國立政治大學國際經營與貿易學系研究所

碩士學位論文

# GDPR 跨境傳輸例外規範與 WTO 規範下 GATS 之合致性分析

# The Legal Analysis of GDPR Cross-Border Data Transfer Exception Regulation under GATS of WTO

指導教授：薛景文 博士

研究生：張安潔 撰

中 華 民 國 109 年 1 月

DOI:10.6814/NCCU202000087

# 謝辭

在法組的日子向前看時，總覺得時間很漫長，此時回頭又覺得時光飛逝，每天寫電子報、後期每天與 GDPR 為伍的日子今天要結束了，這是一趟充滿挑戰、恩典與收穫的旅程。

寫論文的路上特別感謝我的指導教授— 薛景文老師。當初在找題目的時候，抱持著單純的好奇跟興趣跟老師說想寫 GDPR 相關的議題，就這樣一頭栽進 GDPR 的世界。找題目跟定架構的過程中，面對未知跟龐大的資訊，跌跌撞撞又茫然，感謝薛老師總是很有耐心跟親切的引導。在論文撰寫的過程老師也給我很大的彈性，總是亦師亦友給予指導跟幫助，沒有老師的話我是無法完成這篇論文的。同時也非常感謝口試委員楊培侃老師跟張兆恬老師，在口試時非常用心仔細給予建議跟指正，讓我對於 GDPR 研究議題的面向有更深廣的了解，在修改論文上也非常有幫助。

在法組的日子也非常感謝四位老師：楊光華老師、施文真老師、楊培侃老師及薛景文老師的教導，讓我在學習貿法的過程中，理論與實務兼備、紮實豐富，一窺貿法浩瀚的世界。法組最讓人難忘的電子報撰寫過程，感謝老師們不遺餘力地指導，深深影響我對於研究應實事求是、追根究底的精神。

兩年半經歷許多挑戰、走過許多高山低谷，感謝爸爸、媽媽、弟弟跟 Joy，我的家人永遠是最堅實的支持與後盾，當我對自己失去信心，謝謝你們總是對我有信心。感謝一路上陪伴我的朋友們，不論是在政大認識的還是一直在身邊的人們，這條走的不容易的路上，你們總是像及時雨出現，與我同甘共苦、陪我度過難關。

在政大的這趟冒險旅程讓我得以看到過去未以得見的視野與經歷，感謝神帶領我走這條我未曾想像過的旅程，讓我經歷詩篇 23 篇的恩典。何處有不安與恐懼，祢就在何處成為我的勇氣與信心，使我仍然能勇敢地向前奔跑。

DOI:10.6814/NCCU202000087

# 摘要

2018 年歐盟一般資料保護規則（General Data Protection Regulation，GDPR）正式實施為資料保護規範立下重要的里程碑。資料保護的範圍擴及到網路上的使用軌跡，強調資料主體擁有其資料的主權、資料控制者及處理者須嚴謹遵守其義務，除此之外， GDPR 原則上禁止了將歐盟境內資料傳輸到境外，僅允許幾種特定的例外條款。此規定使得 GDPR 不僅對資料保護的發展帶來革新，也對國際貿易的規範帶來衝擊與影響。

大數據時代的興起使得「資料」（Data）成為極具價值的資產，因為網路使得跨國的商業貿易突破地理界線的障礙，可以輕易地觸及跨國消費者。消費者在網路上所產生的資料，企業透過跨境蒐集與處理可以進行行銷分析，是商業發展重要的根據。然而 GDPR 原則上禁止跨境傳輸之規定，直接衝擊到在歐盟進行商業活動的企業，因此引發各界質疑該規範是否是以資料保護之名，行貿易障礙之實。本文聚焦於探討 GDPR 跨境傳輸的三種例外允許：國家適足性認定、適當保護措施以及資料主體同意是否實質上是難以通過的窄門，違反 WTO 最惠國待遇、國民待遇及相互承認等規範。

本文透過整理法規及相關官方條文解釋文件，將歐盟的資料保護法制與背景，GDPR 中關於資料的定義、資料主體及資料控制處理者之權利義務，以及跨境傳輸的原則及各項例外允許規範進行說明，以輔助後續合致性分析。同時本文以文獻回顧之研究方法，整理歸納各界學者探討 GDPR 跨境傳輸與 WTO 貿易法可能的潛在衝突及看法。本文藉由整理歸納 WTO 過往最惠國待遇、國民待遇及相互承認的案例以分析例外允許規範是否有違反 WTO 規範。整體而言，例外允許規範並沒有實質上違反 WTO 規範，並確實有許多國家及企業藉此進行跨境傳輸。惟其仍有值得改進之處，因為縱然其規範沒有違反 WTO 義務，其在申請的程序上多耗時且所費不貲，且追求與 GDPR 相當的資料保護程度，仍可能不利於中小企以及資料保護規範尚在發展中的國家。

關鍵字：GDPR、GATS、資料保護規範、跨境資料傳輸

DOI:10.6814/NCCU202000087

# Abstract

The adoption of General Data Protection Regulation in the European Union in 2018 is an important milestone for data protection regulations. The scope of data protection has been extended to the trajectory of use on the Internet, emphasizing that data subjects have sovereignty over their data, thus indicating data controllers and processors must strictly abide by their obligations. Furthermore, GDPR prohibits the cross-border transfer of data from EU to other countries with only a few specific exceptions. Hence, GDPR not only provides a new perspective to the development of data protection but also exert significant impact on the regulation of international trade.

The rise of the era of big data makes "data" a very valuable asset because the Internet enables transnational commercial trade to break through the barriers of geographical boundaries and can easily reach multinational consumers. The data generated by consumers on the Internet can be analyzed by companies through cross-border collection and processing, which is an important basis for business development. However, the principle that the GDPR prohibits cross-border transmission in principle directly impacts companies doing business in the European Union, which has led to questions from all walks of life whether the norm is a barrier to trade in the name of data protection. This article focuses on the three exceptions to GDPR cross-border data transfers: Adequacy Decision, appropriate protection measures, and whether the data subject agrees that it is essentially a narrow gate that is difficult to pass, a violation of WTO most-favored-nation treatment, national treatment, and mutual recognition and other specifications.

This paper analyzes the consistency of the exceptions of cross-border data transfers under GATS regulation especially in most favored nation treatment, national treatment, and mutual recognition. Overall, the exception regulations did not substantially violate the WTO regulations. However, further improvement is needed, due to its time-consuming and expensive application process, and also the requirement of data protection meeting the standard of GDPR may be cause negative impact to SMEs and developing countries.

Key Words: GDPR, GATS, Data protection regulation, Cross-border data transfers



**DOI:10.6814/NCCU202000087**

# 目錄



DOI:10.6814/NCCU202000087

## 表目錄





DOI:10.6814/NCCU202000087

# 第一章 緒論

數位時代下，「資料」（Data）成為非常寶貴的資產，企業可以透過蒐集、處理、傳輸客戶的資料了解消費者行為，消費者藉由允許企業使用、處理其資料，進行數位的貿易及買賣以獲得更好的消費體驗。數位貿易的時代因著資料自由流通，得以實現國界障礙與成本更低的自由貿易，然資料自由流通與處理也帶來許多資料隱私安全的隱憂，社群軟體龍頭 Facebook 2018 年被揭露在 2014 年不正當的將 5000 多萬的用戶資料給劍橋分析（Cambridge Analytical）使用便是近期最受到關注的事件[1]。各國對於資料保護的意識抬頭，然而 WTO 的服務貿易規範 GATS 仍然維持著 20 年前的內容，使得各國趨向以國內法保障國內人民的資料安全，歐盟的一般資料保護規則（General Data Protection Regulation, GDPR）即是先驅。在 GDPR 通過之後，近乎域外適用的跨境傳輸規範又引起各界質疑是否有 GATS 違反最惠國待遇、國民待遇等重要的國際貿易規範原則。各國及企業為了避免在歐盟市場進行商業活動時，違反 GDPR 的規範而遭課高額罰款，紛紛依循 GDPR 的資料保護原則修改國內的資料保護法規或企業的資料隱私保護政策。GDPR 的誕生，讓資料隱私的保護與國際貿易規範之間的議題被廣泛討論[2]，同時也成為新的資料保護指引準則，帶動各界改革資料保護的規範與政策，因此 GDPR 的跨境傳輸規範對國際數位貿易的市場與規範帶來何種影響值得研究。

## 第一節 研究動機與目的

20 年間網路科技的發展改變了國際貿易的型態，不論是貨品還是服務貿易無不邁向數位化。網路在許多方面都具有巨大的經濟實力和潛力，首先，網路使市場在網路上整合並且全球化，為企業和消費者提供新的機會[3]。其次，網路

[1] Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, THE NEW YORK TIME (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline.

[2] Jan Philipp Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. L. REV. 288, 287-289 (2016).

[3] Meltzer, Joshua, *The Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & THE PACIFIC POLICY STUDIES 90, 90-102 (2013).



DOI:10.6814/NCCU202000087

是創新和生產力增長的關鍵驅動力，因為它降低了交易成本，並使企業能夠更有效地利用現有資源[4]。網路加速了服務型態的創新，諸如 Facebook 的社交網站託管用戶生成的內容並促進社交和業務聯繫[5]。亞馬遜、蘋果和 eBay 等公司已成功利用網路生成了電子商務和行動應用程式平台，以連接各地的買賣雙方[6]。誰持有「用戶數據」或「資料」成了兵家必爭之地，企業無不希望蒐集越多用戶資訊，以進行處理跟分析。而另一方面，資料主體，也就是資料的擁有者意識到資料與隱私的關聯，開始爭取資料保有的權利。

2018 年 5 月 24 日，GDPR 正式實施，為國際社會的隱私保護及數位貿易規範畫下新的里程碑。GDPR 適用於與歐盟領土上所有相關的個人資料處理活動，無關資料控制者、處理者是否是隸屬歐盟的公司或是否位於歐盟。GDPR 成為史上規範最嚴格的資料保護法，如果違反規範將處以高達全球每年營業額 4%或最高 2000 萬歐元的罰則[7]。所有歐盟境內的資料保護機構（資料保護主管機關）都必須執行這些制裁，這些資料保護機構擁有廣泛的任務和權力。新設立的歐洲資料保護委員會（European Data Protection Board, EDPB）可以強制任何成員國的資料保護機構採取、更改或撤回某項措施。從 GDPR 實施起，歐盟原先分散的數位市場以及缺乏執法的資料保護規範將終止，GDPR 成為歐盟統一和直接適用的資料保護法，取代幾乎所有現有成員國的規定，並且不必經由轉換，直接適用於企業、個人、法院和政府。

GDPR 所帶來的影響最重要的，不僅是它怎麼改變歐盟的資料保護法，更是至關重要的是，GDPR 怎樣改變了整個世界。自從歐洲議會和理事會於 2015 年 12 月達成協議以來，已經可以看到它對市場和商業戰略的影響。許多公司已決定將遵守 GDPR 作為其在管理層面的關鍵任務之一，甚至正在改變他們的經營策略，以成為重視資料保護產品和服務的領導品牌。即便這個新的標準尚未實施，歐盟標準的隱私、安全及資料保護已經成了發展中的貿易標誌，這些提

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] 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, 2016 O.J. (L 119), art. 83(4)(5) [hereinafter GDPR].



DOI:10.6814/NCCU202000087

早準備的公司在2018年5月24日規則正式實施後，就具備了一個重要的優勢。因為從那一刻起，資料保護原則和規則不僅在整個歐洲市場上有一致性的嚴厲制裁標準，也將成為往後每項新創新的全球黃金標準，為贏得消費者對資料運用技術的信任，以及進入新興數位市場的基本門檻。

在實質規範上，GDPR 帶來比以往更多的法律確定性和連貫性。在這個沒有公司不想在數位市場上佔有一席地位、並且使用來自世界各地的網路服務的時代，原先歐洲市場 28 個不同的法律體系及和執法文化所建構的資料保護規範，會造成大量的官僚主義和法律上的不確定性[8]。因此單一框架的法律體制，包含為歐洲市場上所有公司帶來公平競爭環境，無論是對於企業還是消費者都是非常正面的影響[9]。此外，通過嚴格實施問責制原則取代之前的資料保護主管機關通知，減少了公司不必要的繁文縟節。為了提高對消費者的控制權並使他們的同意再次有意義，引入若干提高透明度和簡化信息政策的規定至關重要。新的創新概念，如資料可攜帶性、標準化隱私標示以及設計和默認的資料保護，為資料保護和消費者友善產品和服務方面的創新和競爭提供了廣闊的機會。基於風險的方法適用於重要規定，如違規通知，資料保護影響評估或資料保護官員的任命，為企業帶來了合理的方法，但也有效保護了未來數位生態圈中資料保護的基本權利。

從 GDPR 通過之後，歐盟為了維護對資料保護的主要法律義務，歐盟法院明確表示，沒有人能夠規避歐盟對個人資料的高度保護標準。在歐洲法院判決中也看得到 GDPR 的延續，特別是關於 Google 跟西班牙之間關於遺忘權的訴訟，以及 Facebook 跟愛爾蘭之間關於安全港的案件。支持市場定位原則的明確決定以及對國際資料傳輸的嚴格措辭，是過去十年矽谷和其他地區不斷增長的網路經濟中潛在問題的結果。

GDPR 現在設定了一個標準，該標準是世界上最大的單一市場明確的聲明。沒有資料控制者能夠忽視這一點，其他政府將面臨提高其資料保護標準的壓力，

[8] Jan Philipp Albrecht, *supra* note 2, at 287-289.
[9] *Id.*



DOI:10.6814/NCCU202000087

以使其經濟體能夠進入歐盟的數位單一市場。GDPR 所立下的標準與規則也漸漸影響國際間對隱私保護的革新。日本已經通過國家適足性的認定，與歐盟的資料保護水準達到相當的程度，讓日本歐盟間得以跨境傳輸[10]；英國企業正在盡最大努力確保即使在實際脫歐後 GDPR 仍然適用。在修訂歐洲理事會第 108 號公約（Council of Europe's Convention 108）的過程中，GDPR 將把它的足跡留在歐盟的鄰國或甚至國外。

雖然 GDPR 在隱私保護的規範畫下時代性的里程碑，但仍然有來自不同領域的爭議與顧慮，其中國際貿易的角度出發，看 GDPR 中以原則上禁止來規範跨境傳輸資料，質疑其強化保障歐盟公民的隱私權的同時，是否可以解釋為構成一種貿易障礙？現今的興起對數位資料隱私權的重視的同時，對國際貿易而言因著網路科技、跨境電商的蓬勃發展，也提高了在國際貿易中資料「跨境傳輸」的重要性。為了強化保障歐盟公民的隱私權益，因而誕生了歐盟一般資料保護規則，規則內容對於資料的控制、處理方式設下嚴謹的規範，並且受保護的資料種類也囊括了數位使用紀錄等新興的資料類型，最值得關注的是，GDPR 針對跨境傳輸採取「原則上禁止」的規範，這無疑將為從事國際貿易的公司及產業帶來重大的挑戰。

## 第二節 研究架構

本文旨在分析 GDPR 提供第三國可自由跨境傳輸歐盟資料的例外允許，是否可能違反 GATS 的規範。在第二章將首先介紹歐盟資料保護規範的沿革，以了解資料隱私權在歐盟被視為基本人權的法律基礎，從 OECD 的隱私權原則到 GDPR 的前身 1995 年資料保護指令，得以了解 GDPR 生成的歷史背景脈絡。接著，將針對 GDPR 的規範進行說明，包含 GDPR 地域的適用範圍、資料主體的主要權利、資料控制者的義務、取得資料主體同意的規範，以及本文主要探討的規範核心：跨境傳輸的原則與例外允許。之所以將跨境傳輸規範之外的規範一併說明，是為了提供之後在分析跨境傳輸規範有更完整的法規架構背景，跨

[10] 日本取得歐盟 GDPR 例外適足性認定，台灣經貿網，2019 年 1 月 24 日，https://reurl.cc/ObKN6g（最後瀏覽日：2020 年 1 月 13 日）。



DOI:10.6814/NCCU202000087

境傳輸規範同時也與前述的規範息息相關。第二章在介紹完資料保護沿革的脈絡，以及 GDPR 的規範內容之後，將點出跨境傳輸的例外允許：國家適足性認定、適當保護措施及同意與 WTO 的 GATS 規範可能衝突的部分，而進一步的分析將會在第三章進行。

在第三章將會分析本文主要想要探討的議題，即 GDPR 的跨境傳輸例外條款，是否有違反 GATS 的最惠國待遇、國民待遇或相互承認的可能。GDPR 以禁止跨境傳輸為原則，並另外從第 47 條到 49 條設立例外允許的條款，其中國家適足性認定、適當保護措施以及同意是企業及歐盟外的第三國最廣泛受討論的，因此本文將以這三類例外條款作為主要分析的對象。在架構的編排上會以 GATS 的規範（最惠國待遇、國民待遇及相互承認）為主軸，分別先說明該規範的條文內容及要件，以及相關的專家小組、上訴機構判決意見，接著試析國家適足性認定、適當保護措施以及同意是否有違反之虞。最後做一結論於第四章。本文希望能透過以清楚的脈絡介紹歐盟資料保護規範的沿革以及 GDPR 規範，檢驗 GDPR 跨境傳輸的例外條款與 GATS 規範之間的合致性分析，試圖了解數位貿易時代下，國際規範與國家規範之間的衝突與可能解決之道。

## 第三節 研究方法

本文主要透過文獻回顧法整理相關文獻，並進行 GDPR 規範的內容以及 GATS 規範之間的合致性分析。在歐盟資料保護規範沿革，以及 GDPR 規範的部分，由於 GDPR 在法規立法的過程中，歷經許多歐盟政府不同機關之間正反面的意見，以及在 GDPR 通過後法規仍有許多模糊的解釋空間，因此歐盟亦有發布針對不同部分規範的指導文件（Guideline），因此在這部分本文將主要整理歐盟政府機關文件，歸納歐盟機關在立法過程中不同的立場與聲音，以及歐盟針對規範有解釋爭議的部分做出的進一步說明，以輔助本文在介紹及解釋規範上更為完整。在探討跨境傳輸規範與 GATS 之間的衝突部分，即便歐盟針對跨境傳輸的原則禁止提出例外允許，該等例外允許是否有違反 WTO 規範之爭議討論甚多，同時 GATS 規範在數位貿易時代中的困境也隨之被多方討論，因此本文將整理歸納國內外官方機構及學者的意見，以了解各界對於 GDPR 在跨境



DOI:10.6814/NCCU202000087

傳輸上近乎域外適用的規範，與無法跟上科技改變服務型態腳步的 GATS 規範之間的看法。在 GATS 的規範上歸納相關的 WTO 判決，了解專家小組與上訴機構對相關的規範要件解釋，試析跨境傳輸例外規範的合致性。





DOI:10.6814/NCCU202000087

# 第二章 歐盟資料保護法制沿革及 GDPR 規範

本章將針對歐盟資料保護法規的沿革，以及 GDPR 的規範內容進行說明介紹。從 1980 年代便能在法規文字中體現歐盟將資料隱私權利視為「基本人權」的觀念，使得歐洲各國長久以來都非常重要隱私權的保障。從 1995 年的資料保護「指令」（Directive），到現今的歐盟一般資料保護「規則」（Regulation），指令到規則的法律位階提升，更加強化了歐盟對歐洲各國的資料保護規範的影響，歐洲各國必須直接適用 GDPR 的規範內容。GDPR 除了在法律位階上提升之外，在規範內容上也強化了資料主體的權利與資料控制者的義務，為要實現將資料的主權回歸資料主體。透過介紹法規沿革及 GDPR 規範，得以提供更完整的分析背景知識。

## 第一節　法制沿革與背景

**OECD 八大隱私保護原則**

在國際層級的隱私規範中，OECD 隱私保護原則是各國隱私規範的重要參考指標。即便既有資料保護相關的法律與規範有許多地方需要更新，但在既有的資料保護規範中，有許多原則仍然被後進的法規所遵守。正如 GDPR 跟 1995 年的資料保護指令在制定上，仍舊遵守經濟合作與發展組織（Organization for Economic Co-operation and Development, OECD）於 1980 年所公布了一項名為保護隱私與跨境傳輸個人資料的隱私指導原則中，所提及的八大隱私保護原則[11]。在 1980 年，由美國、日本和歐洲國家所組成的 OECD，公布了此隱私指導原則，成為了世界各國最廣泛認可的實務參考。此八大原則分別為：資料蒐集限制原則、資料品質原則、目的特定原則、使用限制原則、安全防護原則、開放原則、資料主體參與原則、義務原則，介紹如下。

1. 限制蒐集原則（Collection Limitation Principle）：強調個人資料的蒐集應受

[11] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).



