Reg. 59,941 (1981), amended by Exec. Order 13,284 (2003), Exec. Order 13,355 (2004), and Exec. Order 13,470 (2008) https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

析在海外居住的外國人的電子郵件，和其它數字通信內容─也就是所謂的「信號監控（signals intelligence）[253]」引發許多爭議。在 *Schrems* 的判決中[254]，CJEU 強調保護歐洲公民基本權利以及尊重其私生活的重要性，如果要減損或是限制保護個人資料的義務，必須嚴格的檢視其必要性[255]。同時法院也裁定如果法律允許公部門機關得在一般的情況下取得電子通訊的內容，此作法應被認為是損害保護個人隱私之基本權利，因此違反歐盟憲章第 7 條[256]。意即如果政府單位得以大規模且無差別的方式取得個人於電子通訊中的資料，應被視為違反歐盟法律。

WP29 表示，在隱私屏障協議的第一次共同審查中，美國政府強調根據第 702 條款授權的資料蒐集行為，皆僅針對特定目標，且關於篩選的條件（selector）會經過內部的檢查，確實遵守美國外國情報監控法院（Foreign Intelligence Surveillance Court）授權的範圍[257]。目前美國有兩個監控計畫─PRISM（稜鏡計畫）和 UPSTREAM（上游監控計畫）以 702 條款為法律依據[258]。有學者認為這些計畫，特別是 PRISM 計畫（PRISM 計畫為 CJEU 認定美國侵害歐盟公民隱私權的主要依據）並不會構成所謂「大規模且無差別的資料蒐集」，因為政府在執行計畫、進行電子通訊監控並蒐集相關資料時，必須要根據法院的命令採用特定的標準去過濾特定的目標資料（通常這些過濾的依據會是電話號碼或是電子信箱等），僅有經過過濾的資料會被蒐集[259]。而在訂定蒐集目標時，必須要符合有效的情報蒐集目標，並以 FISC 核准的程序進行，任何

[253] NSA 將 sigint 定義為針對外國目標透過電子信號和系統進行的監控。
[254] Case C-362/14, *supra* note 176.
[255] Case C-293/12 & C-594/12 Digital Rights Ireland and Seitlinger, Judgement of 16 May 2014, recital 52.
[256] *Id*. recital 94
[257] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 4, at 15.
[258] 根據 PRISM 計畫：美國主管機關要求網路服務提供者必須要提供符合選擇標準之使用者的資料，一旦主管機關要求，不得拒絕；根據 UPSTREAM，提供主要電信搭接幹線(Telecommunications Bonding Backbone，TBB)的服務提供者被要求要在電信傳輸的過程中協助 NSA 去辨認和蒐集符合選擇條件的資料。
[259] David Bender, *supra* note 247, at 124.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

對於這些資料的處理都必須要有合法的依據[260]。另外美國境內的獨立監察機構隱私和公民自由監督理事會（Privacy and Civil Liberties Oversight Board, PCLOB）也發布報告，認為 PRISM 對於保護美國國家安全是有效且非常有價值的作法[261]。而這項計畫的實行也會受到外部的司法機關以及內部機制的監督，而 PCLOB 也不認為實際上有任何無差別的大規模資料蒐集行為。

然而，在隱私屏障協議第一次共同審查時，WP29 認為美國目前的作法是透過設立一個篩選標準（selector）並過濾資料，僅蒐集和監控過濾後的特定目標之資料[262]。這樣的作法可能會因為篩選標準類型的不同而有造成大規模資料蒐集的可能，意即即使是針對特定目標，仍不排除會有大規模無差別的資料蒐集行為，而只要是這類型的資料蒐集都不符合比例原則[263]。在 2017 年進行隱私屏障施行的審查時，WP29 對此做出建議，因為 2017 年 12 月原本的 702 條款就會到期，在討論延期或討論新規範時，得以加入對外國人資料蒐集的額外防衛措施，例如：要求資料的蒐集必須要符合「合理懷疑」標準等。[264]然而 FISA 的修正案表決通過後，原本的 702 條款之有效期限被延長至 2023 年。故在美國境內依據 FISA 之 702 條款所為之情報監控行為，不能排除還是可能會有大規模無差別資料蒐集的行為。

另外則是第 12333 號行政命令和 PPD-28，主要是授權美國情報機構在海外進行資料外國人的情報蒐集。第 12333 號行政命令中沒有提供關於哪些資料可以被蒐集、保留或進一步散播；哪一些行為會引起監控行動，或者任何關於會被蒐集的資料或使用的細節，但仍是美國 NSA 用來進行資料監控的法律依據