DOI:10.6814/NCCU202000087

到限制，並且要在公平合法的情況下被取得，同時以適當的方式來取得資料主體的同意[12]。

2. 資料品質原則（Data Quality Principle）：個人資料的內容應與蒐集的目的有關，或是符合其使用目的而產生的必要性，個人資料的內容必須確保正確與完整性，並且及時地更新[13]。
3. 目的明確原則（Purpose Specification Principle）：個人資料的蒐集目的，必須在開始蒐集時即明確指出，隨後在利用這些個人資料時，也必須限制在目的之內，日後若需要變更時，更要明確指出其變更後的利用目的為何[14]。
4. 利用限制原則（Use Limitation Principle）：個人資料不應在指定目的之外被揭露或利用，除非已事先獲得資料主體的同意或有相關法律授權[15]。
5. 安全措施原則（Security Safeguards Principle）：針對個人資料可能發生遺失、不當存取、使用、修改、損毀及揭露的風險，應採取相對適當的安全控制措施，以降低可能的風險[16]。
6. 公開原則（Openness Principle）：對於個人資料的發展、實務和政策的制定，應依據公開的原則來進行，針對個人資料持有的種類和使用目的，以及資料控制者的連絡方式，應公開並且易於讓資料主體知悉[17]。
7. 個人參與原則（Individual Participation Principle）：個人資料的資料主體，應保有以下的權利：(a)有權利向資料控制者或持有之組織，確認是否保有和其有關的個人資料；(b)在合理的時間和費用範圍內，以合理的方式和可了解的形式，向組織查詢和其有關的個人資料；(c)針對所提出的查詢或主張的權利若遭到拒絕時，可以提出異議要求說明；(d)若所提出的異議成立時，可要求組織刪除、變更、修改、補充其個人資料[18]。
8. 責任原則（Accountability Principle）：個資的控制者必須負起相關責任，並要求落實以上提到的各項隱私保護原則[19]。

[12] *Id.* ¶ 7.
[13] *Id.* ¶ 8.
[14] *Id.* ¶ 9.
[15] *Id.* ¶ 10.
[16] *Id.* ¶ 11.
[17] *Id.* ¶ 12.
[18] *Id.* ¶ 13.
[19] *Id.* ¶ 14.



DOI:10.6814/NCCU202000087

**1995 年資料保護指令**

在 1995 年 10 月 24 日之前，歐盟當時的隱私法規尚未有統一的規範，當時頒布的資料保護指令是歐盟對當時破碎的歐盟隱私法規的解答 [20]。其主要目標包括統一資料保護法以及將個人資料轉移到歐盟以外的國家，即所謂的第三國。資料保護指令在每個成員國建立了稱為資料保護機構（Data Protection Authorities, DPA）的獨立機構，作為監督該指令的適用，並與企業和公民互動的監管機構。資料保護指令還規定允許將個人資料轉移到第三國，條件是第三國被授權對資料提供足夠的保護，以保證移轉出去的個人資料在第三國受到與歐盟內部相當程度的保護。該指令仍堅守 OECD 原本的建議，並且以隱私作為一項基本人權的核心概念。

**歐盟一般資料保護規則（GDPR）**

儘管 1995 年資料保護指令旨在將不同成員國的法律整合在一起，但其在歐盟的法律層級上，是指令層級的法律，歐盟成員國在轉換將其轉換為個別國家法律時留下了一些解釋空間。這一事實，加上當今迅速變化的數據資料格局，導致歐盟需要對其資料的監管環境進行另一次更新，因此誕生了 GDPR。

GDPR 的誕生在立法層次上是一個更大規模的立法，其作為一項規則而非指令，意味者它直接對所有成員國和歐盟資料主體執行的法律。關於隱私的主要原則仍然適用於以前的指令和 OECD 原則，然而社群媒體和雲端儲存在 1995 年並不存在，因為當時只有約 1%的歐洲人在使用網路。而現今的時代，人們借助現代技術創造了比以往更多的個人資料，並且這些資料的處理已經無處不在。因此 GDPR 旨在適應當今的技術，同時保持一般性，以保護未來創新浪潮中的個人基本權利。

歐盟執委會於 2012 年初提出 GDPR 的草案中，其實可以看出歐盟對於此次的修法工程非常有野心，歐盟不但在修正幅度上全面性的檢討既有規範內容，

[20] 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) [hereinafter Directive 1995].



DOI:10.6814/NCCU202000087

且原先在修法時程上，原本是預計在2014年完成立法，並在2016年正式實施。然而在實際修法過程中遇到非常多爭議，各方意見分歧，直到2012年底，歐洲議會公民自由、司法與內政委員會（European Parliament Committee on Civil Liberties, Justice and Home Affairs）方才通過對於執委會版草案之修正意見[21]。在2015年底，歐盟執委會、議會與理事會（European Council）持續進行三方協商討論，才獲致共識並提出歐盟個資規則之三方協議版草案，並於2016年4月27日通過，同年5月4日正式公布[22]。

在修法過程中，許多機關都有提出意見書，包含區域委員會（Committee of the Regions）[23]、歐盟經濟與社會委員會（European Economic and Social Committee）[24]、歐盟資料保護監督機關（European Data Protection Supervisor）等。其中歐盟資料保護監督機關提到，大數據為社會與個人不論是在健康上、科學研究上、環境上都帶來極大的益處，但同時在處理資料的過程中對於個人的權利、自由甚至是隱私都帶來實際上、潛在性的影響，因此需要建立更新的資料保護規範，強化歸責（accountability）以及隱私權設計（privacy by design）、隱私權預設（privacy by default）的原則[25]。歐盟資料保護監督機關在意見書中點出，為負責且永續的發展大數據技術，必須秉持四大原則，同時這四原則也是GDPR立法宗旨[26]。第一，組織在其處理個人資料的過程上，必須更加透明[27]。意即，資料處理透明的程度必須足以讓資料主體了解有何種資料被處理、處理的目的為何，甚至是運用在處理其個人資料的演算法，都必須

[21] Draft Report on the Proposal For A Regulation of The European Parliament and of the Council on the Protection of Individual With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM(2012)0011–C7-0025/2012–2012/0011(COD)), EUR PARL. DOC. PE501.927V02 (2012).

[22] GDPR, at 1.

[23] Opinion of the Committee of the Regions on 'Data protection package', Dec. 18, 2012, 2012 O.J. (C391)127, p. 127–133.

[24] Opinion of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final, 2012/011 (COD), July 31, 2012, 2012 O.J. (C 229)/17, p.90- 97.

[25] Executive Summary of the Opinion of the European Data Protection Supervisor on 'Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability', Feb. 20, 2016, 2016 O.J. (C67)13, p. 13–15.

[26] *Id.*

[27] *Id.*



DOI:10.6814/NCCU202000087

要讓資料主體知道[28]。第二，要賦予資料主體對其資料有更大的控制權，這將賦予個人更大的權利偵測不公平的資料演算結果、挑戰錯誤[29]。對使用者而言有力的使用權限、資料攜帶性以及有效的選擇退出機制可以作為允許使用者更多地控制其資料的實踐方式，並且還可以有助於開發新的商業模式以及更有效和透明地使用個人資料[30]。第三，產品及服務從設計階段就必須將資料保護納入設計考量，且必須是以使用者友善為標準[31]。透過強化系統功能，讓資料主體更容易接近（access）資料，也容易操作撤回其對資料處理的同意[32]。最後透過從系統和處理程序的設計中建立資料保護，並調整數據保護以實現更真實的透明度和使用者控制，資料處理的行為在歸責上更加明確，資料控制者也將能夠受益於大數據的優勢，同時確保個人的尊嚴和自由受到尊重[33]。



[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*



DOI:10.6814/NCCU202000087

## 第二節　GDPR 規範介紹

GDPR 規範中，跟 1995 年資料保護指令最大不同的之處，可以分為五大部分。第一，GDPR 所適用的「地域」範圍擴大，GDPR 不僅對歐盟境內的組織與個人有效，歐盟境外但是有控制或處理歐盟公民資料者亦受規範。第二，資料主體之權利被強化，GDPR 強調讓資料的主權回到資料主體的手中，資料主體有權可以決定資料是否要被處理、如何處理，亦可以要求資料控制者與處理者更正、刪除或遺忘其資料。第三，強化資料控制者、處理者之義務，資料控制者、處理者被要求需要更清楚的向資料主體說明資料處理的位置、目的及方式，且必須用簡單明瞭的語意告知，並且讓資料主體能行使其應有的權利。第四，GDPR 強調了資料主體「同意」的重要性，所謂同意必須要資料主體明示且明確的表示，且同意的範圍只限縮在特定資料處理目的。最後，也是 GDPR 最嚴格也影響最大的規範，資料的跨境傳輸原則上禁止、以例外允許，組織或個人若要合法的資料從歐盟內傳送到境外，需要符合 GDPR 規定的適當保護措施。上述五大規範的重點，以下詳述之。

### 第一目 GDPR 的地域適用範圍

GDPR 第 3 條規範，即使是位於歐盟境外的機構，在一定條件下處理歐盟境內當事人個資，也會落入 GDPR 的適用範圍 [34]。此舉擴大歐盟資料保護法體系的適用範圍，是 GDPR 帶來的主要改變之一。根據 GDPR 規範內容，若滿足特定條件，非歐盟事業機構也需要肩負 GDPR 的義務，惟相關的條件卻規定得相當模糊，以致於有解釋的必要 [35]。EDPB 於 2019 年 11 月 12 日針對這些模糊的條文用語應如何被理解，發布一份指引 [36]。

[34] GDPR, art.3.
[35] *Id.*
[36] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.0, Adopted on12 November 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf [hereinafter Article 3 Guidelines].



DOI:10.6814/NCCU202000087

一、「據點」之認定標準

根據 GDPR 第 3 條第 1 項的規定，不論該資料處理地是否位於歐盟境內，歐盟境內資料控制者（controller）或處理者（processor）之據點（establishment）業務中所進行之個人資料處理，皆落入 GDPR 的適用範圍 [37]。委員會建議一種「三重法（threefold approach）」，逐案認定各相關資料處理活動是否落入 GDPR 第 3 條的範圍內 [38]。

所謂據點指透過穩定安排（stable arrangements）有效且實際地執行業務，無關乎其法律型態為何，例如子公司、分公司或辦事處 [39]。根據指引草案，在某些情況下，即使在境內的是非歐盟機構的單一員工或代理人，只要其行為具有一定程度的穩定性，即足以建立所謂的穩定安排 [40]。故即便負責處理特定資料的非歐盟機構在歐盟沒有分公司或子公司，亦不妨礙其構成 GDPR 定義下的據點 [41]。

即使非歐盟機構於歐盟境內的據點在資料處理中，未實際擔任任何角色，其行為也可能與此等資料處理行為密不可分 [42]。根據指引草案，假如是為了使非歐盟機構提供的服務更有利可圖，其歐盟境內據點對歐盟市場執行潛在客戶之開發與行銷活動，就可能屬於此情形 [43]。

判定 GDPR 適用的地域範圍時，對於資料控制者或處理者的據點，或非歐盟的資料控制者或處理者之商業據點地理所在位置是重要的，但資料處理地卻不然 [44]。非歐盟機構對歐盟境內資料處理者之指示，並不會因此使其自動受 GDPR 管制，但歐盟的資料處理者和非歐盟的資料控制者間需簽訂資料處理協議 [45]。不論該非歐盟機構是否位於歐盟境內，歐盟的資料處理者仍有義務簽訂

[37] GDPR, art. 3.1.
[38] Article 3 Guidelines, at 4.
[39] GDPR, recital 22.
[40] Article 3 Guidelines, at 5.
[41] *Id.*
[42] *Id*. at 6.
[43] *Id.* at 7.
[44] *Id*. at 8, 9.
[45] *Id*. at 10.



DOI:10.6814/NCCU202000087

此類協議，即使是與歐盟境外的資料控制者[46]。

二、「針對性」之認定標準

未在歐盟境內設有據點的資料控制者或處理者，不必然意謂其得被排除於GDPR的地域適用範圍外[47]。GDPR更進一步規定，非歐盟境內的資料控制者或資料處理者在處理歐盟境內當事人的個資時，只要與下列兩類行為相關，仍適用 GDPR[48]：（1）向當事人提供貨品或服務，無論是否要求當事人支付費用；或者（2）監測當事人在歐盟境內的行為。

評估當事人是否位於歐盟境內的標準，為相關行為發生的時點，如提供貨品或服務，或其行為被監測的時候，至於提供或監測的時間長短在所不問[49]。此外，無論是提供貨品或服務或監測個人的行為，對歐盟境內的個人一定要具有針對性（targeting）的要素[50]。只要資料處理並非針對歐盟境內特定個人，也非監測其在歐盟境內之行為，則在歐盟外之第三國處理歐盟公民或居民之個資並不適用 GDPR[51]。

首先，執委會認為資料處理行為與貨品或服務的提供之間，需要有直接或間接的關聯[52]。其次，委員會也確認僅是其網站得自歐盟進入之事實，本身並未提供充份的證據足以顯示資料控制者或處理者有意對歐盟境內當事人提供貨品或服務[53]。

在判斷上是否對歐盟境內當事人提供貨品或服務，判斷時可考慮以下因素[54]：（一）歐盟或至少一個成員國被指名是貨品或服務可能提供的對象；（二）資料控制者或處理者向搜索引擎營運者支付網路參考服務費用，以便有助於歐

[46] *Id*. at 11.
[47] *Id*. at 12.
[48] GDPR, art. 3.2.
[49] Article 3 Guidelines, at 13.
[50] *Id*. at 14.
[51] *Id*.
[52] *Id*. at 15.
[53] *Id*.
[54] *Id*. at 15, 16.



DOI:10.6814/NCCU202000087

盟的消費者訪問其網站；（三）資料控制者或處理者已針對歐盟會員國目標客群發起行銷和廣告活動；（四）業務具有國際性質，例如特定旅遊活動；（五）提及得自歐盟地區聯繫的專用地址或電話號碼；（六）使用不同於資料控制者或處理者所在之第三國的頂級網域名稱，例如「.at」（奧地利的頂級網域名稱）或使用中性頂級網域名稱，例如「.eu」（歐盟的頂級網域名稱）；（七）從一個或多個歐盟成員國到服務提供地之路線指示；（八）提及包含定居於歐盟成員國內的國際客戶，特別是有這些客戶的經驗分享及意見回饋；（九）使用非貿易商所屬國家通常使用的語言或貨幣，尤其是使用一個或多個歐盟成員國的語言或貨幣；或（十）提供在歐盟成員國內交付貨物的服務。

根據指引草案，使用「監測」一詞意謂資料控制者在蒐集歐盟境內個人行為的相關資料和後續再使用上是有特定目的，因此委員會並不認為任何在網路上蒐集或分析歐盟境內個資之行為都會自動落入「監測」的定義中[55]。根據指引草案，有必要考慮資料控制者處理資料的目的，特別是後續任何涉及該資料的行為分析或特徵側寫技術；不過委員會認為透過使用 cookie 或其他追蹤技術如指紋識別，以及地理定位行為（特別是為了行銷目的），正是屬於這種監測行為[56]。綜上所述，如果網站是歐盟居民可及者，則僅是在網站上使用 cookie 是否一定會落入 GDPR 適用範圍，似乎並不清楚。

三、指定代表人

設在歐盟境外的資料控制者及處理者，只有該當上述「針對性」要件時，才有義務指定其在歐盟境內的代表人（representative）[57]。此代表人可以是自然人、商業機構或非商業機構，且必須設立在其提供服務或貨品，或進行監測行為的歐盟成員國境內[58]。固然非歐盟機構有一定程度的自由得選擇於何歐盟成員國境內設置代表人，但不可或忘的是該代表人必須讓當事人及其他成員國（即非代表人設置地）的監管機關容易聯絡，尤其在聯繫上必須以監管機關和

[55] *Id*. at 18.
[56] *Id*.
[57] *Id*. at 19.
[58] *Id*. at 20.



DOI:10.6814/NCCU202000087

相關當事人使用的一種或多種語言進行[59]。此外，指引草案認為該代表的職能與對外資料保護長（Data Protection Officer）的角色並不相容，因此被指定之代表人不能同時被同一機構指派為資料保護長[60]。

委員會更進一步指出，之所以導入代表人之概念，係意圖使執法者能夠對代表人採取與對資料控制者或處理者相同的執行處分[61]。委員會的看法亦表示這將包括可能對代表施以罰鍰或其他行政罰，並使代表人承擔直接責任[62]。然而這樣的見解無法自 GDPR 的規範推導而得；相反地，GDPR 第 58 條明確規定監督機關可以直接對代表人採取的唯一處分，就是命令該代表人提供機關監督所需的資訊[63]。所有其他相關的執法權力（包括加諸行政罰）及 GDPR 的責任制度皆僅針對資料控制者和（或）處理者[64]。因此，委員會認為能對代表施以罰鍰的可能性和承擔責任的看法在 GDPR 中是沒有依據的。

## 第二目 資料主體之權利

資料主體的權利根據 GDPR 的規範，資料主體對其個人資料有查閱權、更正權、被遺忘權、限制處理權及資料可攜帶權，並且 GDPR 擴張了對於個人資料的定義範圍。

### 一、資料之定義

在 GDPR 中所定義的個人資料為，任何可以辨識或可能可以辨識自然人之資訊，稱為個人資料[65]。廣義而言，任何可以辨識自然人，不論直接或間接者，特別例如姓名、身分證字號、地點位置、數位辨識、或一個或多個特定識別物理性、心理性、基因、心理狀態、經濟、文化或社交之因素，皆屬於個人資料。在網路上，個人資料可以多樣的方式及管道被蒐集，包含廣告活動、使用社群

[59] *Id*. at 20, 21, 23.
[60] *Id*. at 20, 21.
[61] *Id*. at 23.
[62] *Id*.
[63] GDPR, art. 58.
[64] Article 3 Guidelines, at 23; GDPR, arts. 83, 84.
[65] GDPR, art 4.1.



DOI:10.6814/NCCU202000087

網站、瀏覽網頁的紀錄，甚至是智慧型手機顯示的位置[66]。除了直接蒐集的方法之外，個人資料亦可以透過間接的方式被蒐集，例如透過蒐集並分析非個人資料，進而推斷並產生個人資料[67]。

二、資料接近使用權（Right of access）

資料主體可以要求查閱、閱覽、複製資料控制者或處理者是否蒐集或處理其資料、蒐集目的、個資種類等，並且當資料被傳遞到第三國時，資料主體亦有權知道資料控制者所採取的適當安全措施、資料預計抱存時間等資訊[68]。在理由第 63 點中，立法者更建議在可行的情況下，資料控制者應使資料主體能從遠端透過安全的查詢系統（remote access to a secured system)直接查詢其個人資料[69]。資料主體亦有權要求資料控制者更正有誤之個人資料，除非有公共利益之目的、學術或歷史研究目的或統計目的之考量下，且具必要性，才得限制資料主體之權利[70]。

三、刪除權/遺忘權（Right to Erasure / Right to be Forgotten）

在 GDPR 規範中資料主體權利與之前指令最大差異之處，在於資料主體除了可以主張刪除其資料之外，可以在網路世界向搜尋引擎要求遺忘其資料。被遺忘權的發展其實在資料保護指令中就已經有初步的概念，在指令第 12 條中，要求各會員國應確保資料主體於資料控制者為遵循指令處理個人資料時，得要求資料控制者更正、刪除或限制資料之使用[71]。在 2012 年歐盟執委會及議會所提出的 GDPR 草案中，也更深入著默被遺忘權的規範。然而關於被遺忘權最具重要性的討論，是發生在 2014 年的 *Google v. Spain* 案，被遺忘權首次被深入的討論在資料保護上作為基本權利發展的意涵[72]。被遺忘權之主張與原先存在的

[66] Article 3 Guidelines, at 23.
[67] *Id.*
[68] GDPR, art. 15.
[69] GDPR, recitals 63.
[70] GDPR, art. 15.5 (b).
[71] Directive, art. 12.
[72] Judgment of the Court (Grand Chamber), 13 May 2014.Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Request for a preliminary ruling from the Audiencia Nacional. Personal data — Protection of individuals with regard to the processing of



DOI:10.6814/NCCU202000087

刪除權之主張的差別在於：被遺忘權主張於刪除搜尋結果之「連結」，而非搜尋結果所連結之「資訊」[73]。

四、限制處理權（Right to Restriction of Processing）

除了被遺忘權之外，GDPR 也將限制處理權獨立於刪除權之外。資料主體若不想主張刪除權或被遺忘權，則可以主張第 18 條的限制處理權，要求資料控制者跟處理者限制對其個人資料之處理。限制權適用的情況包含：資料正確性有疑慮；處理不合法；資料之處理對於處理目的之達成無必要；針對資料處理有異議時，資料主體得主張限制處理其資料[74]。

四、資料可攜帶權 （Right to Data Portability）

最後，GDPR 強化了資料主體對其個人資料的控制能力，即所謂資料可攜帶權[75]。使資料主體在移轉其個人資料，而不受資料控制者的限制，例如資料主體欲轉換電子信箱的系統，其有權自由的將原先電子信箱中的個人資料，移轉到另一個電子信箱系統。資料主體在行使資料可攜帶權時，可要求資料控制者以有組織的、常用的之格式提供其個人資料之副本，以降低在不同的資料系統或社群網站間轉換資料的困難度[76]。



such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8. Case C-131/12.[hereinafter *Google v. Spain*]

[73] *Google v. Spain*, ¶ 94.

[74] GDPR, art.18.

[75] GDPR, art.20.

[76] *Id.*



DOI:10.6814/NCCU202000087

## 第三目 資料控制者、處理者之義務

GDPR 對資料控制者跟處理者的義務重點包含：擴大對資料主體告知義務的範圍跟方式、在個資外洩的情況下通知的義務，以及新增資料保護影響評估。

### 一、告知義務

在 GDPR 的告知義務中，讓資料主體清楚容易了解重要資訊是告知義務核心的修法宗旨[77]。這個原因在於，許多資料蒐集或處理的資訊對一般人來說非常艱深難懂，縱然資料控制者或處理者有說明其資料的處理目的跟方式，資料主體並不一定能全然理解。在無法理解或獲得充分資訊的情況下，資料主體也無法全然行使其原本應有的權利。因此在 GDPR 第 13 條中，強調資料控制者或處理在傳遞重要資訊（例如資料處理目的或方式等）給資料主體時，應簡潔、清楚處易懂、具有可接近性，並使用淺白詞語，特別在向兒童告知的時候也需要遵守此規定。在 GDPR 的草案階段曾經有提出，在告知的時候需使用圖像化或標準化的告知方式，為的也是方便閱讀者可以更容易吸收理解重要資訊[78]。

需要告知的資訊也根據重要性跟蒐集方式分為兩階段的告知方式：資料控制者在蒐集資料的同時，就必須告知的「基本告知事項」與為了確保資料蒐集、處理的公平與透明的「進階告知事項」，分別以下表說明之。

表 1、資料控制者之資料蒐集告知義務

| 直接或間接蒐集之情況 | |
|---|---|
| 基本告知事項<br><br>（第 13 條第 1 項、第 14 條第 1 項） | • 資料蒐集者的名稱及聯絡方式<br>• 資料保護專責人員聯絡方式（如有適用）<br>• 蒐集資料的目的及合法事由<br>• 蒐集時的合法利益<br>• 個人資料的收受者或其類別<br>• 資料控制者是否會將資料傳輸至第三國與歐盟執委會針對該第三國資料安全程度所做的決定 |

[77] GDPR, recital 39; GDPR, art. 12,13.
[78] GDPR draft, art. 13a.



DOI:10.6814/NCCU202000087

| | |
|---|---|
| 進階告知事項<br><br>（第 13 條第 2 項、第 14 條第 2 項） | • 個人資料保存期限或其決定標準<br>• 資料主體相關權利<br>• 資料主體得隨時撤回其同意<br>• 當事人向監督機關提出申訴之權利<br>• 提供資料是否是基於法律規定或契約要求或締結契約所必須、當事人是否得自由選擇提供個人資料及不提供對其權益的影響<br>• 是否存在自動化決定（automated decision-making），包括資料剖析（profiling），與自動化決定的邏輯與對當事人可能的影響 |

二、通知義務

當個資外洩時，資料控制者需分別對監督機關跟資料主體履行通知義務[79]。根據 GDPR 第 33 條第 1 項規定：「當個人資料外洩，資料控制者應避免不當遲延（without undue delay），並在可能的情形下（where feasible），於知悉（become aware of）事件發生後 72 小時內，通知第 55 條規定所定的監督機關。但個資外洩不至於（unlikely）對自然人自由與權利產生危險者，不在此限。通知未能於 72 小時內為之者，資料管理者於通知時應說明理由。」除了向監督機關通知之外，資料控制者還需要向資料被外洩的資料主體通知，根據 GDPR 第 34 條第 1 項規定，當個人資料的外洩可能自然人自由或權利的高度風險時，資料控制者需要避免不當拖延，將資料外洩之情事通知資料主體，且通知方式應以清楚淺白之文字描述。但如果有下列三項事由，則資料控制者可以不需向資料主體通知資料外洩之情事[80]：

- 資料控制者對於外洩的個人資料已採取適當地技術及組織上保護措施，例如：加密，使未經授權者，無法理解資料的內容。
- 資料控制者在事發後採取措施，使第 1 項所稱資料主體自由或權利的高度風險不至於實現。
- 個別通知須付出不合比例的努力（disproportionate effort），資料控制者應採取公告或其他類似措施，使資料主體以相同有效的方式知悉通知內容。

[79] GDPR, art. 33.1.
[80] GDPR, art. 34.3.



DOI:10.6814/NCCU202000087

資料控制者在向監督機關跟資料主體履行通知義務所需要通知的資訊，整理於下表[81]。

表 2、通知義務所需通知之資訊

| 通知對象 | 需通知之資訊 |
| --- | --- |
| 監督機關、資料主體 | • 資料保護專責人員或其他聯絡窗口的姓名及聯絡方式<br>• 描述個人資料外洩可能的影響<br>• 描述資料管理者已經採取或即將採取的因應措施，包括減輕或緩和個人資料外洩可能造成不利影響的作法 |
| 監督機關 | • 個資外洩事件本質的描述，包括受影響當事人之種類及其大略人數，以及外洩個人資料的種類及大略數量 |

## 第四目 同意之規範

在 GDPR 中規範關於同意之內容，要求企業所取得之同意須是資料主體基於其意思，透過聲明或明確肯定之行動，所為之自主（freely given）、具體（specific）、知情（informed）及明確表示之同意（unambiguous indication of the data subject's wishes）[82]。此外 GDPR 在第 8 條中亦對於取得兒童之同意有特別的規範，除了條文本身外，歐盟資料保護工作小組（Article 29 Data Protection Working Party, 以下簡稱工作小組）亦有進一步對於同意規範進行解釋[83]。本段將先介紹同意規範的內容，再進一步介紹兒童同意規範的要件與內容。

### 一、同意權規範的內容

GDPR 的核心目標是加強和協調個人資料保護，其規範不僅包含企業應如何處理、儲存和保護識別性個人資料之新規定，更包含罰款之懲罰性規定，以

[81] GDPR, art. 33.3, 34.3.
[82] *Id.* art. 4(11).
[83] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, as Last Revised and Adopted on 10 April 2018, WP259 rev. 01 [hereinafter Consent Guidelines].



DOI:10.6814/NCCU202000087

確保企業遵循 GDPR 之規範[84]。如若未遵循 GDPR 之規範，將可能面臨高達 2000 萬歐元的罰款，或如為企業者，其可能面臨最高達前一會計年度全球年度營業額 4%之罰款，並以較高者為準[85]。根據 GDPR 第 4 條第 11 項之規定，所謂資料主體之「同意」，係指資料主體基於其意思，透過聲明或明確肯定之行為，所為自主性具體、知情及明確之表示同意處理與其有關之個人資料[86]。以下將就同意的定義分述之。

自主性意味著對資料主體的真正選擇和控制[87]。作為一般規則，GDPR 規定資料主體在沒有真正的選擇權、被迫同意，或如果不同意將會承受負面後果的情況下，所作成之同意無效[88]。如果該同意中含有不可商議之條件與條款的部分，則推定資料主體並非為自主地表示同意[89]。因此，如果資料主體無法在被侵害的情況下拒絕或撤回其同意，則該同意並非自主同意，由此可知，GDPR 將資料控制者與資料主體之間是否處於對等的平衡關係納入考量[90]。此外，評估是否自主地給予同意時，還應考慮將同意納入契約中，或提供 GDPR 第 7 條第 4 項之規定中所述服務的具體情況[91]。故一般而言，任何對資料主體施加不當壓力或影響的因素，阻止資料主體行使其自由意志，該同意應皆視為無效[92]。

GDPR 第 6 條第 1 項第 a 款[93]確認資料主體的同意必須是針對一個或多個特定（specific）目的處理其個人資料，使資料主體可以對每個目的進行選擇，並確保資料處理的透明度[94]。GDPR 沒有改變這一要求，並且與知情同意的要求

---

[84] Jesper Zerlang, *GDPR: A Milestone in Convergence for Cybersecurity and Compliance*, 2017(6) NETWORK SECURITY 8, 8 (2017).
[85] GDPR, art. 83.
[86] *Id.* art. 4(11).
[87] Consent Guidelines, at 5.
[88] *Id.*
[89] *Id.*
[90] *Id.*; GDPR, art. 7(4).
[91] Consent Guidelines, at 5; GDPR, art. 7(4).
[92] Consent Guidelines, at 5; GDPR, art. 7(4).
[93] GDPR, art. 6(1)(a).
[94] Consent Guidelines, at 11.



DOI:10.6814/NCCU202000087

密切相關[95]。同時，必須按照詳盡（granularity）的要求來解釋，以獲得自主地同意[96]。為了符合「特定」這項要件，資料控制者必須[97]：具體化說明其使用目的，以避免挪用作其他目的之使用（purpose specification as a safeguard against function creep）、同意請求詳盡化，以及明確化獲得資料處理同意之相關資訊。

GDPR 強調同意必須係在資料主體已經知情的前提下取得[98]。為使資料主體在知情同意下作決定，以及理解其同意之內容，例如行使撤回的權利，資料控制者於獲得同意前提供相關資訊是非常重要的[99]。倘若資料控制者未提供相關資訊，猶如虛應故事一般地設置同意機制，而導致使用者同意之操作並非實際的同意，其個資處理之同意也將是無效的[100]。

GDPR 清楚地要求同意需要資料主體的陳述或明確的肯定行為，這意味著資料主體的同意必須以積極的行為或意思表示為之，且必須明顯同意具體特定的資料處理[101]。在歐盟資料保護指令第 2 條第 h 項中規定，同意係指資料主體表示其同意處理與其有關的個人資料的意願，而 GDPR 第 4 條第 11 項條以此定義為基礎，規定有效同意需要通過意思表示或明確的肯定行為[102]。

明確的肯定行為（clear affirmative act）意味著資料主體必須慎重地同意特定資料處理[103]。同意可以通過書面或記錄的口頭陳述蒐集，包括透過電子的方式，在不違反各國既存之契約法下，可以透過記錄的口頭陳述行使同意，但在徵得同意前必須注意資料主體可獲得之資訊，因為預設已勾選之選項框在 GDPR 規範下是無效的[104]。而資料主體之默示與不作為，即僅持續使用該服務，

[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.* at 12.
[99] *Id.* at 13.
[100] *Id.*
[101] *Id.* at 15.
[102] Consent Guidelines, at 15; GDPR, art. 4(11); Directive 95/46/EC, art. 2(h).
[103] Consent Guidelines, at 16.
[104] *Id.*



DOI:10.6814/NCCU202000087

皆不視為主動之意思表示[105]。

資料控制者尚須注意，不能將「同意契約」和「接受所有一般條款和條件」一併視為獲得資料主體之同意，因為一般條款和條件的概括承諾不能被視為同意使用個人資料的明確肯定行為[106]。GDPR 不允許資料控制者提供已預設勾選之選項框或選擇退出之機制，這些選項框需要資料主體的干預才能防止達成協議，例如選擇退出鍵[107]。如資料主體之同意係基於電子方式之請求者，該請求必須清楚、簡潔，且不應對服務之使用造成不必要的中斷，資料主體必須以積極的作為表示同意[108]。在 GDPR 合理範圍內，資料控制者可以自由地制定符合其企業的同意流程，在這樣的情況下，資料主體之實際操作即視為明確的肯定行為[109]。

資料控制者應設計得以讓資料主體清楚明瞭的同意機制，確保資料主體明白資料使用之目的，必須避免含糊不清，意即確保同意內容之下的使用行為，和其他非同意內容之下的使用行為有所區隔[110]。僅僅持續使用網站並不是一種明確的肯定行為，因為該行為無從推斷資料主體對處理操作之明確意思表示[111]。

二、兒童同意權規範

在資料處理方面，與歐盟原本的資料保護指令相比，對於較弱勢之自然人，特別是兒童，GDPR 創建了一個額外保護層[112]。GDPR 第 8 條納入了額外的義務，以確保提高兒童在資訊社會服務方面的資料保護水準[113]。GDPR 增強保護兒童的原因在於，兒童可能不太了解相關的風險、後果和保護措施及使用者處理個人資料有關的權利[114]。根據 GDPR 第 38 號釋義指出，此特殊保護應特別適

105 *Id.*
106 *Id.*
107 *Id.*
108 *Id.*
109 *Id.* at 17.
110 *Id.*
111 *Id.*
112 *Id.* at 23.
113 *Id.*; GDPR, art. 8.
114 Consent Guidelines, at 23.



DOI:10.6814/NCCU202000087

用於兒童個人資料的使用，以用於行銷或建立用戶檔案等特定目的，以及在使用直接向兒童提供的服務時，蒐集相關兒童個人資料之情況[115]。

根據 GDPR 第 8 條第 1 項規定，在適用同意的情況下，對於直接向兒童提供資訊社會服務，如果兒童年滿 16 歲，則兒童的個人資料處理應屬合法；如該兒童未滿 16 歲，僅限於其法定代理人授權或同意之範圍內，該等處理始為合法[116]。而關於有效同意的年齡限制，於 GDPR 第 8 條第 2 項中則規定，歐盟成員國可以透過法律為該等目的規定較低年齡，但不能低於 13 歲[117]。

為了獲得兒童的「知情同意」，資料控制者必須用淺顯易懂的字句，以向兒童解釋其將如何處理蒐集的資料[118]。倘若欲使其父母（以下概稱父母）之同意，那麼必須提供完整的資訊，以使父母做出明智的決定[119]。從上述內容可以清楚地看出，GDPR 第 8 條僅在滿足直接向兒童提供資訊社會服務之處理，或是基於同意之處理的情況下，而非所有資訊社會服務皆有適用[120]。以下將簡介兒童同意權之要件，包含資訊社會服務之定義、服務需直接向兒童提供、年齡之規範以及兒童的同意與親權責任之關係。

工作小組在評估 GDPR 中「資訊社會服務」之定義範圍時，援引了歐洲法院（European Court of Justice）過往的判例[121]。歐洲法院認為，資訊社會服務涵蓋線上締結或傳輸的契約和其他服務，如果該服務涉及兩個獨立之經濟活動，只要一方是在網路上提供的服務，例如在簽訂契約或與產品或服務相關的資訊，包括行銷活動中的要約和承諾，則該部份即被定義為資訊社會服務，而另一部份若是貨物的實際交付或分配，則不落入資訊社會服務的範疇[122]。故提供網路

115 *Id.*; GDPR, recitals 38.
116 Consent Guidelines, at 23.; GDPR, art. 8(1).
117 Consent Guidelines, at 23; GDPR, art. 8(2).
118 Consent Guidelines, at 23; GDPR, art. 8(2).
119 Consent Guidelines, at 23; GDPR, art. 8(2).
120 Consent Guidelines, at 23; GDPR, art. 8(2).
121 *See* Case C-108/09, Ker-Optika bt v. ÀNTSZ Dél-dunántúli Regionális Intézete, 2010 E.C.J. I-12213, ¶¶ 22, 28.
122 *Id.*



DOI:10.6814/NCCU202000087

服務將屬於 GDPR 第 8 條規定中「資訊社會服務」的範圍[123]。

GDPR 第 8 條僅適用於直接向兒童提供的資訊社會服務，而非所有資訊社會服務[124]。如果資訊社會服務之提供業者明確表示，其僅向 18 歲或以上的潛在使用者提供服務，且網站內容或企業之行銷策略皆表明如此的意圖，則該服務將不被視為直接向兒童提供，因而不適用 GDPR 第 8 條規範[125]。

GDPR 明確規定「歐盟成員國得訂定較低的法定年齡，惟年齡限制門檻不得低於 13 歲」，且資料控制者必須注意各歐盟成員國不同的法律規定，並同時考慮其服務的對象[126]。特別應注意的是，提供跨境服務的資料控制者不單要考慮其營業處所在地成員國的法律，更需要遵守資訊社會服務對象所在之歐盟成員國法律[127]。這取決於歐盟成員國選擇使用資料控制者營業處所在地，或資料主體處所作為其法律依據，且歐盟成員國在做出選擇時應以兒童最大利益作為首要考量，而工作小組亦鼓勵歐盟成員國在此問題上尋求一致的方案[128]。基於同意向兒童提供資訊社會服務時，資料控制者將需要做出合理的努力來驗證使用者是否已超過同意的年齡，且這些措施應與處理資料的性質和風險成比例[129]。

如果使用者聲明其已超過同意年齡，則資料控制者可以執行適當的檢查以驗證此陳述是否為真[130]。雖然在 GDPR 中對於「需要採取合理的努力來驗證年齡」之要求並不明確，但是如果兒童在未達有效同意年齡的情況下同意該資訊社會服務，則使用者所為之同意是無效的，如此一來致使企業對該資料之處理變成非法[131]；而當使用者聲明其低於同意年齡，則資料控制者可以接受此聲明而無需進行檢查，但仍需進一步獲得父母行使授權同意並驗證之[132]。

---

123 Consent Guidelines, at 24.
124 *Id.* at 25.
125 *Id.*
126 *Id.*
127 *Id.*
128 *Id.*
129 *Id.*
130 *Id.*
131 *Id.*
132 *Id.*



DOI:10.6814/NCCU202000087

關於父母的授權，GDPR 沒有規定取得父母同意或確定某人有權執行此行動的實際運作方法 [133]。工作小組建議在兒童之法定代理人授權或同意之情況，資料控制者應作出合理努力，在考量現有科技之情況下，確認該法定代理人之同意或授權，且須同時兼顧資料蒐集最小化的原則，亦即以適當、相關且限於處理目的所必要，其著重在獲取有限的資料，例如蒐集父母的聯繫方式即可 [134]。

在驗證使用者年齡足以行使的同意，以及在驗證代表兒童同意的人是父母方面，驗證方式之合理性可能取決於處理以及可用的技術 [135]。在低風險案例中，透過電子郵件驗證行使親權者之身分可能即已足夠；反之在高風險情況下，可能需要提供更多證據，以便資料控制者能夠根據 GDPR 第 7 條第 1 項驗證和保留資訊，而可信第三方提供的驗證服務，可以協助資料控制者處理最小化之個人資料量 [136]。工作小組承認驗證可能存在著挑戰性，例如兒童在尚未建立身份足跡的情況下行使同意，或者在驗證親權的行使上有困難 [137]。在決定採取何等措施始為合理時，應將上述情況也納入考量，且資料控制者也要不斷審查其處理流程和可用技術 [138]。

資料主體擁有完全控制處理其個人資料之權利，親權行使者雖能同意兒童個人資料之處理，但當兒童達到同意年齡，則得以修改或撤銷同意 [139]。在實務中，這代表著如果兒童尚未為任何同意行為，若親權行使者或被授權代為行使親權者，直接同意兒童資料之處理，則該同意將視為有效同意 [140]。根據 GDPR 第 7 條第 3 項規定，在達到同意年齡後，兒童將得自行撤回同意，GDPR 中亦規範兒童在使用一些特定服務時不需要父母的同意，例如直接向兒童提供的預防或諮詢服務，或是藉由線上聊天服務向兒童提供保護服務等 [141]。

---

[133] *Id.* at 26.
[134] GDPR, arts. 8(2), 5(1)(c).
[135] Consent Guidelines, at 26.
[136] *Id.*
[137] *Id.* at 27.
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*; GDPR, art. 7(3).