[260] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, (Dec. 12, 2013) http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[261] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, (July 2, 2014) https://www.pclob.gov/library/702-Report.pdf.
[262] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 4, at 15.
[263] Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, *supra* note 3, at 39.
[264] Zakharov v. Russia, App. No. 47143/06, 4 Eur. H.R. Rep. 260 (2015).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

[265]。PPD-28 則是在史諾登事件後所發布針對美國情報機構的指令，特別是針對信號監控行為設下限制。將大規模收集數據限於 6 大國家安全目的，並且情報部門收集數據應當有明確的針對對象，此外也為授權和執行信號監控活動設立一致的標準[266]。然而 PPD-28 並非資料蒐集的具體法律依據。PPD-28 的效果必須要透過將這些原則納入監控活動的政策和程序之中[267]。且在共同審查時，WP29 認為雖然 PPD-28 已經透過 6 個國家安全目地去限制情報資料的蒐集行為，但此種「目地性」的限制還是過於廣泛，且對於這 6 個目地也沒有更詳細的說明。所以即使 PPD-28 可以作為情報機構資料蒐集的防衛措施和限制，但仍沒有消除大規模且無差別的蒐集資料的可能性，甚至資料蒐集的規模也不清楚[268]。PCLOB 應該對第 12333 號行政命令和 PPD-28 進行更進一步的分析，並發表相關報告以減少不確定性並增加可預期性。

(二)、有效之救濟管道

CJEU 判決安全港無效的另外一個主要原因是認為隱私權受到損害的歐盟公民，在美國的法律制度下並未有有效的救濟途徑。CJEU 和 ECtHR 不斷強調，個人如果有正當理由去懷疑其基本權利受到損害，應該有權利去尋求行政或司法救濟[269]。在美國的司法制度下尋求救濟有一項重要的限制，即要求個人必須要證明其具有當事人適格，提起救濟之個人必須證明該措施對其構成直接且個別的影響或損害，而該損害得以提起救濟[270]。此當事人適格的要求同樣適用於關於監控計畫的案件。然而，在情報監控計畫中，為了保持機密，不一定會將資料蒐集的行動告知個人，因此要基於監控計畫於法院提起訴訟有一定的

[265] Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, *supra* note3, at 38.
[266] 對抗美國的間諜行為、恐怖主義的威脅、對美國造成威脅的大規模毀滅性武器、網路安全威脅、對美國或同盟之人員造成威脅、跨國的犯罪。
[267] Implementing Procedures under Presidential Policy Directive-28, Signals Intelligence Activities, May 16, 2017, https://www.dni.gov/files/CLPT/documents/Chart-of-PPD-28-Procedures_May-2017.pdf.
[268] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 16.
[269] Zakharov v. Russia, *supra* note 264, at §171.
[270] Clapper v. Amnesty International, 568 U.S. 398 (2013).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

困難[271]。

為了解決歐洲公民在美國的法律制度下難以取得救濟途徑的問題，隱私屏障協議中為歐盟公民設立一個全新的救濟管道─行政監察官（Ombudsperson）[272]。行政監察官主要負責基於執行國家安全政策所進行之資料監控計畫所引發的問題，但不僅限於以隱私屏障為傳輸基礎的個人資料，如果企業是以 SCC 或 BCR 或任何減損條件的管道，傳輸資料到美國而產生相同的問題，歐洲公民同樣得向行政監察官提起行政救濟之請求[273]。整個機制運作的流程主要是歐洲公民可以向歐盟會員國國內負責處理國家安全事務監管的主管機關提起救濟的請求；該單位會先檢視請求之內容是否符合隱私屏障之規範，以及是否完整；確認後會將請求提交給美國的行政監察官，行政監察官會在進行調查後，對該請求做出回應，如果確定監控行為有違反個人權利或違法的情況，必須要對此進行補償[274]。行政監察官會和美國的其他政府機構合作以調查歐盟公民提出的控訴[275]。接著必須檢視此特殊的救濟機制是否可以視為符合歐盟憲章第 47 條的要求[276]。ECtHR 同意在一般的法院提起訴訟並非有效解決違反規範的監控行為，必須要有特殊的救濟管道[277]。另外如果是由行政機關提供之行政救濟，該機關必須獨立於進行監控行為的組織，且被授予足夠的權利和權限去執行有效和持續性的控制[278]。要確定該制度確實符合歐盟憲章第 7.8 條、47 章和 ECHR 第 8.13 條，需要檢視下列事項：

（1） 救濟機制適用範圍：所有歐盟法律適用範圍內之個人都屬於隱私屏障

[271] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 18.
[272] U.S. Department of State, *Privacy Shield Ombudsperson*, https://www.state.gov/e/privacyshield/ombud/ (last visited: June 1, 2018).
[273] *Id.*
[274] Privacy Shield adequacy decision, *supra* note 235, at Annex III, section 4.e.
[275] Privacy Shield adequacy decision, *supra* note 235, at Annex III, section 2.a.
[276] Explanations relating to the Charter of Fundamental Rights, 2007 O.J. (2007/C 303/02), Dec. 14, 2007.第 47 條要求必須要有公正的法庭提供有效的救濟。
[277] Klass and Others v. Germany, App. No. 5029/71, Eur. H.R. § 56, 67 (1978)..
[278] *Id*, at § 21, 53.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

協議保護的範圍，因為所有歐盟公民皆享有歐盟憲章所授予之基本權利，故原則上在歐盟法律適用範圍內之個人，都應得向行政監察官提起救濟。行政監察官主要負責和國家安全有關的監控行為。

（2） 提起救濟之當事人適格：因為與監控計畫相關的案件個人很難證明具體、特定和實際上的損害，因此在美國制度下很難取得當事人適格[279]。但在行政監察官救濟管道中，要提出救濟請求時，個人並不需要去證明其個人資料確實被電子監控計畫蒐集並因而受到損害[280]。

（3） 行政監察官的獨立性：歐盟憲章第 47 章和基本人權憲章對於救濟機制的獨立性和公正性之標準很高。目前行政監察官由國務院次長擔任，任命將會由總統提名參議院通過，由國務院的高級官員去擔任此項職務雖然不一定會影響其公正和獨立性，但也因此使行政監察官可能會因為官員身分而有影響。但這並不直接構成違反歐盟憲章第 47 章下獨立性和公正性的要求，在第一次隱私屏障協議共同審查時 WP29 表示，透過檢視行政監察官實際處理歐盟公民請求的情況，原則上皆合法且有效率，故可視其具有適當的獨立性和公正性[281]。

（4） 行政監察官的調查權：法院或法庭必須要有足夠的事實基礎才得以做出判決，而個人也有權了解法院判決的理由，因此法院或法庭應有權取得機密的資料。行政監察官也必須要被賦予相同的權利，以取得其做出決定所需要的資料，進而符合 CJEU 的要求。但因為目前行政監察官如何取得資訊，或是如何和其他情報單位互動的相關資料仍被視為機密，所以如果未能了解行政監察官的調查過程，很難真正了解行政監察官是否有足夠的權利去取得需要的資訊[282]。

（5） 行政監察官對違反義務行為之補償：即使行政監察官確認監控行為確

[279] Clapper v. Amnesty International USA, 568 U.S. (2013) II, 10.
[280] Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, *supra* note 3, at 48.
[281] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 19.
[282] *Id*., at 19.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

實不符合規範時得以採取何種救濟目前仍不明確[283]。行政監察官僅能認定歐洲公民所提之請求內容確實不符合規範，但目前尚未發現其亦被賦予得採取相關措施處理不符合規範行為的權力。僅基於此問題，在隱私屏障第一次的共同審查中，WP29 認為行政監察官的救濟制度尚未能被視為符合歐盟憲章第 47 章下的「有效救濟」[284]。

基於這些分析和觀點，目前的行政監察官必須要被賦予更多的權力，同時其調查及處理個人救濟請求的過程不應該被視為機密，應該要提供給各方審查，以確保行政監察官的公正和獨立性。因此雖然行政監察官機制的設立，給予受到基於國家安全目地之監控計畫影響之歐洲公民新的管道尋求救濟，然而目前尚未能證明此救濟管道是否能滿足歐盟憲章第 47 條下要求的有效的救濟管道。此些疑慮必須要立即修正以確保歐盟公民的權利不受影響。

(三)、其他問題

除了上述兩項缺失，可能會使隱私屏障協議被 CJEU 認定為不足以提供歐盟公民個人資料充足保護水準外。在第一次隱私屏障協議共同審查中，各方尤其是 WP29，更指出隱私屏障協議還存在其他問題並須要在下一次共同審查前改善。

（1） 缺乏指導和必要資訊：

DOC 發布了一份針對企業的自我認證指導，以及關於隱私屏障常問問題的回應於隱私屏障的網站上。然而該指導的資訊主要都是用於解決程序上和組織層面的疑問，對於規範要求的本質和內涵僅維持廣泛籠統的說法，缺乏對於實體義務更具體的說明與指引[285]。DOC 和 FTC 強調隱私屏

[283] Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, *supra* note 3, at 50.
[284] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 19.
[285] *Id*., at 8.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

障是一個以原則為基礎的自我認證機制，且其傾向在各項議題被提出時進行個案性的分析，而非在事前給予一個具體規範性的指導。以避免企業組織會直接「複製貼上」建議的內容，而未將個別組織的需求和特性納入考量。但 WP29 仍然認為要讓隱私屏障協議有效的施行，仍必須要提供企業實質義務的適用指導和說明，以使這些原則性的規定得正確且以一致的標準轉換成公司內部的隱私政策[286]。