DOI:10.6814/NCCU202000087

## 第五目 跨境傳輸規範：原則禁止例外允許

根據 GDPR 的規定，個人資料原則上是禁止傳輸到歐盟境外之第三國，只有符合特定例外才能夠傳輸到第三國 [142]。GDPR 明定三種可合法跨境傳輸之例外，第一種為第三國之資料保護程度通過歐盟認定，即符合國家適足性認定（Adequacy Decision），歐盟內公民的個人資料便可以被傳輸到該國家 [143]；第二種則是企業須做出適當的保護措施，所謂保護措施依 GDPR 之規定有四種，分別是拘束企業準則（Binding Corporate Rules, BCR）[144]、標準契約條款（Standard Contractual Clauses, SCC）[145]、行為守則（Codes of Conduct）[146]及取得認證（Certification）[147]；最後一種例外情形，則是取得資料主體之同意 [148]。上述三種跨境傳輸禁止之例外允許規範內容為何，以下將分別介紹之。

### 一、取得國家適足性認定

所謂適足性認定，指的是歐盟藉由整體評估第三國的法制環境、獨立的監管機關或其簽訂的國際協定合約，來判斷該第三國的隱私保護程度是否與歐盟的保護程度（level of protection）相當。根據 GDPR 第 45 條規定，歐盟的個人資料便可以傳輸到經歐盟評估通過適足性認定的第三國 [149]。在工作小組發布的指導文件中，針對國家適足性認定規範的定義、程序與審核原則有更進一步詳細的說明 [150]。

首先，工作小組針對何謂「適足性」，有做出一些廣義的解釋。歐盟執委會設立適足性認定的目的，在於審視第三國的資料保護體制保護程度是否跟歐盟相當，並非追求一模一樣 [151]。實際上在 GDPR 的前身，即資料保護指令中相

[142] GDPR, art. 44.
[143] GDPR, art. 45
[144] GDPR, art. 46.2(b), art. 47.
[145] GDPR, art. 46.2(c).
[146] GDPR, art. 46.2(e).
[147] GDPR, art. 42(f).
[148] GDPR, art. 49.
[149] GDPR, art. 45.
[150] Article 29 Data Protection Working Party, Adequacy Referential (updated), Adopted on 28 November 2017, WP254 [hereinafter Adequacy Referential Guideline].
[151] Adequacy Referential Guideline, at 3.



DOI:10.6814/NCCU202000087

同適足性認定的概念就已經存在[152]。根據歐洲法院在 *Schrems* 案中對保護程度的定義，保護程度相當並非要求第三國的資料保護法制體系跟歐盟的完全一樣，而是旨在追求具有相同的核心的保護法制準則[153]。歐盟執委會必須評估第三國的法治、對人權與基本自由之尊重、一般與部門之相關立法，包括有關公共安全、防衛、國家安全及刑法、公務機關對個人資料之接近使用權、及該等立法、資料保護規則、專業規則及安全措施之執行，包括個人資料向其他第三國或國際組織進一步移轉，該其他第三國或國際組織之規則、判例法、及有效且可執行之資料主體權利及個人資料受移轉之資料主體有效之行政與司法救濟[154]。第三國相關的立法中，是否具備一個或多個有效運作且獨立監督機構。第三國的國際承諾以及已進入的國際組織[155]。因此，適足性認定必須包括兩個基本的要素：適用規則的內容和確保其有效適用的手段[156]。

在適足性認定審核上的程序規範，欲申請國家適足性認定的第三國，應向 EDPB 提供審核文件，包括相關信件和歐盟執委會的調查結果[157]。如果第三國法律架構過於複雜，則應包括任何有關第三國或國際組織所作關於資料保護級別的報告[158]。應盡量把歐盟執委會所提供的信息盡可能詳盡提供給 EDPB，使 EDPB 足以能夠獨對第三國的資料保護水平進行評估。EDPB 會就歐盟執委會提供的裁決做出意見，並辨識法律適當性框架中的不足之處，並提出變動或修正以解決可能的不足之處[159]。此外歐盟執委會有責任持續監測可能影響適足性認定功能的發展[160]，且適足性的認定必須至少每四年進行一次定期審核[161]。但是

[152] *Id.*
[153] Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. Request for a preliminary ruling from the High Court (Ireland). Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities. Case C-362/14, ¶¶ 73, 74 [hereinafter *Schrems*].
[154] Adequacy Referential Guideline, at 3.
[155] *Id.*
[156] Adequacy Referential Guideline, at 4.
[157] *Id.*
[158] *Id.*
[159] GDPR, art. 1(s).
[160] GDPR, art.45. 4.
[161] Adequacy Referential Guideline, at 4; GDPR, art.45. 3.



DOI:10.6814/NCCU202000087

這個時間的長度只是一個原則性的規定，仍然必須視每個第三國或國際組織的個案情況，做出適當的調整，因此根據當下的特殊情況，也有可能需要縮短審核週期[162]。另外，第三國或國際組織中與法律架構相關的變更，可能會導致需要提前進行審查。歐盟傾向盡快對一個全新的適足性認定進行第一次審查，並根據結果逐漸調整審查週期[163]。

前述提到歐盟對於適足性的認定旨在達到相當的保護水準，而非與歐盟的體制完全一樣，因此工作小組列出了欲申請適足性認定的第三國，其資料保護的規範、法律體制中必須包含一些原則，下以表格整理之[164]。

表 3、國家適足性認定審核參考參考原則

| 規範層面 | 原則 | 說明 |
|---|---|---|
| 規範內容之原則 | 1. 名詞定義需相當 | 第三國法規中一些與資料保護相關的名詞概念需與 GDPR 相符。例如：個人資料處理、資料控制者、資料處理者、敏感性資料。 |
| | 2. 資料之處理必須合法公平 | 歐盟承認一些資料處理的理由是具合法性：國家法律的規定、資料主體的同意、履行契約、資料控制者或第三方契約的合法利益且並未超越個人的利益。 |
| | 3. 目的限制原則 | 應為特定目的處理資料 |
| | 4. 資料品質與比例原則 | 資料須保持準確、必要且更新。蒐集的資料須適當，與其處理目的相關。 |
| | 5. 資料保存時間原則 | 資料的保存應不超過處理目的所必需的數據。 |
| | 6. 安全與保密原則 | 處理個人資料的任何主體都應確保資料的安全性，包括防止未經授權或非法處理使用適當的技術或組織措施防止意外丟失，破壞或損壞。安全級別應考慮到現 |

[162] Adequacy Referential Guideline, at 4.
[163] *Id.*
[164] Adequacy Referential Guideline, at 4, 5.



DOI:10.6814/NCCU202000087

| | | |
|---|---|---|
| | | 有技術和相關成本。 |
| | 7. 透明度原則 | 以清晰、易於接近、簡潔、透明和易懂的形式，告知資料主體其資料處理的要素。但以保護犯罪、調查、國家安全，司法獨立和司法程序或其他重要公眾利益之目的不在此限。 |
| | 8. 取得、修改與異議之權利 | 資料主體應有權取得、修改其資料並對其資料被處理之方式或目的提出異議。 |
| | 9. 資料轉發之限制 | 原始資料傳輸的初始接收者，僅在進一步接收者（即轉發的接收者）也受到約束的情況下允許進一步傳輸資料 |
| 特定處理類型的內容原則 | 1. 特殊類別的資料 | 涉及 GDPR 第 13 條中的特殊類別資料的處理時，應設有具體的保護措施 |
| | 2. 直接行銷 | 在直接行銷目的處理資料的情況下，資料主體應該能夠在任何時候為此目的處理其資料，且不需支付任何費用。 |
| | 3. 自動決策和分析 | 資料處理者需要獲得資料主體的明確同意或簽訂表明有自動決策和分析必要性的契約。第三國的法律應規定必要的保障措施，包括資料主體有權了解決策所依據的具體原因和邏輯，糾正不准確或不完整的資訊，並對基於在不正確的事實基礎上採取的決定進行爭論。 |
| 程序性與法律執行機制 | 1. 主管獨立監督機構 | 第三國必須設置一個或多個獨立監督機構，負責監督，確保和執行遵守第三國的資料保護和隱私條款。該監督機關在履行職責時應當完全獨立、公正。 |
| | 2. 資料保護系統必須確保良好的合致性 | 第三國需確保資料保護規範的高度問責性，具備有效的制裁手段，以及資料控制者對蒐集處理資料的義務的認知。 |



DOI:10.6814/NCCU202000087

| | | |
|---|---|---|
| | 3. 問責制 | 第三國的法規必須有具體措施要求資料控制者、資料處理者遵循該規範。該等措施例如：資料保護影響評估、資料處理活動的諄宗紀錄等。 |
| | 4.資料主體的法律救濟措施 | 第三國法規應確保資料主體能尋求法律救濟，以迅速有效地執行其的權利，並且沒有過高的成本。 |

目前除已獲得適足性認定的12國家之外，歐盟執委在積極合作對象包含日本、韓國、印度、拉丁美洲及歐洲鄰近國家等[165]。台灣於今年三月也開始進行適足性認定評估程序[166]。在國家沒有通過適足性認定的情況下，若企業仍想要跨境傳輸歐盟資料，可以透過標SCC，或是BCR實現之。

二、適當保護措施—標準契約條款（Standard Contractual Clauses, SCC）

所謂標準契約條款，是歐盟提供的資料保護契約模板。企業或組織在簽定契約時，於契約中納入，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，而標準契約條款即為進行跨境資料傳輸的法律依據[167]。目前的標準契約條款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境外的資料控制者的情況（controller-controller），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境外的資料處理者的情況（controller-processor）。

在資料控制者傳輸給資料控制者（controller-controller）的情境下，歐盟境內資料控制者要傳輸給境外資料控制者，要選擇使用標準契約條款時，可以選擇使用模板一（set I）或模板二（set II）[168]。但不可修改模板內容也不可合併

[165] EUROPEAN COMMISSION, *Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Dec. 31, 2019).
[166] 國家發展委員會，歐盟對台歐展開GDPR適足性對話表示歡迎，國家發展委員會，2019年3月11日，https://reurl.cc/72k4qN（最後瀏覽日：2019年12月31日）。
[167] GDPR, art. 46.
[168] Controller-Controller 模板一（setI）: 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539)；
模板二（setII）: 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the



DOI:10.6814/NCCU202000087

兩個模板使用兩個模板要求的填寫基本上相同，只有在排版跟順序上不同。至於在資料控制者傳輸給資料處理者（controller-processor）的情境下，模板中需要填寫的資訊，與資料控制者傳輸給資料控制者大致相同，差別在於需填寫資料處理方式（Processing operations）[169]。

簽訂標準契約條款需填寫之資訊包含：資料標的（Data subjects）；傳輸目的（Purposes of the transfer(s)）；資料類別（Categories of data）；資料接收者（Recipients），並且個人資料只能向下列接收者，或下列類型的接收者揭露：敏感性資料（Sensitive data）、資料輸出者的資料保護註冊資訊（Data protection registration information of data exporter）、其他有用資訊，例如資料儲存時間限制或其他相關資訊（Additional useful information (storage limits and other relevant information)）、資料輸入者（Data importer）、資料輸出者（Data exporter）[170]。

三、適當保護措施—拘束企業準則（Binding corporate rules, BCR）

拘束企業準則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歐盟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 [171]。拘束企業準則可對同一集團內的隱私資料傳輸，提供全球性的資料保護政策，其中包括對隱私資料類別、資料處理形式、資料處理目的、將受影響的資料主體等規定。因此，企業就不需要每次簽署標準契約條款，也有助於節省資料當地語系化處理的成本，增強隱私資料保護當責制，並將資料保護和安全管理融入公司原有的制度體系中。企業若有分公司（資料控制者或資料控制者）在歐盟境內，需在企業內部大量傳輸數據資

transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance, Dec. 29, 2014, O.J. L 385, at 74–84。

[169] Controller-Processor 之契約模板: 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance), Feb. 12, 2010,O.J. L 39, at 5–18 。

[170] *Id.*

[171] GDPR, art 47.



DOI:10.6814/NCCU202000087

料進行處理者，例如 e-Bay、Intel、HP 等企業，則適用拘束企業準則[172]。

企業在申請拘束企業準則的時候除了需要準備拘束企業準則申請表（W133）之外，也需要註明明確的數據保護防衛措施：透明度、數據品質、安全性、有效性工具如審計、培訓或投訴處理系統、足以證明該拘束企業準則具法律拘束力之證據[173]。

在拘束企業準則的申請審核過程中，需要先確認歐盟成員國中何者的資料保護機關將擔任主要監管機關（Lead Supervisory Authority，簡稱為 BCR Lead）。接著 BCR Lead 才會進入審核拘束企業準則的程序流程[174]。企業若想要提交拘束企業準則給監管機關審核通過，需要先確定其應提交的監管機關為歐盟成員國中何者的監管機關。企業可以根據以下幾個標準，從相關監管機關[175]中選擇其 BCR Lead，但這些標準並非制式的標準[176]。

(1) 企業集團在歐盟地區的總部所在地。（此為重要考量因素）例如：Intel 的 BCR Lead 在愛爾蘭。
(2) 企業集團內部被委派資料保護責任的公司所在地。
(3) 最適合處理申請並在集團內執行拘束企業準則的公司所在地（最適合之認定依據管理職能，行政負擔等方向）。
(4) 對於資料處理相關活動之目的與手段，具決定權的公司所在地。
(5) 將會傳輸最多資料到境外的歐盟成員國。

企業提案給其選擇欲作為 BCR Lead 的監管機關時，需同時提出所有足以佐證其提案的適當資訊，尤其是歐盟境內處理資料活動的性質和一般結構，特別

[172] EUROPEAN COMMISSION, *Binding Corporate Rules (BCR) Corporate rules for data transfers within multinational companies*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en(last visited Dec. 31, 2019).
[173] Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, Adopted on 11 April 2018, WP263 rev.01, at 1 [hereinafter BCR Working Document].
[174] BCR Working Document, ¶ 1.
[175]「相關監管機關」係指因下列事由涉及之個人資料處理之監管機關： (a) 控制者或處理者係在該監管機關會員國境內成立； (b) 資料主體居住於該監管機關會員國境內，且受處理之實質影響或可能受到實質影響者；或 (c) 已向該監管機關提出申訴者。
[176] *Id.*



DOI:10.6814/NCCU202000087

是作出決策的地點、歐盟境內分公司的地點和性質、有關僱員或人員的數量、處理資料的手段和目的，移轉到第三國的地方以及移轉這些資料的第三國[177]。

受理提案的監管機關經審核若同意成為該企業的 BCR Lead，其他原本亦可作為 BCR Lead 的監管機關可以在兩個星期內提出異議[178]。若受理提案的監管機關認為其不適任作為該企業之 BCR Lead，則該監管機關需說明原因，並推薦其認為適任之監管機關。確認 BCR Lead 之後，將進入審核 BCR 的程序[179]。

在審核企業提交的拘束企業準則草案時，需同時提交將受該拘束企業準則拘束的企業實體名單、申請表（WP133）[180]。BCR Lead 會將企業提交的申請書跟相關資料給一到兩個其他國家資料監管機關（通常視企業傳輸資料會牽涉到的成員國數量而定）作為共同審查機關（co-reviewers），並幫助 BCR Lead 評估。若共同審查機關在收到申請書跟相關資料後一個月內未給予任何意見，則視為同意[181]。

BCR Lead 跟共同審查機關討論的結果會集結成一份合併草案（consolidated draft），並且傳閱給相關監管機關[182]。相關監管機關可以在一個月內給予建議，若一個月內沒有提出建議，則視為同意該合併草案[183]。BCR Lead 也會提出修正建議，待 BCR Lead 認為申請草案已滿足所有建議，則可以請企業提交最終草案（final draft）[184]。

根據 GDPR 第 64.1、64.4 條，BCR Lead 會將拘束企業準則的最終草案、相關資料及相關監管機關的意見一併提交給 EDPB。BCR Lead 應充分考量委員會之意見，並應在收到意見後兩週內，透過電子方式使用標準化格式向委員會主席通知是否維持或修訂其裁決草案，以及有修訂時，修訂之裁決草案[185]。若

[177] *Id.*
[178] *Id.*
[179] BCR Working Document, ¶ 2.
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*



DOI:10.6814/NCCU202000087

BCR Lead 決定維持其草案則適用 GDPR 第 64.8、65.1 條，若 BCR Lead 決定修改草案則通知申請人修改之，待 BCR 已經依照 EDPB 的意見修正後，BCR Lead 可通過該拘束企業準則，並通知 EDPB 其通過之決定[186]。

一旦 BCR Lead 通過 BCR，BCR Lead 會將該拘束企業準則副本給相關監管機關。並且根據 GDPR 第 46.2b 條，經批准的拘束企業準則將提供第 46.1 條所述的適當保護措施，而無需其他有關監管機構的任何具體授權。此外申請者需要將所有的申請文件都需要提供 BCR Lead 所在國家之語言及英文版本，最終草案需要由翻譯成各相關監管機關國家的語言[187]。

表 4、標準契約條款、拘束企業準則比較圖表

| | 標準契約條款 | 拘束企業準則 |
|---|---|---|
| 定義 | 兩不同公司之間的傳輸資料的契約 | 使跨國公司可在同一集團內傳輸隱私資料的認證 |
| 目的 | 允許歐盟公民的個人資料傳輸到沒有被歐盟認可資料保護適足性的國家 | |
| 授權 | 不需要得到資料保護權責機關授權 | 需要資料保護權責機關授權 |
| 責任 | 即使資料主體不是契約的一方，也能使資料主體行使契約權利；並且接受方同意受歐盟 DPA 和法院的約束 | 拘束企業準則必須具有法律約束力。總部設在歐盟的公司對不在歐盟的任何成員所犯的違規行為負責 |
| 優點 | (a) 歐洲理事會已經提供範本<br>(b) 適用僅需傳輸特定資料<br>(c) 適用於小型公司 | (a) 可以客製化規章內容<br>(b) 可以傳輸大量資料<br>(c) 不需要每次傳輸都重新簽合約<br>(d) 歐盟有很多指引文件（guidelines）<br>(e) 適用於有跨國分公司的集團 |

[186] *Id.*
[187] *Id.*



DOI:10.6814/NCCU202000087

| | | |
|---|---|---|
| 缺點 | 大公司若使用標準契約條款，需簽大量的契約會造成過高行政成本。 | 拘束企業準則驗證過程耗時耗成本。 |

表 5、BCR 申請流程圖


四、取得資料主體同意

資料蒐集者若不透過適足性認定或保護措施來達到傳輸歐盟公民資料的話，亦可透過取得資料主體對於跨境傳輸資料的同意為之。依循 GDPR 第 8 條的規範，向資料主體清楚明確的傳達其應有的權利，資料之蒐集、使用之目的、使用方式等資訊，使資料主體充分了解，並且確保資料主體是自主地、明示地表示同意。

惟由於 GDPR 賦予資料主體充分的權利，使其任何時候都可以撤回其資料被蒐集或使用。在這樣的情況下，對資料控制者或資料使用者而言，資料處於不確定性的狀態，是非常不利的。同時由於 GDPR 在同意的規範上要求資料蒐集者必須很明確的向資料主體說明資料的使用目的及方式，這意味著限縮了資料使用者對於資料的使用範圍，資料使用者若在資料主體同意某項資料的使用之後，欲將資料用於其他使用目的，則需要再向資料主體取得同意。企業在使用資料的目的或方式上，常隨著數據分析的策略或數位行銷策略的變動而有所調整，若需一一向資料主體說明並取得同意，非常不便利也具有高度不確定性。

在跨境傳輸上若資料控制者欲使用取得資料主體的同意，作為其取得跨境傳輸例外允許的手段的話，同樣也存在著不確定性的風險，因為資料主體仍保



DOI:10.6814/NCCU202000087

由其隨時可以撤銷其同意的權利。這將增加資料處理的不確定性，因此不建議將同意作為向第三國資料傳輸的法律依據。企業若想使用向資料主體取得同意來達到跨境自由資料傳輸，實有許多不便跟不確定性。

五、行為守則（Code of Conduct）與取得認證（Certification）

所謂行為守則係指，資料控制者自行訂定符合 GDPR 規範之行為守則並交至主管機關核准[188]。GDPR 第 40 條規定，歐盟各會員國、監督機關、委員會及執委會應鼓勵資料控制者制定行為守則，行為守則內容包含資料處理之公正及透明、蒐集方式、資料當事人權力之行使、兒童資訊之保護等。

所謂取得認證係指歐盟各會員國、監督機關、委員會及執委會建立之資料保護機制與資料保護標章，以證明資料控制者遵守 GDPR 規範[189]。目前歐盟成員國已有各自之認證機制，但歐盟層級之認證尚未實施。

上述介紹之例外允許中，由於保護措施中的行為守則及取得認證為較少數使用及討論的措施，故本文在討論適當保護措施時，將聚焦在 BCR 及 SCC。下一節將介紹 GDPR 之跨境傳輸例外規範可能跟現行貿易規範產生之衝突。

[188] GDPR, art. 40.
[189] GDPR, art. 42.



DOI:10.6814/NCCU202000087

## 第三節 GDPR 與貿易規範可能之衝突

GDPR 以維護數位隱私權之名誕生的同時，也引來許多爭議，其是否現行貿易規範有所矛盾。鑑於線上交易和服務消費的範圍越來越廣，服務貿易協定（General Agreement on Trade in Services, GATS）與數位貿易尤其相關，因此本文所提及之現行貿易規範，以 GATS 為主。GDPR 被廣泛的探討是否違反 GATS 的規定，而 GATS 本身在規範數位貿易上面臨的挑戰跟困境也是探討背景的重點之一，本段將首先介紹網路科技的發展，如何改變國際貿易的型態，以及對於國內規範和國際規範帶來什麼樣的挑戰，接著聚焦於國際規範中的 GATS，初步提出 GDPR 可能會跟 GATS 產生的衝突及原因，並於下一章進一步深入的分析。

### 第一目 數位貿易帶來國際貿易規範上的困境

20 年以來，科技轉化了國際貿易的型態，然而國際貿易的規範體系卻仍在追趕著這個變化的速度[190]。產業都隨著科技數位轉型，電商不再只是專指一個特定的產業，而成為每個產業為提升買賣交易效率，一個必備的途徑或方法。網路與科技帶來也服務與產業型態的改變，分類的界線越發模糊，服務型態的分類也面臨需要重新檢視的必要。科技公司開始跨足提供金融科技服務，金融業者追求透過科技優化其金融服務，也就是追求所謂金融科技（Fintech）上的提升[191]。交通運輸業者結合應用程式提高效益的服務，是交通運輸產業抑或科技業者[192]？網路消弭了地理國界對貿易帶來的障礙，中小企業在過去受限於高成本、跨國貿易的複雜性以及地理距離的障礙難以快速成長，而現今因著網路全球性、去中心化且由下而上的特性，中小企業得以在數位經濟中快速擴張[193]。

---

[190] R. Fefer, S. Akhtar, and W. Morrison, *Digital Trade and US Trade Policy*, CONGRESSIONAL RESEARCH SERVICE (Nov. 5, 2018), https://fas.org/sgp/crs/misc/R44565.pdf.

[191] 張凱君，創新金融模式 下一步是 FinTech 還是 TechFin？，經濟日報，2019 年 6 月 5 日，https://money.udn.com/money/story/5613/3855248（最後瀏覽日：2019 年 12 月 31 日）；鈦媒體，馬雲和他的兆元級「長子」螞蟻金服，數位時代，2019 年 1 月 3 日，https://www.bnext.com.tw/article/51818/antfin-1000-billion-cny（最後瀏覽日：2019 年 12 月 31 日）。

[192] Usman Ahmed, *The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade*, 18 WORLD TRADE REVIEW, 107, 99-120 (2019).

[193] *Id,* at 99.



DOI:10.6814/NCCU202000087

網路與科技在促進數位經濟的同時，因著其去中心化的特質，使得在網路這個疆域上進行的商業活動，該如何界定歸屬的實際地界、又該如何分類服務的類別與型態，讓貿易規範不論是在國內層級或是國際層級上都面臨諸多挑戰，特別在國際層級上例如 WTO 內的談判，又因長年難以推動規範的改革，在新興的數位議題上又更是艱難，因此至今 GATS 的規範內容仍然維持 20 年的內容。以下進一步介紹 GATS 的規範內容與數位服務貿易衝突的困境。

GATS 涵蓋的服務提供方式分為四種模式：

1. 模式一：跨境提供服務（Cross-border Supply）即服務提供者和服務消費者皆不移動，僅服務移動。如遠距教學、電子商務及網路銀行等。
2. 模式二：國外消費（Consumption Abroad）即服務消費者至服務提供者所在國接受服務，例如觀光及留學等。
3. 模式三：商業據點呈現（Commercial Presence）即服務提供者至服務消費者所在國設立商業據點提供服務。例如銀行至國外設立分行、各級學校至國外設立分校等。
4. 模式四：自然人呈現（Presence of Natural Persons）即服務提供者以自然人移動方式至服務消費者所在國提供服務。例如藝人跨國進行巡迴表演，或律師、會計師及商業管理諮詢顧問等，跨國實際面對客戶執行業務、提供服務。

數位貿易可能會落入的服務提供模式有模式一跟模式三。一般數位貿易透過網路出口服務構成跨境貿易，屬於模式一的服務提供 [194]。另外當企業通過建立商業據點（模式三），透過外國子公司提供數位貿易來提供服務時，也可能發生數位貿易。基本上 GATS 的服務提供方式在技術上是中立的，這意味著模式一承諾適用於所有提供方式，無論是通過郵件、電話、網路等，除非在會員

[194] Panel Report, *United States-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 6.285–87, WT/DS285/R (Nov. 10, 2004) [hereinafter US-Gambling Panel]; Appellate Body Report, *United States— Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 215, WT/DS285/AB/R, April 7, 2005. [hereinafter US-Gambling AB]



DOI:10.6814/NCCU202000087

的承諾表中另有規定[195]。

GATS 在 1990 年代初期於烏拉圭回合被簽訂，大部分的 WTO 會員國在當時填寫 GATS 承諾表的時候，服務的分類是參考聯合國的主要產品分類系統（UN Central Product Classification System, CPC）或 WTO 公布的服務業分類表（Services Sectoral Classifications List, 以下簡稱 W120 分類表）[196]。這兩個分類系統及表格皆制定於網路非常不普及的 1990 年代，即使 CPC 之後有更新，大部分國家的 GATS 承諾表仍然是以舊制的 CPC 分類為基礎。GATS 的服務承諾表沒有與時俱進，GATS 的規範是否足以涵蓋適用在現今的數位貿易議題，成為一個問題，尤其是許多新興的數位服務例如搜尋引擎、雲端運算或線上遊戲等許多線上服務，在承諾表被制定填寫的時候是根本不存在的，如何被 GATS 規範是一大挑戰[197]。

WTO 會員國對此採取了不同的立場。根據美國和歐盟的說法，GATS 的承諾是基於服務的本質而不是提供方式，因此很難開發真正新的服務類別[198]。歐盟認為，雲端計算可以歸類於 CPC 843 的資料處理服務（data processing service），而且線上的服務提供方式不會改變服務的性質[199]。加拿大的立場也認為 CPC 包含所有服務，所謂的新服務是可以對應到現有的 CPC 分類或其他的服務類別[200]。雖然根據前述歐盟跟加拿大主張難以開發新的服務類別，然而最近加拿大和歐盟在其 2017 年自由貿易協定中列入了附件，聲明國民待遇（National Treatment），最惠國待遇（Most-Favored National Treatment）和國內規章義務不適用於「不能歸類於 CPC1991 的新服務」[201]。從這點可以看出，WTO 有會員國某種程度上是同意 CPC 並未涵蓋所有服務的觀點，但歐盟的立場

[195] Aaditya Mattoo, Joshua P. Meltzer, *International Data Flows and Privacy: the Conflict and Its Resolution* 21 J. INT. ECON. LAW 769, 779 (2018).
[196] Group of Negotiations on Services, Uruguay Round, S*ervices Sectoral Classification List*, Note by the Secretariat, MTN.GNS/W/120, 10 July 1991[hereinafter CPC List].
[197] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 770-780.
[198] WTO Committee on Specific Commitments, Report of the Meeting Held on 18 September 2014, Note by the Secretariat, S/CSC/M/71; Shin-yi Pent, 'GATS and the Over-the-Top (OTT) Services—A Legal Outlook', Journal of World Trade 50 (1), at 10-13.
[199] WTO Committee on Specific Commitments, Report of the Meeting Held on 18 September 2014, Note by the Secretariat, S/CSC/M/71, ¶ 1.6.
[200] *Id*, ¶ 1.3.
[201] Comprehensive Economic and Trade Agreement Between Canada and the European Union and its Member States, Annex 9-B.



DOI:10.6814/NCCU202000087

認為服務的提供方式不會改變服務的本質，因此在服務的分類上仍可持續適用現存的分類方式。

## 第二目 GDPR 與 GATS 可能之衝突

在GDPR通過之後在國際貿易上一直有爭議的，就是GDPR是否違反GATS的義務。GATS 框架中包含適用於所有服務的一般義務，例如最惠國待遇、相互承認；除此之外，還有 GATS 的特定承諾，是僅適用於會員已安排承諾且受會員規定限制的部門，其中最重要的就是市場進入和國民待遇。

在最惠國待遇方面，雖然 GDPR 對跨境傳輸資料採原則禁止，但歐盟在 2016 年與美國簽訂了歐美隱私屏障協議（Privacy Shield Framework），允許美國能將歐盟的資料傳輸出境，並儲存在美國 [202]。這項協議的內容並沒有讓其他 WTO 會員國相同受惠，其他的會員國仍然要遵循 GDPR 跨境傳輸的例外允許措施才能在歐盟進行跨境傳輸，因此引來對於歐美隱私屏障協議是否有構成違反最惠國待遇的質疑 [203]。同時在跨境傳輸的例外中，適足性的評估也被質疑是否存有相互承認上的歧視。根據 GATS 第 7.3 條規定，相互承認之方式對不同國家不得有歧視之對待，或對服務貿易有隱藏性之限制 [204]。但歐盟通過歐美隱私屏障協議即與其他國家需通過之適足性評估有所不同，難謂沒有在相互承認上有歧視之虞 [205]。

在國民待遇方面，凡舉 GDPR 中要求要在歐盟市場提供數位服務的企業要在歐盟設立代表處、對應資料保護機構要採行一站式機制等規範，國外企業在遵循上需要投入的成本跟歐盟本土企業無庸置疑是不同的 [206]。國外企業在進入市場的成本跟優劣勢跟歐盟本土企業有很大落差的情況下，歐盟在實施 GDPR 上是否有履行國民待遇的義務，值得檢視。

---

[202] Privacy Shield Framework, PRIVACY SHIELD FRAMEWORK, ttps://www.privacyshield.gov/welcome.
[203] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 781.
[204] GATS, art. 7.3.
[205] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 781.
[206] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 780.



DOI:10.6814/NCCU202000087

**市場進入與國民待遇**

在市場進入方面，首先從 *US-Gambling* 上訴機構的裁決中，上訴機構認為一個措施如果禁止某特定的服務輸入，但該特定服務在會員國原先在承諾表中是有開放市場進入的話，很有可能就會構成零配額的問題[207]。若以 *US-Gambling* 上訴機構的意見來看，歐盟在服務承諾表中有開放數位服務的市場進入，但 GDPR 中原則禁止跨境轉移個人資料，有可能會被視為構成與歐盟市場准入承諾不一致的零配額。

在國民待遇方面，由於國民待遇之義務需視會員國特定承諾表針對特定服務部門與模式之開放限制論之，故估不論目前數位貿易服務在 CPC 分類上分歧的看法，且以歐盟認為任何形式的服務都可以納入既有的服務分類，雲端計算服務可以歸類於 CPC843 的資料處理服務作為前提，來檢視歐盟的特定承諾表[208]。歐盟就 CPC 843 的服務部門「模式一」、「模式二」及「模式三」的服務提供方式皆有承諾國民待遇，則可認為歐盟就數位貿易之跨境服務可能涉及的服務部門及服務提供模式是有承諾保障國民待遇的[209]。在這個前提下，GDPR 有潛在可能性會違反國民待遇的規範包含兩個部分。第一個部分是，GDPR 要求任何企業組織在歐盟境內都要設有代表處，此要求所造成的成本對國外提供服務的企業跟歐盟本土企業而言是截然不同的，這也有構成與歐盟的 GATS 國民待遇承諾不一致的情形[210]。另一個部分，即一站式機制之執行效率所帶來的成本問題[211]。根據 GDPR 前言第 127 條規定，如果爭議事件之資料管控或資料處理所在地包括歐盟內部數個會員國，爭議得提交至其中主要監管機關（lead supervisory authority）進行爭端解決，判決內容對於歐盟其他相關會員國具影響力（implications for all of Europe）。因此，歐盟之跨國公司僅需面對一個監管機關，而非 28 個會員國之監管機關，此為所謂一站式（one-stop shop）機制。如果一站式機制未能確實的全面執行，國外企業若要輸出數位服務到歐盟境內，就意味者該國外企業需要面對歐盟境內各國無數的資料保護機構，這對國外企

[207] US-Gambling, ¶ 238, 251.
[208] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 780-781.
[209] *Id.*
[210] *Id.*
[211] *Id.*



DOI:10.6814/NCCU202000087

業所造成的進入成本跟歐盟本土企業所需的成本無庸置疑的是不平等的，在這種情況下難不被質疑沒有實踐國民待遇的要求[212]。

**最惠國待遇與相互承認**

GATS 要求會員國在服務貿易也必須遵守最惠國待遇之義務，如果可以證明歐盟在其應用 GDPR 時在成員國之間存在歧視，那麼 GDPR 有可能也會涉及違反 GATS 最惠國待遇義務。最惠國待遇要求會員國的措施，應賦予不低於其所賦予任何其國家之同類服務與服務提供者之待遇，但歐盟在跟美國簽訂了美國 - 歐盟安全港（US–EU Safe Harbor）以及隨後更新的歐美隱私屏障協議之後，並沒有讓其他會員國同美國受惠，其他會員國仍須依循資料保護適足性的審核程序進行，顯然低於歐盟賦予美國的待遇，印度申請資料保護標準適足性被拒絕，就是強烈對比的例子。

歐美隱私屏障協議除了有違反最惠國待遇的疑慮之外，亦有違反相互承認的可能。GATS 第 7 條允許各會員國自主或通過協議承認另一國家的法規，此為所謂相互承認（Mutual Recognition）[213]。相互承認並非義務性的規範，會員國之間可以自願為之，透過這種較寬鬆的原則亦可達到降低障礙的目的，但仍然需要秉持平等待遇的原則。在 GATS 第 7.2 條中，要求簽訂相互承認協議的 WTO 會員國，要為其他也有意願相互承認的會員國提供充分機會，以協商它們加入此類協議或談判可比較的協議[214]。此外根據第 7.3 條的規定，會員國於給予相互承認時，不得使適用於服務提供者之許可、核照或檢定等之標準或要件，在各國間造成差別待遇或造成服務貿易之隱藏性限制[215]。 GDPR 要求其他會員國若要被歐盟認可具有同等保護水準的資料保護法規，就必須通過適足性的審核，但卻與美國簽訂了歐美隱私屏障協議，歐盟也未因此以歐美隱私屏障協議形式取代其他國家的適足性審核程序，可能構成違反相互承認的規範[216]。

[212] *Id.*
[213] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 781-783.
[214] GATS, art. 7.2.
[215] GATS, art. 7.3.
[216] Aaditya Mattoo, Joshua P. Meltzer, *supra* note 195, at 781-783.