（2） 人力資源的資料（HR Data）：

關於人力資源最大的疑慮是歐盟執委會和美國主管機關對於人力資源資料的解釋不同。DOC 認為只有在同一公司中進行員工的資料處理才被歸類成 HR 資料，享有在隱私屏障下額外的資料隱私防衛措施[287]。如果歐盟的公司將其員工的資料跨境傳輸到有隱私屏障認證的美國處理者，則這些資料將不會被視為是 HR 資料而是商業資料。這樣認知上的差異可能會影響隱私屏障協議的適用[288]。WP29 認為歐盟執委會應該要積極與美國主管機關進行協商，以確保企業員工的資料隱私都可以獲得高標準的保護[289]。

（3） 缺少對於企業遵守原則的監督和管理：

相較於安全港協議，隱私屏障協議在確認清單上企業是否符合義務的部份已有加強，例如：DOC 對於提出要加入隱私屏障之公司會進行事前的審查[290]。然而，WP29 認為還是應該要更進一步加強對於後續企業是否確實履行義務和遵守原則的監督，目前大部份 DOC 和 FTC 都著重在完善「認證」的程序，企業只要確定完成認證程序，一般而言主管機關都不會進行更進一步的監督和檢查，然而此現象可能會形成隱私保護的漏洞，因

286 *Id*., at 9.
287 *Id*.
288 *Id*.
289 *Id*.
290 Privacy Shield adequacy decision, *supra* note 235, at Annex 1.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

此應加強認證後的監督，例如 DOC 和 FIT 應依其職權展開調查確保自我認證的這些企業確實有執行隱私屏障的相關要求，並且對於通過認證的公司進行持續性的監督[291]。

（4） 資料處理者對於隱私屏障適用的問題：

隱私屏障中原則的設計主要是適用於得以決定資料處理目地和方法的資料控制者，舉例而言：對資料主體的通知義務，或是目地限制原則等。但資料處理者僅負責依照資料控制者的指示進行部份的資料處理，許多隱私屏障上的原則並不適用[292]。處理者可能無法提供資料主體完整的通知義務內容。然而，DOC 承認實際上在審查公司提出遵守隱私屏障的申請時，並不會特別就其控制者或處理者的身分加以區分[293]。雖然 GDPR 中有特別處理處理者和控制者義務差異的問題，但 WP29 仍呼籲美國的主管機關應該要提供針對處理者特殊情況的額外訊息和措施，以確保資料處理者也得以確實利用隱私屏障協議作為跨境傳輸的依據[294]。

（5） 缺乏資料自動化決定（automated decisions）之規定[295]：

在先前的意見書中，WP29 就有提出隱私屏障中並沒有對於會對個人產生法律影響的自動化處理提供法律上的保障。雖然根據「公平合理信用報告法（Fair Credit Reported Act）」目前仍有一些特殊的規範存在，但根據企業的回應，這些規範是否符合現實或是得以適用非常不清楚，且也不是所有的領域都可以適用此法所規範的方式[296]。因此 WP29 認為歐盟執委會

[291] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 10.
[292] *Id*., at 11.
[293] *Id*.
[294] *Id*.
[295] 資料自動化決定係指以自動化之方法取得個人資料，並根據獲取資料作出影響個人權益的評估、決定，例如以自動化之方式評估個人工作績效，並依照績效評估之好壞決定發放之薪水；或以自動化之方式評估個人之信譽，以決定是否貸款等
[296] 15 USC § 1681 et seq.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

應該要提供一些和自動化處理有關的特別規定，以確保會於所有自動化處理有關的處理行為充足的保護水準[297]。

（6） 自我認證程序以及隱私屏障機制中美國主管機關的合作

目前 DOC 已經建立了關於企業認證的審查程序，以驗證這些自我認證的企業是否符合隱私屏障協議的規範，但實際上施行的狀況仍有疑慮[298]。且現在 DOC 所建立的程序並沒有包含時間的限制，WP29 認為應該要訂定程序的時間限制，以避免對申請之企業造成不利影響[299]。

第三節 小結

根據上述的分析可知，隱私屏障協議施行一年後仍有許多問題。其中最具爭議且可能使隱私屏障面臨有效性問題的即是大規模無差別監控計畫，以及有效救濟途徑的不確定性。在安全港協議被宣告無效後，歐美政府積極談判新的隱私屏障協議希望可以提供有效且安全的傳輸途徑，讓美國企業得以安心地進行大量的跨大西洋資料傳輸並提供服務。然而，雖然美國政府在 2013 年史諾登事件後修改了很多境內情報監控相關的法律，希望減少對隱私權侵害的疑慮，但仍不足以證明此些規範的修正得以避免情報機構對於歐盟公民的個人資料進行大規模無差別的資料監控。對於 CJEU 與 WP29 而言，只要是大規模無差別的情報蒐集都是不符合比例原則，且違反歐盟基本人權憲章第 7.8 條的行為。而目前唯一提供外人情報蒐集限制和防衛機制的 PPD-28 規範不明確也不夠具體，FISA 和 EO12333 雖然會透過篩選標準去過濾特定資料蒐集之目標，但同樣缺乏具體的細節以確實避免大規模無差別的情報蒐集行為。甚至美國司法部

[297] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 10.
[298] 例如企業在提交自我認證到 DOC 進行驗證時，其隱私政策已經公開放在該企業的網站上。根據規則企業被列在隱私屏障網站清單以及美國公司將其隱私政策公開的時間應該要一致。但目前的制度是 DOC 會鼓勵提供「working link」而非個別的政策文件。
[299] EU – U.S. Privacy Shield – First annual Joint Review, *supra* note 257, at 13.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

以及國家情報局辦公室已承諾會限制資料和情報的蒐集行為，但並未見具體有效且具法律拘束力的方式，故仍不排除情報機構仍會採行違反歐洲公民基本權利的情報蒐集計畫。另外，歐盟公民非常難以證明秘密情報計畫已經或將會對其隱私權造成的損害，因此難以在美國一般的法院取得當事人適格。為了避免取得適格的困難造成歐洲基本權利憲章第 47 條賦予公民之權利受到侵害，隱私屏障協議特別為情報蒐集行為所造成的損害疑慮建立新的救濟途徑─行政監察官。但因為目前行政監察官調查程序以及與其他情報機構接觸的資料仍為機密文件，未能提供各界檢視，其獨立性和公正性仍有疑慮。此外，行政監察官在認定情報機構的資料蒐集行為確實違反規範後是否有權得以提供補償或救濟也不確定，故行政監察官目前不能被認為符合基本權利憲章第 47 條中所謂有要的救濟途徑。

在隱私屏障通過後，愛爾蘭的隱私保護組織愛爾蘭數位權利（Digital Rights Ireland, DRI）」向歐盟的普通法院提出控訴，主張隱私屏障協議未能提供歐盟人民適當的隱私權保護，違反歐盟基本權利憲章[300]。雖然最後法院於 2017 年 12 月駁回其控訴，認為 DRI 不具有提出控訴之當事人適格[301]。主要原因是身為隱私保護組織 DRI 並不具有個人資料也並非資料主體，再加上也非隱私屏障主要適用的美國組織，因此基本上 DRI 在隱私屏障協議中並沒有任何受到損害的權利以及義務，故其不具有當事人適格[302]。然而，雖然 DRI 的控訴並未成功，但法院並未就隱私屏障的質內容進行審查，但目前有另外一個由法國的隱私倡議組織 La Quadrature du Net 領導的非營利組織團體提出同樣針對隱私屏障協議有效性的控訴，目前正在審理中，雖然此案件和 DRI 的案件一樣都是由組織提出的控訴，是否會面臨和 DRI 同樣未能取得當事人適格而遭駁回的問題目

300 Case T-670/16, Digital Rights Ireland v Commission, Action brought on 16 September 2016.
301 ORDER OF THE GENERAL COURT (Second Chamber) http://curia.europa.eu/juris/document/document.jsf?text=&docid=197141&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=838174
302 *Id*.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

前尚未能得知[303]。即使如此，目前隱私屏障協議的內容仍有諸多問題不排除未來還會有更多個人或組織提出相似的有效性控訴，根據上述之分析，現在的隱私屏障協議的內容很難符合 CJEU 對於歐洲公民個人資料隱私保護，以及有效救濟途徑的要求。歐盟執委會和美國主管機關應該積極處理此些問題以避免協議未來被判決無效的風險，而造成企業的損失。

[303] Case T-738/16, La Quadrature du Net and Others v Commission, Action brought on 25 October 2016.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