DOI:10.6814/NCCU202000087

**一般例外的可能性**

如果初步假設 GDPR 構成了違反 GATS 的事由，則要進一步地檢驗 GDPR 是否有符合 GATS 的例外條款。根據 GATS 第 14 條一般性例外規定，GATS 允許 WTO 會員國為特定目的，取得執行措施之合理性，但該措施不得有專斷或不正當之歧視，或造成對服務貿易之隱藏性之限制 [217]。特定目的包含：該措施是保護公共道德（Public Morals）或公共秩序（Public Order）的必要條件，或在必要時確保遵守與 GATS 不相抵觸的法律法規，包括與防止欺詐和欺詐行為有關的法律法規和保護個人隱私 [218]。若歐盟可以設法證明 GDPR 之實施是為上述特定目的，則可以取得例外的合理性。

在檢驗一措施是否符合 GATS 第 14 條一般性例外條款時，首先要先檢驗措施之實施目的是否有其「必要性」，第二檢驗其是否有違反第 14 條「前言」的規定。若試以第 14（a）條主張 GDPR 是為保護公共道德或維持公共秩序所需分析是否成立。首先根據 *US-Gambling* 案的小組報告，「公共道德」意指由社群或國家所維持，或代表該社群或國家之正確與錯誤行為之標準 [219]。「公共秩序」係指保存社會之基本利益，且由公共政策與法律所反映者 [220]。從前述的定義解釋可以看出爭端解決小組和上訴機構對會員國認定公共道德之標準實為寬鬆。以 GDPR 而言，由於隱私權在歐盟是被視為一項基本人權，而 GDPR 是基於保護人民隱私權和資料保護權之目的所以實施，不排除爭端解決小組可能會接受歐盟是為公共道德目的而實施 GDPR。

若 GDPR 符合公共道德之目的，則下一步將是歐盟必須證明 GDPR 對於實現其合法目標是具有「必要性」。根據上訴機構的意見，一項措施是否具有「必要性」，應評估該措施所實踐之利益或價值之相關重要性、措施對實現所追求之目標之貢獻程度、措施對國際商務之限制衝擊等要素，並且將該措施與可能之替代措施進行比較 [221]。GDPR 雖然也許可以符合公共道德的目的，但在

[217] GATS, art. 14.
[218] GATS, art. 14(a), (c).
[219] US-Gambling AB, ¶ 6.465
[220] *Id.*
[221] US-Gambling AB, ¶¶ 306-307.



DOI:10.6814/NCCU202000087

必要性上就有合理性的疑慮。其他 WTO 會員國可以主張歐盟其實可以通過對數位貿易限制較少的方式保護其人民的隱私權，包含減少對跨境資料傳輸的限制的方式。相較歐盟執委會嚴格的適足性評估，歐盟美國之間的隱歐美隱私屏障協議就可以顯示，透過較有彈性跟靈活的談判協議，達到兼顧減少貿易限制跟實現歐盟所需的隱私保護水平仍是可行的。

在檢驗「必要性」要件之後，最後需要簡要是否符合「前言」要件。根據 *US-Shrimp* 案中上訴機構的意見，專斷之歧視、不正當之歧視與隱藏性限制雖是不同之概念，但隱藏性限制亦包括對國際貿易之隱藏性歧視，因此隱藏性限制可被解讀為包含對國際貿易構成專斷或是不合理之歧視，所以在決定是否構成專斷或不正當之歧視時，亦必須考量對國際貿易構成隱藏性限制是否存在[222]。歐美隱私屏障協議允許美國在歐盟進行跨境資料傳輸，且該優惠並沒有讓其他 WTO 會員國一同受惠，這便可能可做為歐盟對其他 WTO 成員有構成專斷或不正當歧視疑慮之有利證據。

[222] Appellate Body Report, *United States — Import Prohibition of Certain Shrimp and Shrimp Products*, ¶ 150, WTO Doc WT/DS58/AB/R (Oct. 12, 1998) [hereinafter US-Shrimp].



DOI:10.6814/NCCU202000087

# 第三章 GDPR 跨境傳輸例外規範與 GATS 合致性之評析

在進入本章分析 GDPR 跨境傳輸例外規範與 GATS 之合致性之前，需先檢視此歐盟資料保護措施是否落入 GATS 之適用範圍內。在檢視特定系爭措施是否落入 GATS 之適用範圍時，需透過兩個要件判斷該措施是否足以影響服務貿易。第一，GATS 第 1.2 條意義下之服務貿易是否存在；第二，依據 GATS 第 1.1 條評估該措施對服務貿易之影響。在檢視貿易活動是否落入服務貿易的規範時，必須根據 W120 分類表（該分類表係遵循 CPC 分類表制定）判斷[223]。

在 W120 分類表中電腦部門包含資料處理活動，而資料處理活動係屬於第 1.1B(c)項：資料處理服務（data processing services），在 CPC 分類表中線上資訊及/或資料處理服務（on-line information and / or data processing services）亦包含在電腦相關服務（computer-related service）[224]。再加上歐盟同樣認為資料處理服務歸屬在電腦部門，而非電信部門[225]。歐洲法院在 *Schrems* 案中認為不只是資料的蒐集及使用，連同將資料傳輸到歐盟境外都屬於資料保護指令所規範之資料處理活動本身（*per se*）[226]。綜上可知，GDPR 關於跨境資料傳輸的規範，系落入 GATS 的適用範圍，且任何限制資料傳輸之行為，都有可能在 GATS 的規範之下構成對資料處理服務之障礙。

在了解 GDPR 能落入 GATS 的適用範圍之後，便需要進一步探討 GDPR 跨境資料傳輸規範中「原則禁止」與 GATS 可能產生的衝突。根據 *US-Gambling* 上訴機構的裁決中，上訴機構認為一個措施如果禁止某特定的服務輸入，但該特定服務在會員國原先在承諾表中是有開放市場進入的話，很有可能就會構成零配額的問題，違反 GATS 市場進入的義務[227]。歐盟在資料處理服務部門

[223] GATS, art. 1.2.
[224] W120 List, ¶ 1.1B(c).
[225] WTO, Communication from the European Communities, *Classification in the Telecom Sector under the WTO-GATS Framework*, TN/S/W/27, S/CSC/W/44, 10 February2005, ¶17-22.
[226] *Schrems*, ¶ 45.
[227] US-Gambling, ¶ 238, 251.



DOI:10.6814/NCCU202000087

（CPC843）的「模式一」、「模式二」及「模式三」服務提供方式皆有開放市場進入。根據 GDPR 第 44 條規定：「任何經處理或於移轉至第三國或國際組織後將欲處理之個人資料之移轉，僅得於資料控制者及處理者遵循例外允許之途徑進行，並符合本規則其他條文，包括從第三國或國際組織所為之進一步移轉」從條文文義觀之，GDPR 原則上禁止資料跨境傳輸到歐盟境外 [228]。前段提及歐盟法院在 *Schrems* 案中認定資料傳輸活動亦屬於資料處理服務本身，由此可認為GDPR係針對資料跨境傳輸這項「服務」採以原則上禁止，根據*US-Gambling*的上訴機構裁決 GDPR 就有可能有零配額的問題，跟 GATS 產生衝突。

然而 GDPR 在對跨境傳輸採取原則禁止之外，尚提供了三種允許跨境資料傳輸的例外途徑，因此可能不會違反市場進入之規範。三種例外途徑包含大三國之隱私保護制度通過歐盟執委會的適足性評估，企業或組織採取適當的保護措施（BCR、SCC、行為守則、取得認證），以及特別例外條款：取得資料主體之同意。乍看之下歐盟提供了國家層次、企業組織層次的例外允許方式，讓第三國或境外企業組織在具備足夠的隱私保護下，仍可以跨境傳輸歐盟公民的資料，似乎並非專斷的全面禁止跨境資料傳輸。

惟這三種例外的允許方式是否實質上有遵循 GATS 對於會員國在服務貿易措施亦須維持貿易自由度的要求，所設立的標準是否容易達成值得探討。本章將分別以最惠國待遇、國民待遇及相互承認檢視 GDPR 三種跨境傳輸例外允許之方式。若這些例外允許方式實際上非但沒有為境外企業創造更容易的跨境傳輸途徑，還增加境外企業跨境傳輸資料的困難跟成本，則 GDPR 很有可能構成以隱私保護之名，行貿易障礙之實的問題。

[228] GDPR, art. 44.



DOI:10.6814/NCCU202000087

# 第一節 最惠國待遇

## 第一目 條文要件

GATS 第 2.1 條規定：「關於本協定所涵蓋之任何措施，每一會員應立即且無條件對其他會員之服務與服務提供者，賦予不低於其所賦予任何其他國家之同類服務與服務提供者之待遇。」任何會員國實施關於服務貿易協定之措施，不得特惠特定會員國，或使特定會員國遭受不相同之待遇。根據上訴機構在 *Canada- Autos* 案[229]中的判定，檢驗系爭措施是否違反最惠國待遇之規範，應透過三階段測試檢驗：

(1) 系爭措施是否落入 GATS 第 2.1 條中稱本協定所涵蓋之措施
(2) 系爭措施所涉及的服務與服務提供者是否為「同類」
(3) 同類服務與服務提供者是否遭受較其他會員國所受較低之待遇

首先，判斷系爭措施是否落入 GATS 第 2.1 條中所稱本協定所涵蓋之措施。根據 GATS 第 1.1 條規定，需遵守 GATS 的措施需是會員所實施的措施，且該措施「有影響」（affects）服務貿易。在 GATS 第 28 條 c 款中，有針對所謂對服務貿易有影響的措施舉例，包含系爭措施規範有涉及服務的購買、支付、服務的使用以及服務的取得[230]。在 *Canada-Autos* 案的上訴機構報告中，上訴機構認為在檢視系爭措施是否有影響服務貿易時，需要檢視兩個要件，一是檢視是否有「服務貿易」的存在，二是是否有「影響」的存在[231]。關於何謂有「影響」在 *EC-Bananas III* 案中上訴機構有較明確的解釋，上訴機構認為立法者使用有影響一詞，與規範（regulating）、治理（governing）有所區別，係有意給予較廣義的解釋空間[232]。因此在論及系爭措施對服務貿易產生影響時，必須不是在指措施在對服務的規範或治理的層次上，因此一個針對貨品貿易的措施即使沒有

[229] Appellate Body Report, *Canada — Certain Measures Affecting the Automotive Industry*, WTO Doc. WT/DS139/AB/R (adopted June 19, 2000) [hereinafter Canada-Autos].
[230] Canada-Autos, ¶ 220.
[231] Canada-Autos, ¶ 7285.
[232] Appellate Body Report, *European Communities - Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc. WT/DS27/AB/R (adopted on Sept. 25, 1997) [hereinafter EC-Banana Appellate Body Report].



DOI:10.6814/NCCU202000087

直接規範到服務貿易，只要對服務貿易有所影響，便須遵守 GATS。而所謂有影響的情況，指足以對服務提供的競爭條件產生改變[233]。

第二，措施中所涉及的服務與服務提供者須為同類，然關於同類服務或同類服務提供者之定義在 GATS 中並未有明確的定義。根據 *Argentina- Financial Services* 案，上訴機構認為在判斷服務或服務提供者之同類性時，需要依個案之情形判定[234]。有學者認為可藉由服務或服務提供者之特性、CPC 對服務之分類及描述消費者之習慣偏好等因素來判斷[235]。

最後一個要件，是要判斷同類服務或服務提供者是否有遭受與其他會員國相比，較低之待遇。此項要件之判斷方式在 GATS 第 2.1 條中並未有明確的說明，惟在 GATS 第 17 條國民待遇的規範中，有針對較低之待遇有進一步的解釋。這裡的關鍵問題是，「不低於有利待遇」是否應被解釋為僅僅是形式上（de jure）的歧視，還是包含事實上（de facto）的歧視。在 *EC-Banana* 案中上訴機構維持了小組的結論，即該條款禁止兩種形式的歧視，但在理由上有所不同[236]。

小組認為，在 GATS 第 2.1 條和 GATS 第 17.1 條中，給予「不低於有利待遇」的基本要件是相同的。第 17.1 條中「不低於有利待遇」的標準旨在規定不低於有利的競爭條件，無論這是通過採用形式上或實際上的措施來實現的。第十七條第 2 和第 3 款的目的是編纂這一解釋，這種解釋是在 GATT 的國民待遇條款的判例中確立的，並且除了第 1 款所載的內容之外，沒有對成員施加新的義務。而雖然在 GATS 第 2 條最惠國待遇條款中並沒有類似的詳細說明，但這便不代表可以對於「不低於有利待遇」做出不一樣的解釋。小組認為該要件在第 2.1 條和第 17 條中意義都是相同的。因此儘管第 2 條未清楚闡述，亦可合理推斷，最惠國待遇同時禁止形式上及事實上的歧視[237]。

---

[233] Canada-Autos, ¶ 7281.
[234] VAN DEN BOSSCHE, PETER & WERNER ZDOUC, THE LAW AND POLICY OF THE WORLD TRADE ORGANIZATION: TEXT, CASES AND MATERIALS 333 (3rd ed. 2013).
[235] 林彩瑜，WTO 制度與實務：世界貿組織法律研究（三），2 版，頁 308（2013 年）。
[236] VAN DEN BOSSCHE ET AL., *supra* note 234.
[237] Panel Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, ¶ 6.133, WTO Doc. WT/DS27/R/ECU (adopted on May 22, 1997).



DOI:10.6814/NCCU202000087

但上訴機構並不認為最惠國待遇及國民待遇中，「不低於有利待遇」的判斷方式是完全相同的。上訴機構認為，GATS 第 2 條中的最惠國義務應該根據 GATT 第 1 條的最惠國待遇解釋，而非根據 GATS 第 17 條中的國民待遇義務。而 GATT 第 1 條也適用於涉及事實上的歧視的措施。而且出於規範目的在於避免歧視性措施，在服務貿易的規範上亦禁止事實上的歧視性措施，更能有效確保競爭機會的平等[238]。

判斷事實上歧視的重要關鍵在於，系爭措施之實施是否有影響到其他會員國之競爭條件之平等性。若系爭措施導致某一外國的同類服務產品或服務提供者獲得較好的競爭條件，進而削弱其他第三國會員國之服務或服務提供者之競爭條件，則可能認為有違反事實上歧視[239]。由於事實上的歧視多依個案的情況處理，在判斷服務貿易事實上歧視的案件中，也會藉助貨品貿易的判決作為參考。例如在 *EC- Banana* 案中，上訴機構就有引用 *EC- Canada Beef* 案[240]。在 *EC- Canada Beef* 案中，歐盟實施一法規，針對高品質的穀飼牛肉實施免關稅配額，但需要進口商提供真品證明，以減免關稅。然而被授權出示真實性證書的證明機構只有一美國機構。因此，專家小組認為，該歐盟與 GATT 的最惠國待遇義務規範不符，因為該法規實施的結果在事實上拒絕讓美國以外的任何來源的產品出口進入歐盟市場[241]。

以下將以最惠國待遇的規範分析國家適足性認定及同意，是否違反最惠國待遇之歧視。由於保護措施是針對非歐盟境內的私人企業向歐盟申請跨境傳輸的許可，凡舉非歐盟境內的企業要達到在企業集團之內自由跨境傳輸歐盟公民的資料，就必須通過 BCR，而要針對單筆資料跨境傳輸則需要透過 SCC。因此保護措施在本質上顯然不會涉及最惠國待遇歧視的問題，故不會在此段落討論。

[238] EC-Banana Appellate Body Report, ¶ 234.
[239] Aaditya Mattoo,Thomas Cottier(eds.),Petros C. Mavroidis(eds.), REGULATORY BARRIERS AND THE PRINCIPLE OF NON-DISCRIMINATION IN WORLD TRADE LAW 2 (2000).
[240] EC-banana, ¶ 232.
[241] Panel Report, *European Economic Community - Imports of Beef from Canada*, ¶ 4.2-4.3, WTO Doc. L/5099 (Mar. 10, 1981).



DOI:10.6814/NCCU202000087

## 第二目 國家適足性認定

GDPR 提供的第一個例外允許跨境傳輸資料途徑為國家適足性認定，第三國可透過向歐盟執委會申請審核該國體制對於資料保護的程度，是否與歐盟資料保護的程度相同，若是審核通過歐盟境內的資料便可傳輸到該第三國。凡歐盟以外的國家若想要與歐盟之間自由跨境傳輸資料，皆須通過此審核程序，乍看之下符合 GATS 最惠國待遇義務中，要求會員國對其他第三國需施以相同程度之待遇，惟實質上此國家適足性認定是否有落實平等對待，可以從兩個面向探討之。第一，是否所有第三國皆有依循該程序達成自由跨境傳輸；第二，適足性認定所要求的條件跟標準，是否在形式上及實質上皆有平等，尤其是對於開發中國家，資料保護體制與歐盟落差較大的國家有所歧視。

第一，歐盟雖要求所有第三國都需依照適足性認定，但卻與高度仰賴資料傳輸的貿易夥伴美國之間簽訂了安全港協定，使得美國跟歐盟之間可以自由跨境傳輸，且此歐美隱私屏障協議的簽訂並沒有因此讓其他 WTO 會員國受惠 [242]。若隱私屏障協議的規範程度有比 GDPR 規範低的話，則歐盟可能就有違反最惠國待遇義務之虞。

從歐美隱私屏障保護架構內容觀之，在資料、傳輸、資料控制者等定義上都與 GDPR 規範相同 [243]。隱私屏障協議中，在資料控制者的義務規範及資料主體的權利規範上，與 GDPR 的規範是相似的。要求資料控制者在向資料主體蒐集資料時，應告知資料主體的訊息包含蒐集處理的資料類型、蒐集處理目的、方法，以及向資料主體告知其接近資料的權利等，與 GDPR 要求任何蒐集處理歐盟工資料時，應遵守的通知義務相同 [244]。同時確保資料主體有權決定是否讓其資料被處理使用 [245]。在跨境傳輸的規範上，要求資料處理者確保遵守資料處理目的限制原則，且要求其在處理並保護資料上，保持與歐盟相同的保護水準 [246]。若美國的企業欲在其集團內傳輸資料，而集團內有事業處不在美國或歐盟

[242] *Id.*
[243] Privacy Shield Framework, supra note 202, ¶ I.8.
[244] *Id,* ¶ II. 1; GDPR, art. 13,14.
[245] *Id,* ¶ II. 2.
[246] *Id,* ¶ II. 3.