第六章 結論與建議

近年來雲端運算產業快速發展，透過將資料傳輸到遠端由雲端服務提供者進行處理或儲存，可以為企業帶來降低成本的效益，同時也刺激市場上的創新。然而大量使用資料和遠端設施的產業型態也造成許多不確定性和風險，其中最具爭議性的問題是對於個人資料隱私的危害。對於雲端運算產業而言，資料的跨境傳輸為提供服務不可或缺的條件。然而根據歐盟 1995 年指令與近期生效 GDPR，唯有在第三國的資料保護法律體系與歐盟提供「本質上相當」的保護才得視為有充足的保護水準，並得以進行跨境資料傳輸。如果未能取得適足性的認定，則僅得在符合特定要件之下例外進行傳輸。美國雲端業者針對例外的規定，發展出資料主體同意、SCC、BCR 等跨境傳輸途徑。但連同 GDPR 下的新途徑─DPA 條款、行為準則與認證制度，現有的制度根據本文的分析都未能提供雲端運算產業有效的法律基礎進行跨境資料傳輸。因此美國商務部與歐盟執委會另外發展出──隱私屏障，作為跨大西洋資料傳輸的折衷辦法。雖然隱私屏障在適用上仍有諸多問題，特別是仍未能防止政府大規模無差別的資料蒐集行為，以及未能提供有效的救濟途徑。但此折衷辦法的訂定和規範內容亦得作為我國未來與歐盟之間就跨境資料傳輸議題進行協商的參考與示範。

在 GDPR 生效後，我國雲端運算產業業者同樣也會遇到相同的跨境資料傳輸問題。以資料主體同意、SCC 和 BCR 作為跨境傳輸的途徑，同樣使我國業者在提供雲端運算相關服務時面臨許多挑戰。基於雲端運算大量且重複進行資料傳輸的特性，執委會之適足性認定與跨境資料傳輸協議為較可行之傳輸途徑，有利於我國數位經濟與雲端運算產業發展。作為 GDPR 與我國個資法主管機關的國家發展委員會已於今（2018）年 5 月 26 日前往歐盟總部拜訪，並表達將爭取歐盟執委會適足性認定之意願。根據 GDPR 之規範與 CJEU 之見解，要取得適足性的認定，我國的個資法必須要提供與歐 GDPR 本質上相同之保護水

DOI:10.6814/THE.NCCU.IB.015.2018.F06

準。目前根據法務部針對 GDPR 與我國個資法的比較分析可知，我國個資法的規範仍有不足，例如：我國個資法並未包含 GDPR 新增的「資料可攜帶權」；另外我國的資料保護系採用分散式的管理制度，並非由一獨立機構專職處理個人資料保護相關議題；我國個資法並未有個資外洩後 72 小時的通知義務等[304]。這些法規上的落差可能會影響我國取得適足性認定的可能性。故本文認為若我國欲取得歐盟之適足性認定，必須主管機關─國發會確實針對個資法進行全面性的盤點，並將 GDPR 第 45 條所揭示適足性認定應考量之標準作為參考，修正個資法以符合歐盟 GDPR 所要求的充足資料保護水準。

另外，除了修改我國個資法外，爭取與歐盟簽訂跨境資料傳輸協議亦為可方向。目前我國主要爭取的方向是取得適足性的認定，但如果最後未能成功，跨境資料傳輸協議作為一折衷辦法亦得提供雲端業者有效的傳輸途徑。跨境資料傳輸協議的本質在於透過企業每年的自我認證，以確保符合 GDPR 之義務，一旦成為協議清單所認可之企業，該企業及得大量不限次數的進行資料跨境資料傳輸，比起其他資料主體同意、SCC 和 BCR 等方法都更具可行性。且歐美之間的隱私屏障協議中所揭示的 7 項基本原則得作為我國協商的參考依據。

歐盟為我國第五大貿易夥伴，進入歐盟市場對我國業者而言事關重要。歐盟司法總署在我國積極表達爭取適足性認定之意願後，建議我方參考以公布之相關文件，先針對我國個資保護整體的架構進行自我評估，並將該報告送交歐盟，雙方得展開技術性對話，以解決法規上之落差。故為求我國業者之利益，國發會應如前述，進行資料規範的盤點，以作為日後對話之基礎。

304 法務部，「歐盟資料保護一般規則（General Data Protection Regulation, GDPR）與我國個人資料保護法之重點比較分析」，https://www.ndc.gov.tw/Content_List.aspx?n=92A54D2FBC1D329E。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

參考文獻

中文文獻

劉定基，「雲端運算與個人資料保護－－以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心」，東海大學法學研究，頁 53-106。

翁逸泓，「OTT 發展之隱私與個人資料保護問題初探」，世新大學法學院，頁 25-85。

孫鈺婷，「歐美跨境資料傳輸新框架－－從歐美安全港協議無效談起」，科技法律透析，第 28 卷第 7 期，頁 22-30。

孫鈺婷，「準備好了嗎？歐盟一般資料保護規則施行進入倒數計時」，科技法律透析，第 28 卷第 4 期，頁 6-8。

林俊宏，「數位化時代個人資料隱私之問題」，月旦法學教室，總號：55，頁 92-103。

劉靜怡，「之十一：資訊隱私權保護的國際化爭議─從個人資料保護體制的規範協調到國際貿易規範的適用」，月旦法學雜誌，總號：86，頁 195-205。

陳俐伶，「歐美針對跨大西洋資料之流動達成新架構性協議」，經貿法訊，第 192 期，頁 1-3。

DOI:10.6814/THE.NCCU.IB.015.2018.F06

英文文獻

書籍

CHRISTOPHER KUNER, INTERNATIONAL REGULATION OF TRANSBORDER DATA FLOWS (2016).