DOI:10.6814/NCCU202000087

境內，隱私屏障協議要求該企業仍需依循例如申請 BCR 等方式獲得資料傳輸許可，同時美國境內的企業仍需遵循隱私屏障協議的規範[247]。

隱私屏障協議雖然是採行企業組織自行遵守（self-certify）的方式，但這些企業組織仍必須進行驗證（verification）程序，以示其有確實遵守隱私屏障協議的規範。該驗證可以自行進行驗證，亦可委外進行驗證[248]。企業組織必須顯示其有準確地、充分地、完整地執行其公開的隱私保護政策中，關於保障歐盟公民的資料的規範[249]。企業組織也必須指出其公開的隱私保護政策有遵守隱私屏障協議的規範原則[250]。此外，企業組織也必須顯示有確實向資料主體告知其申訴權利與管道[251]。企業組織在驗證聲明中揭示以上要求後，由企業主管簽名，並且最少每年都要驗證一次[252]。由此可以看到，隱私屏障協議的內容實與 GDPR 的規範內容相當，在針對跨境傳輸上的要求也沒有允許較低的保護程度，甚至也要求在集團內第三國跨境傳輸時，仍需透過 BCR 之途徑。乍看採自律規範的形式，由企業組織自行遵守協議規範似乎是較寬鬆的遵循方式，實際上企業組織仍需要透過驗證程序證明其有確實遵循隱私屏障協議規範，且確實保護歐盟公民資料，若被歐盟認為不符合同樣受 GDPR 的罰則規範，從此觀之尚難謂歐盟在隱私屏障協議上有給予美國較高之待遇。

第二，即使歐盟對所有國家的適足性認定檢驗的程序跟要件都相同，不同國家依照其資料保護體系發展的程度，要通過 GDPR 的適足性認定有著不等同的困難度。各國的資料保護發展落差之大，有些開發中國家甚至還在建制法規的過程，要求這些國家要通過與歐盟有相當的資料保護程度的審核標準，幾乎可以認為有實質上的窒礙難行。而這些國家可能又在數位貿易上與歐盟有著密切的合作，在國際的供應鏈中，有許多開發中國家大量出口高科技產品到歐洲、或提供相關的服務（例如客服電話會轉接到印度或東南亞國家）輸出到歐洲，這些國家的經濟與歐洲息息相關，適足性認定對於這些國家而言，可能已經形

[247] *Id,* ¶ III. 10.b.
[248] *Id,* ¶ III. 7.
[249] *Id.*
[250] *Id.*
[251] *Id.*
[252] *Id.*



DOI:10.6814/NCCU202000087

成一種貿易障礙[253]。

這些開發中國家的經濟可以說高度仰賴科技及資料的傳輸，但同時這些國家在資料保護的立法規範上，都尚在發展階段，多數國家沒有獨立規範資料保護的專法，僅只有由基礎法律規範[254]。國家及人民對於隱私保護的觀念仍在發展建立中，可想而知這些國家的資料保護規範程度遠遠不及發展成熟的歐盟，遑論達到與歐盟相等的適足性評估。在這樣的情況下，對於隱私保護發展尚未成熟的開發中國家而言，歐盟的適足性評估是非常不利的，且有可能形成一種障礙，尤其是高度仰賴資料跨境傳輸，出口到歐洲市場的開發中國家。

以印度為例，印度服務出口的很大一部都依賴於跨境資料傳輸，包含輸出服務到歐盟市場[255]。但同時也因著印度是一個開發中國家，其公民獲得金融和其他服務的機會相對較少。印度的隱私法規正在制定中，也已經提交了歐盟的適足性評估[256]。

對印度的服務出口而言，跨境資料傳輸是至關重要的，同時對歐盟而言印度亦是其重要的經濟夥伴，外包許多資料處理的服務[257]。在印度出口的商品及服務中，近 40%的商品和服務是包含軟體和資訊技術服務，此外印度大約三分之二的資訊科技及資訊科技相關產品服務是透過跨境的方式提供，只有大約三分之一是透過印度的商業據點或個人提供[258]。可以看出印度的服務貿易出口大多都是透過網路提供，並且非常依賴於國際間資料的傳輸。在 2016 到 2017 年間，印度約有 23%的資訊科技及資訊科技相關產品服務輸出到歐洲，使其成為僅次於美國和加拿大，第三大的印度出口目的地[259]。提供這些服務通常需要收集歐盟公民的資料，因此會受到歐盟隱私規範的影響。對於一個人口有五分之一低於貧窮線的開發中國家而言，印度蓬勃發展的資訊科技產業和出口導向型

[253] VAN DEN BOSSCHE ET AL., *supra* note 234.
[254] *Id.*
[255] Aaditya Mattoo, *supra* note 195, at 777-779.
[256] *Id.*
[257] 印度 IT-BPM 資訊外包產業介紹(二之一)，台灣經貿網，2015 年 8 月 24 日，https://reurl.cc/pDekxZ（最後瀏覽日：2020 年 1 月 13 日）。
[258] *Id.*
[259] *Id.*



DOI:10.6814/NCCU202000087

企業為尖端服務貿易和刺激經濟增長提供了重要機會。但同時也因為身為一個開發中國家，印度在保護資料隱私的方法上仍然不夠純熟，導致縱然個人資料的使用具有經濟和貿易潛在價值，但在管理個人資料的使用上可能會導致隱私洩露的風險，造成隱私保護跟貿易利益無法平衡。

印度的隱私保護法制還在發展中，在印度強調對社區規範和其他後殖民地優先事項（postcolonial priorities）重視，意味著到目前為止，個人隱私權已通過普通法和一些立法逐步發展，但迄今為止，印度並沒有一個歐盟認為足夠的隱私保護法制 [260]。事實上，歐盟執委會在 2010 年發表的白皮書中得出的結論是，印度沒有提供足夠的隱私保護 [261]。如果印度不另立隱私保護的專法，而是要將國家既有的法律修法達到歐盟適足性標準，好處在於印度的企業及個人就可以免去使用 BCR 跟 SCC 造成額外的成本，但缺點是這等同要求所有企業，無論其供給市場是國內還是歐盟，都要遵守同一嚴格的隱私保護法規。並非所有產業或企業都需要輸出服務到歐洲市場，以國家既有規範商業的法律達到與歐盟同等的隱私保護程度，會對這些企業造成過多的成本並非必要跟適合。

目前涉及最惠國待遇事實上歧視的案例中觀之，需要該措施有明確具體的造成對特定第三國有優惠的情況下（例如前述提及的 EC- Canada Beef）才會被認定為構成事實上歧視行為。縱然歐盟設立的國家適足性認定要求繁瑣，對於開發中的國家而言門檻甚高，然而 GDPR 中國家適足性認定的實施至目前為止，已有多個國家通過認定程序 [262]，目前尚難謂成立明確的事實上歧視。

## 第三目 同意

取得資料主體對跨境傳輸資料的明確同意，亦是跨境傳輸的例外允許之一。如果第三國未通過適足性的評估，且資料控制者缺乏適當保護措施的情況下，資料控者可以透過明確向資料主體告知資料跨境傳輸的風險，並獲得資料主體

[260] *Justice K S Puttaswamy v Union of India and Ors*, Supreme Court of India, Writ Petition (Civil) No. 494.
[261] Aaditya Mattoo, *supra* note 195, at 778.
[262] 詳見註 165。



DOI:10.6814/NCCU202000087

明確同意後，資料控制者或處理者得將其資料傳輸到歐盟境外之方法[263]。這是根據 GDPR 核心的立法目的：資料主體有權決定其資料是否被處理與使用而設立的例外允許[264]。

最惠國待遇的規範要求會員國的措施必須對所有第三國都平等。而 GDPR 的第 49 條規範是任何歐盟外的第三國家若想要透過取得資料主體同意，以進行資料跨境傳輸的話皆需要遵守的規範。即使是在美國跟歐盟的歐美隱私屏障協議中，亦要求資料控制者須向資料主體清楚通知跨境傳輸目、限縮資料處理目的，並必須取得資料主體的明確同意。在第 49 條跨境傳輸的取得同意規範上，GDPR 基本上對所有第三國的規範都是一視同仁的，因此可以認為在這部分歐盟並未違反最惠國待遇的規範。



[263] GDPR, art. 49.1(a).
[264] GDPR, art. 6.1(a), 7.1.



DOI:10.6814/NCCU202000087

## 第二節 國民待遇

### 第一目 條文要件

根據 GATS 第 17.1 條之規定：「就會員之特定承諾表所載之服務部門，每一會員就所有影響服務提供之措施，應賦予任何會員之服務及服務提供者，不低於其所賦予本國同類服務及服務提供者之待遇；惟此待遇尚須受該會員特定承諾表所列條件與限制之拘束。」不同於貨品貿易規範，在服務貿易之規範中，國民待遇之義務僅屬於特定承諾範圍，並非一般適用，因此國民待遇之內容會因服務部門與承諾範圍之不同有所差異。要檢驗服務貿易之措施是否違反 GATS 國民待遇之規範，需經過四階段的檢驗：

(1) 會員是否承諾對與系爭措施相關的服務部門及服務模式開放國民待遇；
(2) 系爭措施是否為由會員實施且影響服務貿易之措施；
(3) 系爭服務與服務提供者是否與國內服務及服務提供者「同類」
(4) 系爭外國服務及服務提供者是否受有較不利之待遇

首先，需要檢驗會員是否曾經承諾過系爭措施相關的服務部門及服務模式開放國民待遇。判斷之方法根據 *China-Publications and Audiovisual Products* 案中，小組以維也納條約法公約（The Vienna Convention on the Law of Treaties，VCLT）第 31 條及第 32 條之解釋方式解釋中國的承諾表[265]。第二，判斷系爭措

[265] 第三十一條 解釋之通則
一、條約應依其用語按其上下文並參照條約之目的及宗旨所具有之通常意義，善意解釋之。
二、就解釋條約而言，上下文除指連同弁言及附件在內之約文外，並應包括：（甲）全體當事國間因締結條約所訂與條約有關之任何協定；
（乙）一個以上當事國因締結條約所訂並經其他當事國接受為條約有關文書之任何文書。
三、應與上下文一併考慮者尚有：
（甲）當事國嗣後所訂關於條約之解釋或其規定之適用之任何協定；
（乙）嗣後在條約適用方面確定各當事國對條約解釋之協定之任何慣例；
（丙）適用於當事國間關係之任何有關國際法規則。
四、 倘經確定當事國有此原意，條約用語應使其具有特殊意義。

第三十二條 解釋之補充資料
為證實由適用第三十一條所得之意義起見，或遇依第三十一條作解釋而：
（甲）意義仍屬不明或難解；或
（乙）所獲結果顯屬荒謬或不合理時，為確定其意義起見，得使用解釋之補充資料，包括條約



DOI:10.6814/NCCU202000087

施是否為 GATS 第 28 條中所稱之措施，且該措施是否是有影響服務貿易之措施，根據 *Canada-Autos* 案中，上訴機構在判斷該要件時，留意該系爭措施須符合 GATS 第 1.2 條下服務貿易定義，且落入第 1.1 條下「影響服務貿易」之定義[266]。

第三，需要判斷系爭服務與服務提供者是否與國內服務及服務提供者「同類」（like）。此處的同類分析方式不得直接適用貨品貿易規範中對同類產品的判斷，因為考量到服務貿易與貨品貿易本質上有重大的不同。關於同類的判斷，根據 *China-Electronic Payment Services* 案，小組定義所謂服務貿易中的同類，比較產品有相同的特定或品質，不須完全相同，只需要有大致相似即可（approximately similar）[267]。此外比較產品之間，必須存在一定程度的競爭關係，足以使一會員之措施改變競爭的條件，導致特惠於其中一方服務[268]。在 *Argentina-Financial Services* 案中，上訴機構認為在 17 條中「同類服務和服務提供者」是不可切割的概念，需要放在一起認定。上訴機構提供三個可作為認定基準的參考要素：(1)服務及服務提供者的特質；(2)消費對服務及服務提供者的偏好；及(3)稅則編號。在 *Argentina-Financial Services* 案中，阿根廷政府機構可取得外國服務提供者的稅務資訊可被視為是一個和競爭關係相關聯的要素[269]。如果給予不同待遇的標準純粹基於服務來源，則可直接跳過「同類性」的判斷，推定產品為同類產品。

最後，需判斷系爭外國服務及服務提供者是否受有較不利之待遇。根據 GATS 第 17.2、17.3 條之規定，國民待遇之義務應包含「形式上」及「事實上」的相同待遇。判斷是否有不利之待遇可以從形式上及事實上判斷。若規範在形式上就有不利於國外服務提供者，會違反國民待遇義務，然而即便規範在形式上對待國內及國外的服務提供皆相同，亦仍有可能產生事實上的不利待遇，構成國民待遇之違反。

---

之準備工作及締約之情況在內。

[266] Canada-Autos, ¶ 200.

[267] Panel Report, *China - Certain Measures Affecting Electronic Payment Services*, ¶ 7.699, WTO Doc. WT/DS413/R (adopted on Aug. 31, 2012) [hereinafter China-Electronic Payment Services].

[268] China-Electronic Payment Services, ¶7.700.

[269] Appellate Body Report, *Argentina - Measures Relating to Trade in Goods and Services*, WTO Doc. WT/DS453/AB/R (adopted on May 9, 2016).



DOI:10.6814/NCCU202000087

所謂事實上的歧視，與貨品貿易不同之處在於，判斷服務貿易有無受不利之待遇，關鍵在於判斷措施是否有偏袒國內廠商的「競爭條件」。在 *China-Electronic Payment Services* 案中，小組採取兩階段測試系爭措施是否有造成較不利之待遇。第一，判斷系爭措施是否在國內服務及服務提供者和同類的外國服務及服務提供者間有所差異；第二，判斷差別待遇是否造成較不利之待遇[270]。若措施在形式上對國內外服務提供者適用，卻在實際上使外國服務提供者享有較為不利之競爭條件，則仍會構成實質上國民待遇之違反[271]。換言之，若措施在形式上雖對國內外服務提供者賦予不同之待遇，但實際上並未改變競爭條件，則仍未違反國民待遇義務。

以下將以國民待遇的規範分析保護措施及同意是否違反國民待遇之歧視。之所以排除國家適足性認定之分析，是因為適足性認定係歐盟對第三國要求之資料保護水平評估，主要涉及是否對所有第三國之評估皆一致平等，即前一節討論之最惠國待遇問題，與歐盟對內的規範之間較無關聯性，故不在國民待遇討論之。

### 第二目 適當保護措施

適足性認定是透過第三國以國家的身分爭取歐盟的跨境資料允許，而保護措施則是私人企業想要取得跨境資料傳輸自由時，可採取的措施，包含 SCC 及 BCR。保護措施最可能違反的 GATS 義務，便是國民待遇的規範，因為保護措施是針對境外的私人企業的規範，歐盟境內的企業蒐集、傳輸或使用歐盟公民資料並不需使用 SCC 或 BCR。乍看歐盟給予境外企業除了適足性認定之外，另一個自由跨境傳輸的解套方案，使企業可以以私人身分申請，似乎是一個很好的例外允許途徑。然若進一步檢視 SCC 與 BCR 申請的程序與規範，會發現這兩項保護措施的申請程序之繁瑣，需投入的時間、金錢成本之高，使得境外企業要蒐集、傳輸或使用歐盟公民的資料遠比歐盟境內的企業來的困難，足以構成實質上國民待遇歧視之虞，以下分析之。

[270] China-Electronic Payment Services, ¶ 7.687.
[271] China-Electronic Payment Services, ¶ 7.700.



DOI:10.6814/NCCU202000087

首先，需檢視歐盟對於數位貿易相關的服務是否有開放國民待遇。根據前一章，提到現今因為數位貿易的型態在 CPC 的服務分類中應如何分類，存有很多爭議，同時使得 CPC 的服務分類被認為有很大的改空間。但由於歐盟曾表示雲端計算服務可以歸類於的 CPC 843 資料處理服務，且認為線上服務的提供方式並不會改變服務的性質，故本文暫不討論數位貿易服務在 CPC 分類的問題[272]。探討歐盟的特定承諾表針對數位貿易服務是否有開放國民待遇。以 CPC 843 資料處理服務部門為例，歐盟對其「模式一」、「模式二」及「模式三」的服務提供方式皆有承諾國民待遇，則可認為歐盟就數位貿易之跨境服務可能涉及的服務部門及服務提供模式是有承諾保障國民待遇的。故國民待遇的第一要件成立，同時 GDPR 是由歐盟實施的措施也無爭議，故第二項要件也成立。第三項要件要檢視系爭服務與服務提供者是否與國內服務及服務提供者「同類」，由於本文要分析的對象是歐盟外的國家在與歐盟進行貿易時，會須要蒐集、處理歐盟公民資料的服務提供者，並未限縮特定服務類型及服務提供者，且歐盟內亦有在向歐盟公民提供服務時需要蒐集、處理歐盟公民資料之服務提供者，故不進一步探討第三要件的內容，僅視為第三項要件成立。

在分析第四要件，系爭外國服務及服務提供者是否受有較不利之待遇，會分別就保護措施中的 BCR 及 SCC 進行分析。BCR 旨在允許跨國企業集團將歐盟資料保護規定納入其企業隱私政策，從而形成與其業務組特定資料處理要求相關的充分保護，適合頻繁在集團內部傳輸資料的跨國集團[273]。與 GDPR 的前身資料保護指令相反，GDPR 引入了有關 BCR 內容的詳細要求，有效的 BCR 具有法律約束力，適用於企業集團的每個成員，或由參與聯合經濟活動的商業組織的合作實施，這具有將 BCR 轉變為商業組織內部的隱私政策的效果。然而雖然對跨國企業集團而言，BCR 是將有效地將歐盟資料保護規範轉換到集團內部隱私政策有效的方式，要通過 BCR 卻並非易事，實際上是非常耗時耗成本的，BCR 流程一般耗時超過 6 個月，在前一章中有更詳細的介紹申請 BCR 繁瑣冗長的流程。跨國企業集團若是想要在集團內，不受國家限制的蒐集、處理跟傳輸歐盟公民的資料，就需要經過 BCR 的申請。在這個只要有網路就能觸及到世界

[272] WTO Committee on Specific Commitments, *supra* note 199.
[273] WP 256, 257.



DOI:10.6814/NCCU202000087

各地的時代，要成為一個跨國企業擴張海外市場的成本大幅降低，與過去在網路不發達的時代相比，觸及到國外市場，困難度大幅降低，因為地理距離已經不再是障礙。在台灣起家的電商也可以進軍美洲、歐洲的市場，在歐洲設立的雲端服務公司，也可以輕易觸及亞洲的市場。然而在歐盟境外的企業若想要透過 BCR 的途徑進行跨境資料傳輸，想要將歐盟消費者的資料傳輸回本國的話，就需要經過 BCR 耗時耗經費的程序，無疑是非常沉重的負擔，他們需要先評估要以哪個歐盟國家作為其選擇 BCR Lead 的國家，並遞交繁瑣的文書資料，配合 BCR Lead 的要求修改，直到審核通過。網路讓企業擴張海外市場的成本降低，成為跨國企業集團不再像過去網路上未發達的時代，必須有雄厚的資本基礎為前提，同時這也意味著這些企業可能沒有辦法負擔 BCR 流程的經費。歐盟內設立的企業要處理或傳輸境內或境外的資料並不需要透過 BCR 的程序，此外歐盟境內的企業享有一站式服務，企業只需要面對一個主要的監理機關，該機關有義務與企業有活動的其他歐盟國家的監理機關合作，以減少企業的法遵成本，但非歐盟境內設立的企業就沒有辦法享有一站式服務，每個該企業有營業活動的歐盟國家，企業都需要面對該國家的監管機關 [274]。在無形成本的負擔上境外企業原先就需要負擔比境內企業多，在這樣的情況下，尚且給予歐盟境內企業一站式服務，對於境外企業卻不得適用一站式服務，要求其需要分別面對各國的監管機關企業，實有增加境外企業法遵成本的可能。

惟任何跨國的貿易行為對境外企業而言，必定會有相對於國內企業較不便之處，或較高的負擔，因此無法因此認為其就等於違反國民待遇。從企業組織規模的角度進一步切入思考成本負擔的話，BCR 是適合跨國企業在歐盟及其他國家皆設有實體營業據點的情況下，若是大型的跨國集團，其資本額足以讓其在一個以上的國家境內設有實體據點，則可以合理認為 BCR 的程序成本應仍在其可負擔的範圍之內，實際上也已有一些企業有通過 BCR 的認證 [275]。BCR 對大型集團而言也可被認為是一種投資，因為企業通過 BCR 的認證之後，有助於整個企業集團內在資料的保護上更有系統架構的執行，往後在企業集團內資料

[274] Guidelines for identifying a controller or processor's lead supervisory authority, 9.
[275] EUROPEAN COMMISSION, *List of companies for which the EU BCR cooperation procedure is closed*, EUROPEAN COMMISSION, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=61384 (last visited Dec. 31, 2019).