PAUL M. SCHWARTZ AND DANIEL SOLOVE, PRIVACY LAW FUNDAMENTALS (2011).

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW (Alan Charles Raul et al. 4th ed. 2017)

期刊

Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 Mich. St. Int'l L. Rev. (2013).

David Bender, *Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective*, 6 INTERNATIONAL DATA PRIVACY LAW (May 13, 2016).

WK Hon and C Millard, *Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4*, 9 SCRIPT-ed (2012).

Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 79, WASHINGTON AND LEE LAW REVIEW, 341(2013).

Mantelero, A, *Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution*, 3 EUROPEAN JOURNAL FOR LAW AND TECHNOLOGY (2012).

Sean Marston, *Cloud Computing —Business Perspective*, 51, DECISION SUPPORT SYSTEMS, 176(Apr., 2011).

Justice Opara-Martins, Reza Sahandi & Feng Tian, *Critical Analysis of Vendor Lock-in and Its Impact on Cloud Computing Migration: A Business Perspective*, JOURNAL OF CLOUD COMPUTING ADVANCES, SYSTEMS AND APPLICATIONS, (Apr. 15, 2016).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

Judith Rauhofer & Caspar Bowden, *Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud*, EDINBURGH SCHOOL OF LAW RESEARCH PAPER (June 21, 2013)

Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593 (2010).

Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, BERKELEY LAW 1974 (May 2013).

Marina Škrinjar Vidović, *EU Data Protection Reform: Challenges for Cloud Computing*, 12 CROATIAN YEARBOOK OF EUROPEAN LAW & POLICY 171 (2016).

P Swire and Y Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72(2) MARYLAND LAW REVIEW 335 (2013).

Mark Webber, *The GDPR' impact on the cloud service provider as a processor*, 16 PRIVACY & DATA PROTECTION JOURNAL 12 (March, 2016).

Legal Challenges against Privacy Shield Begin to Mount in Europe, Inside US Trade, Vol.34, No.43, Nov.3, 2016.

機構報告

Cloud Standards Customer Council, *Public Cloud Service Agreements: What to Expect and What to Negotiate Version 2.0.1.*, Aug. 2016, http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf.

ENISA, *The Right to Be Forgotten – Between Expectations and Practice,* Oct. 18, 2011, www.enisa.europa.eu/publications/the-right-to-be-forgotten.

ITA, *2016 Top Markets Report Cloud Computing,* Apr., 2016, https://www.trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.

Kommerskollegium, *Swedish National Board of Trade. How Borderless is the Cloud？: An Introduction to cloud computing and international trade*. Sept., 2012.

OECD, *Cloud Computing: The Concept, Impacts and the Role of Government Policy*, OECD Doc. DSTI/ICCP(2011)19/FINAL, (Aug. 19, 2014).

DOI:10.6814/THE.NCCU.IB.015.2018.F06

官方文件

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final, Sept. 27, 2012.

Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, July 26, 2000, C(2000) 2441, 2000/520/EC.

Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, O.J. (L 181), July 4, 2001.

Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, O.J. (L 6), Jan. 10, 2002.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. 2000 (L 215).

Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, 2000 O.J. (L296/41).

European Telecommunications Standards Institute, *Cloud Standards in the Digital Single Market*, Cloud Standard Coordination, Jan. 28, 2016, http://csc.etsi.org/.

EU – U.S. Privacy Shield – First annual Joint Review, Nov. 28, 2017, WP255, 17/EN.

European Commission, *Guide to the EU-U.S. Privacy Shield*, Aug. 1, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en#eu-us-privacy-shield.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

European Commission, *Right environment for digital networks and services*, May 16, 2017, https://ec.europa.eu/digital-single-market/en/environment-digital-single-market.

Explanatory Document on the Processor Binding Corporate Rules, Apr. 19, 2013, WP204, 00658/13/EN.

Guidelines on the right to data portability, Dec.13, 2016, WP242 rev.01, 16/EN.

Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government, Jan. 26, 1999, WP 15, 5092/98.

Opinion 1/2010 on the concepts of "controller" and "processor", Feb. 16, 2010, WP29, 00264/10/EN.

Opinion 05/2012 on Cloud Computing, July 1, 2012, WP196, 01037/12/EN.

Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Sept. 22, 2015, WP232, 2588/15/EN.

Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, Apr. 13, 2016, WP238, 16/EN.

Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, Sep,. 2011, *available at*: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, (July 2, 2014) https://www.pclob.gov/library/702-Report.pdf.

Recommendation 1/2007 on the Standard Application for the Approval of Binding Corporate Rules for the Transfer of Personal Data, Jan. 10, 2017, WP133.

Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, Apr. 14, 2005, WP108, 05/EN.

Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Nov. 25, 2005, WP114, 2093/05/EN.

Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, June 24, 2008, WP153, 18/EN.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

Working Document Setting up a framework for the structure of Binding Corporate Rules, June 24, 2008, WP154, 1271-00-01/08/EN.

判決文件

Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, Judgement of 6 October.

Case T-670/16, Digital Rights Ireland v Commission, Action brought on 16 September 2016.

Case C-293/12 & C-594/12 Digital Rights Ireland and Seitlinger, Judgement of 16 May 2014.

Case T-738/16, La Quadrature du Net and Others v Commission, Action brought on 25 October.

Clapper v. Amnesty International USA, 568 U.S. (2013) II, 10.

Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, [2016] No. 4809 (H. Ct.) (lr.).

Klass and Others v. Germany, App. No. 5029/71, Eur. H.R. § 56, 67 (1978).

Zakharov v. Russia, App. No. 47143/06, 4 Eur. H.R. Rep. 260 (2015).

網頁資料

Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica & Matei Zaharia, *Above the Clouds: A Berkeley View of Cloud Computing*, at 8, Feb. 10, 2009.

P. Chase, S. David-Wilp & T. Ridout,*Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies*, 2016, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

Louis Colunbus, *Roundup of Cloud Computing Forecasts*, 2017, Forbes, Apr. 29, 2017, https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#5135867031e8.

Barb Darrow, *Amazon Still Leads Cloud Rankings, But Competition Is Coming on Strong*, Fortune, June 15, 2017, http://fortune.com/2017/06/15/gartner-cloud-rankings/.

Ron Davies, *Cloud Computing : An Overview of economic and policy issues*, May 2016, http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf.

Deloitte, *Measuring the economic impact of cloud computing in Europe*, at 56, Jan.10, 2017 https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe.

EU Cloud Code of Conduct Version 2.0, EU Cloud CoC Information Portal, May, 2018 https://eucoc.cloud/fileadmin/cloudcoc/files/European_Cloud_Code_of_Conduct.pdf.

EU Cloud Code of Conduct Version 2.0, EU Cloud CoC Information Portal, May, 2018 https://eucoc.cloud/fileadmin/cloud-coc/files/European_Cloud_Code_of_Conduct.pdf.

London Economics, *Implications of the European Commission's Proposal for a General Data Protection Regulation for Business*, May 2013, https://ico.org.uk/media/1042341/implications-european commissions-proposal-general-data-protection-regulation-for-business.pdf.

GDPR Portal: Site Overview, EU GDPR Information Portal, https://www.eugdpr.org/.

GDPR Key Changes, EU GDPR Information Portal, https://www.eugdpr.org/key-changes.html.

Detlev Gabel &Tim Hickman, *Chapter 10: Obligations of controllers – Unlocking the EU General Data Protection Regulation*, White& Case, Sept. 13, 2017, https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection.

DOI:10.6814/THE.NCCU.IB.015.2018.F06

Detlev Gabel &Tim Hickman, *Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation*, White& Case, Jul. 22, 2016, https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection.

Detlev Gabel, Robert Blamires, Tim Hickman & Matthias Goetz, *EU-US Privacy Shield approved*, White & Case, July 12, 2016, https://www.whitecase.com/publications/alert/eu-us-privacy-shield-approved.

B Gellman and L Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Washington Post (June 7, 2013), https://www.washingtonpost.com/ investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.accessed 20 April 2016.

John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RES. CTR., Sept. 12, 2008, http://pewresearch.org/pubs/948/cloud-computing-gains-incurrency.

Vivek Kundra, *Federal Cloud Computing Strategy*, Feb. 8, 2011, https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.

Privacy shield list, EU Privacy shield Information Portal, https://www.privacyshield.gov/list.

V. Reading, *Binding Corporate Rules: Unleashing the Potential of the Digital Single Market and Cloud Computing*, Nov. 29, 2011, at 4, file:///C:/Users/lorra/Downloads/SPEECH-11-817_EN.pdf.

U.S. Department of Commerce, *Safe Harbor Privacy Principles and Related Frequently Asked Questions*, July 21, 2000.

Darrell M. West, *Saving Money Through Cloud Computing*, Apr. 7, 2010, https://www.brookings.edu/wp-content/uploads/2016/06/0407_cloud_computing_west.pdf.

DOI:10.6814/THE.NCCU.IB.015.2018.F06