DOI:10.6814/NCCU202000087

傳輸及處理過程中，也不需要透過 SCC 或反覆取得資料主體同意，減少了資料處理的不確定性[276]。

然而對資本不雄厚的中小型企業而言，可能就會是難以負擔的成本。中小企業若在歐盟境內設有基本的據點，仍可能會有在集團內傳輸資料的需求，若想要使用 BCR 可能就會無法負擔申請 BCR 的金錢跟時間成本。因此 BCR 縱然對於大型集團而言，BCR 的成本應無法認為有實質上的降低境外企業的競爭條件，也有值得投資的好處，但在網路時代，對於眾多提供網路數位服務的中小型企業而言，則有實質上降低境外企業競爭條件之虞。

除 BCR 之外，SCC 亦是例外跨境傳出的途徑之一。SCC 是一個歐盟提供給企業的契約範例、模板，讓企業想要跟資料主體簽訂資料蒐集處理的契約時，減少重擬一份遵循 GDPR 的契約的成本[277]。在資料保護指令的時期 SCC 被頻繁的使用在資料跨境傳輸上。需要注意的是，SCC 僅保證第三國的特定資料控制者傳輸單筆歐盟公民資料，而非整個企業流通資料。根據 SCC 的規範，如果資料傳輸者符合相關的條件，則該資料傳輸者可被視為有達到適當資料保護水準[278]。到目前為止，歐盟執委會已經採用了三個 SCC：兩個從歐盟內部的資料控制者向歐盟以外的資料控制者傳輸資料的契約範例，以及一個從歐盟內部的控制者到歐盟以外的資料處理者傳輸資料的契約範例[279]。

SCC 模板中的規範包含對於資料控制者、處理者的規範內容，以及保障資料主體的權利等 GDPR 中核心的基本規範，是歐盟境內企業在蒐集歐盟公民資料時，也需要遵守的規範，故 SCC 在本質上較沒有違反國民待遇之虞[280]。SCC 的優點在於資料控制者可以直接拿來使用，因為 SCC 基本上是 GDPR 現成的契約範例，已經遵循了 GDPR 的資料保護要求，且 SCC 對於締約雙方之間的關係

[276] Daniela Fabian Masoch, *Why Should Companies Invest in Binding Corporate Rules*, ICLG, https://iclg.com/practice-areas/data-protection-laws-and-regulations/3-why-should-companies-invest-in-binding-corporate-rules (last visited Dec. 31, 2019).
[277] GDPR, art. 46.
[278] GDPR, art. 46.
[279] 詳見註 168, 169。
[280] 同上註。



DOI:10.6814/NCCU202000087

沒有額外限制。

但 SCC 欠缺彈性跟靈活度，在使用上也有諸多缺點。SCC 的條款不能更改，必須維持 SCC 的完整性，條款才能生效。此外 SCC 必須資料主體跟單一資料控制者或處理者之間簽訂的，如果該資料控制者或處理者要將資料傳輸給另一個資料處理者處理，則需要簽訂新的 SCC，而 SCC 的簽訂本身就已經是耗時的流程，平均需要通過三個月的時間來完成 [281]。這對大量進行集團內部資料傳輸及處理活動、每天交換傳輸資料的跨國企業集團而言，是非常艱鉅又耗費成本的。

## 第三目 同意

在第 49.1(a)條中關於向資料主體取得資料主體跨境傳輸的同意的規範上，並沒有特別跟前部分要求在資料蒐集、資料處理時徵求同意的規範有所區別，這意味著 GDPR 對於不論是在跨境傳輸的情境下，或是在蒐集或處理資料的情境下，規範都是一視同仁。取得同意的規範不論是在歐盟境內蒐集處理，或是需要將資料傳輸到歐盟境外，資料控制者都必須確保同意的有效性，即資料主體的同意必須是明示、明確針對資料的跨境傳輸目的，不得以暗示性、一般廣泛的同意為之。同時，資料控制者跟處理者必須據實地告知資料主體與資料傳輸相關的潛在風險，讓資料主體明白資料在跨境傳輸的過程中，不會受到與 GDPR 相同級別的資料保護。並且確保資料主體能自主地行使其應有的權利，包含撤回或拒絕其資料用於行銷用途。這些規範對於只是在歐盟境內進行的一般資料蒐集跟處理的資料控制者跟處理者而言一樣要遵守，因此可以認為取得資料主體以進行資料跨境傳輸之例外允許手段，並沒有造成國外資料控制者跟國內資料處理者在競爭條件上有所落差，因為雙方在取得同意的法遵成本上是相似的，並沒有違反國民待遇的規範。

[281] NASSCOM-DSCI (National Association of Software and Services Companies—Data Security Council of India). 2013. Survey of the Impact of EU Privacy Regulation on India's Services Exporters.



DOI:10.6814/NCCU202000087

## 第三節 相互承認

### 第一目 條文要件

國民待遇與最惠國待遇的規範是追求會員國之間進行規範調和（Regulatory Harmonization），透過沒有差別跟一致性促進貿易自由度[282]。相互承認（Mutual Recognition）則是讓會員國之間保有各自不同的規範準則，並透過認許彼此的規範是平等一致的，以消除規範間不一致帶來的障礙[283]。根據 GATS 第 7 條之規定，會員國之間得相互承認特定國家所授予服務提供者之執照或證書，包含學位、經歷、資格或執照等，可以透過簽訂協議或單方自主給予之方式達成[284]。相互承認並非強制要求，會員國可以依各自的意願為之，但會員國在給予承認的時候，不得針對服務提供者之許可、核照或檢定等標準或要件，並且不得在各國之間造成差別待遇或造成服務貿易之隱藏性限制[285]。

以下將分別檢視適足性認定、適當保護措施與同意是否違反相互承認之規範。此外將進一步探討相互承認在現今國際貿易的規範應扮演什麼樣的角色。當大量倚重資料跨境傳輸的數位貿易興盛，同時重視個人資料保護隱私的意識抬頭，增加了自由貿易與限制資料流通之間的張力。加上國際貿易的規範無法跟上數位貿易的更新，造成各國開始試圖以國內法保護資料隱私，在這樣的情況下，規範的相互承認是否能成為一個兼顧自由貿易的流通，與資料保護的折衷方案，值得探討。

### 第二目 適足性認定、適當保護措施與同意

在檢驗適足性認定上，在條文上沒有明文規定相互承認的必要性，在通說上也沒有強制會員國要做相互承認。因此以相互承認的規範檢視適足性認定這種單向的檢驗程序時，適足性並不會違反相互承認的規範或涉及歧視，因為歐

[282] Usman Ahmed, *supra* note 192, at 114.
[283] *Id.*
[284] GATS, art. 7.1.
[285] GATS, art. 7.3.



DOI:10.6814/NCCU202000087

盟並無義務要跟其他會員國進行相互承認。

在檢驗適當保護措施上，BCR 是企業集團向歐盟提出申請，使歐盟審核其集團內的資料保護政策是否符合歐盟的要求標準，待審核通過始得在集團內部限歐盟境內境外進行資料跨境傳輸，此並非相互承認中雙向的承認證照或資歷[286]。而 SCC 更只是歐盟提供的符合 GDPR 資料保護規範的契約模板，提供給資料控制者在與資料主體簽訂跨境資料傳輸時，可以直接使用，因此亦與相互承認規範的標的無關，故 GDPR 關於適當保護措施的規範，並不會違反相互承認的規範[287]。在取得跨境傳輸的資料主體同意上，亦因與相互承認無直接關係，故不會涉及違反相互承認的可能。

值得思考的是，相互承認是否是歐盟應該考慮採用的規範方式，而非採取沒有雙方談判空間、僅單方決定審核標準及規則的方式，例如國家適足性認定。對於同樣非常重視國際貿易的歐盟而言，築起數位貿易障礙對其並沒有好處，透過與貿易夥伴相互承認規範達成雙贏局面。以下將進一步說明國際規範與國內規範面對數位貿易的困境，以及歐盟應採用相互承認之理由。

### 第三目　相互承認— 數位貿易規範可能的解答

保有網路帶來自由貿易的效益，同時兼具資料隱私的保障是現今數位貿易時代下，國際貿易規範制定者無不追求的規範。然這對國際規範制定者或國內規範制定者而言，都各自面臨困境，在這樣的情況下，追求各國規範之間的合作，可能可以成為數位貿易規範困境上的解答。

保護本國公民資料安全是國內法律政策的範疇，而涉及國際貿易的規範則是國際法治例如 WTO 所應處理的領域。惟 WTO 本身在各項多邊貨品貿易談判上已經停滯十幾年，論及諸多法規上的更新，已經是多年來爭論確沒有實際進展的狀態，更遑論在面對變化過於快速的服務貿易型態。即使可以廣義的將所有數位貿易服務都納入 1995 年所立下的 GATS 的適用範疇，若是進一步的適用，

[286] 詳見本文第二章第二節第二目之說明介紹。
[287] 同上註。



DOI:10.6814/NCCU202000087

便會發現 20 年前與今日從對服務的定義與分類範圍、到服務提供的型態都已經有天差地遠的更新與改變，試想 10 幾年前 *US-Gambling* 涉及的網路賭博，與今日的區塊鏈、互聯網、自駕車等技術所應用的服務，若皆適用同樣的貿易規範，殊難想像能符合各服務型態的需求與特性。然即使 GATS 有首當其衝應該修改的規範，在談判上諸多的窒礙難行是眾所皆知[288]。

在國際規範無力提出符合情勢規範的情況下，各國自然出於為捍衛自身利益與公民的資料安全等原因，朝修改強化本國法制的途徑發展。然而對於國家規範制定者而言，卻有許多考量因素使得其在制定規範或談判的過程中，難以實現這樣的理想，甚至會使得各國在本國的法律規範上越發保護本國利益，反之便增加了在自由貿易上的困難度。

首先，國家制定規範會受到主權國界的限制，但在網路上進行的商業活動卻不受地理國界的拘束。發生在網路上的法律糾紛可能有跨管轄範圍的可能，就會引發管轄權的問題[289]。一般法律上強制執行的方法是透過實際進行罰款或逮捕的，但是，當主體居住在另一個主權國家的管轄範圍內，可能就沒辦法執行法律[290]。若國家規範制定者試圖將所有可能侵犯其國內資料保護的網路行為都納入其管轄範圍內，就會發生像 GDPR 第三條的地域範圍規範，可能過度擴張其管轄權，引來域外適用的質疑，因此國家規範是有其行使的侷限性。

第二，規範通常是圍繞一個監管特定產業實體、從事特定類型活動的單一監管機構建立的。例如，管理金融產業的中央銀行。金融服務相關的規範就可以圍繞這些關鍵角色設計法規，以便在系統中提供確定性與穩定。然而在網路上進行商業活動只是一種途徑或管道，可以運用在任何產業中，這使得規範制定者若要針對網路商業行為制訂規範，就需要考慮跨產業可能涉及的差異性，這使得制定規範變得越來越困難[291]。反之，單一規範適用於所有產業及行為則可能會無法切合產業或行為的特性，造成過度規範。

[288] Usman Ahmed, *supra* note 192, at 114.
[289] Usman Ahmed, *supra* note 192, at 105.
[290] *Id.*
[291] Usman Ahmed, *supra* note 192, at 106.



DOI:10.6814/NCCU202000087

第三，如何分類或調整實體在網路中的活動，以及隨之而來的變動性也是一大挑戰。當國家規範制定者決定如何對網路經濟中實體的活動進行分類或調整時，它將立即迫使其他國內監管機構重新審查其處境類似的法律。這對於外國實體而言，是一個錯綜複雜的環境，很難在其中進行活動，尤其是當網路本身原本旨在簡化跨境障礙的複雜度。甚至在制定規範的過程中，增加了對外國企業的跨國貿易障礙。

GDPR 雖然經本文初步分析後並無違反 GATS 的規範之虞，惟合致於法規並不代表就是最適的規範。歐盟透過 GDPR 築起保護規範的高牆，各國也可能會仿效之。而比起各自築起保護規範的高牆，各國之間進行規範的合作，透過相互承認確保貿易的自由流通，又同時兼顧資料的保護，可能會是現今數位貿易規範困境的解答。GDPR 反映出在數位經濟貿易的發展趨勢下，資料保護意識的興起，而跨境資料的傳輸是數位經濟貿易中非常重要的核心。

歐盟自身也非常仰賴國際貿易的情況下，數位貿易自然也是歐盟非常重要的經濟來源，正如前述有提及歐盟與印度、東南亞國家等，在服務業、數位貿易供應鏈上有密切的貿易合作關係。歐盟一味的限制歐盟公民的資料被傳輸出歐盟，等同增加了自身對外進行數位貿易的障礙與困難，同時這個障礙還是以歐盟規則的法律層級規範，歐盟各國沒有調整的空間，歐盟的貿易夥伴能免除障礙的方式卻皆是難以達成的要求。歐盟在保護其公民個人資料的人權的同時，可能也限制了自己公民的對外進行商業貿易的機會或讓數位貿易失去了其本身最強的優勢，即無國界與便利性 [292]。出於維護數位貿易的利益，最終卻可能攔阻了數位貿易本質上的優勢，這便是實施 GDPR 的歐盟未來可能面對的光景。因此面對這樣的情況，各國應走向彼此間規範的合作，透過相互承認的方式，以作為其兼顧資料保護與國際貿易的首要手段。

[292] Andrew D Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data Driven World: How WTO Law Can Contribut*e 22 J. INT. ECON. LAW,3 (2019).



DOI:10.6814/NCCU202000087

# 第四章 結論

網路與科技為國際貿易消除了地理國界帶來的障礙，為國際貿易更高度的自由貿易便利性。這樣無國界阻礙的自由貿易，讓「資料」的價值水漲船高，也同時開始讓人們重視數位資料的隱私。長久以來視隱私權為基本人權的歐盟首當其衝的以保衛歐盟公民數位資料之名實施了 GDPR，為資料隱私保護的法治立下里程碑，也成為各國隱私法修法上參考的範本。GDPR 的誕生讓人們重新理解資料的定義、資料處理應肩負的義務以及資料主體應對其資料有決定是否被處理的決定權。在網路虛擬世界裡蒐集、使用資料應遵守的規範，資料擁有者—資料主體被賦予的權利。

惟 GDPR 不只對國際上隱私保護規範帶來開創性的革新，對於國際貿易也帶來不小衝擊。從 GDPR 第三條對地域適用範圍的定義開始：GDPR 將適用於任何針對歐盟境內資料主體的資料蒐集、處理行為，不限該行為發生於歐盟境內，到最讓國際社會關注的規範：GDPR 原則禁止資料的跨境傳輸，只開放幾種例外允許，使得從 2016 年 GDPR 頒布之後國際間，各商業組織紛紛修正趕緊隱私保護政策。同時也讓國際社會不禁質疑 GDPR 地域適用範圍是否有過度擴張管轄權，並且原則上禁止資料的跨境傳輸，是否有不合致於 WTO 的義務規範。只開放幾種特定的例外允許途徑，包含國家層次的國家適足性認定、組織層次的 BCR 跟 SCC 以及取得資料主體同意，以允許資料合法跨境傳輸的情況下，乍看有提供多樣的例外允許途徑，是否實質上是難以通過的窄門，構成國民待遇的違反，或是最惠國待遇的違反。這也是本文研究的初衷跟動機，因此本文特別著重於了解 GDPR 資料跨境傳輸規範中，歐盟所提供的例外允許途徑本質及運作方式，另一方面整理 WTO 過去案例中與 GATS 規範中對於最惠國待遇、國民待遇、相互承認的解釋與判斷方式，試圖釐清 GDPR 是否有不合致於 WTO 規範。

透過整理歸納歐盟官方對於 GDPR 的解釋以及相關文件，並參考學界對於該議題探討的文獻，試圖進行分析之後，可以發現 GDPR 在法規合致性的面向上，並無具體的違反 WTO GATS 最惠國待遇義務、國民待遇義務、相互承認等



DOI:10.6814/NCCU202000087

規範。國家適足性認定雖因著看似很高的要求，同時又因歐盟先前跟美國簽訂了歐美隱私屏障協議，被質疑有違犯最惠國待遇義務的可能。最惠國待遇的違反必須建立在法規上有不平等或實質上有不平等，而實質上不平等需要該措施有很明確的只受惠於某第三國，但國家適足性認定實際上並沒有只受惠於特定國家，已有許多國家通過。此外進一步歐美隱私屏障協議的話，會發現其規範內容標準並沒有較 GDPR 的規範標準低，美國的資料處理者必須遵守歐美隱私屏障協議，是相當於其他國家資料處理者遵守 GDPR 的規範。BCR 跟 SCC 是提供歐盟境外企業合法傳輸資料的途徑，其中 BCR 雖因程序繁瑣、需耗費許多時間及金錢成本而有違反國民待遇的疑慮，僅增加境外企業的法遵成本並不能當然成立國民待遇的違反，且境外企業若通過 BCR 之認證後，實際上有助於企業集團內更有架構的執行資料保護，也可以維持資料處理的穩定性，因此亦對企業有所幫助。SCC 跟同意則因本質上是向資料主體尋求資料跨境及處理的同意，與歐盟境內企業欲處理歐盟境內資料時所需要徵求的資料主體同意是相同的，沒有涉及違反 WTO 規範的問題。在相互承認的分析上，國家適足性認定單方面設立規範要求他國符合該標準以確保資料跨境傳輸有一定的保障，雖然並非理想的手段，但因相互承認並未要求會員國一定要採用相互承認，因此亦未有違反相互承認的部分。

縱然經本文分析之後，GDPR 跨境傳輸的例外允許規範大部分並沒有實質違反 WTO 的規範，然而歐盟透過 GDPR 保護其資料的隱私與安全，即便在法規的層次上並沒有違反 WTO 的規範，然其所產生的影響也不完全都是有益於歐盟。尤其對中小企業而言，高度的資料保護管制是非常大的法遵負擔，這可能使得境外中小企業為考量成本，因此退出歐盟市場，使得在歐盟境內無法使用到一些網路上的服務或產品 [293]。除了造成歐盟境內居民的不便之外，這也會抑制創新的發展。此外其規範本身對境外企業而言，仍有許多在實踐上不易的部分。例如若資料處理者要透過 SCC 或取得資料主體的同意以跨境傳輸，由於 GDPR 要求徵求資料主體的同意時必須針對特定資料處理行為，而且是一次性的處理，

[293] Forbes Technology Council, *15 Unexpected Consequences of GDPR*, FORBES, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#2770880794ad(last visited Dec. 31, 2019).



DOI:10.6814/NCCU202000087

同時還要面對資料主體有任何時候撤銷資料處理的權利，因此對資料處理者而言是具有不確定性，也非常繁瑣的。在國家適足性認定方面，雖然其可能沒有違反最惠國待遇的規範，但當各國在追求歐盟所謂與其資料保護水準「相當」的標準時，對不同開發程度的國家而言實質上就有不同的困難程度，有的國家可能連資料隱私保護的規範都還在發展中，而這些國家可能跟歐盟在數位貿易上有密切的合作關係。在這樣的情況下，GDPR 反而可能成為歐盟跟其合作夥伴之間的貿易障礙，不利於歐盟。現今因著多邊協定已無法契合數位貿易的需求，各國在資料保護的規範上逐漸移轉到雙邊協定中，以確保資料跨境傳輸的流通與資料保護的兼顧，歐盟若能透過相互承認或簽訂協議的方式達成兼具資料保護與自由貿易的資料跨境傳輸，可能會比現行的國家適足性認定更適合。GDPR 是網路場域上資料規範重要的里程碑，隨著各國也紛紛跟進修改國內資料隱私法，國內的資料保護與維持國際間的數位自由貿易，如何在規範上的合作與平衡將持續是重要的議題，值得吾等研究與關注之。



DOI:10.6814/NCCU202000087

# 參考文獻

## 中文文獻

日本取得歐盟 GDPR 例外適足性認定，台灣經貿網，2019 年 1 月 24 日，https://reurl.cc/ObKN6g（最後瀏覽日：2020 年 1 月 13 日）。

林彩瑜，WTO 制度與實務：世界貿組織法律研究（三），2 版，頁 308（2013 年）。

國家發展委員會，歐盟對台歐展開 GDPR 適足性對話表示歡迎，國家發展委員會，2019 年 3 月 11 日，https://reurl.cc/72k4qN （最後瀏覽日：2019 年 12 月 31 日）。

凱君，創新金融模式下一步是 FinTech 還是 TechFin？，經濟日報，2019 年 6 月 5 日，https://money.udn.com/money/story/5613/3855248（最後瀏覽日：2019 年 12 月 31 日）

鈦媒體，馬雲和他的兆元級「長子」螞蟻金服，數位時代，2019 年 1 月 3 日，https://www.bnext.com.tw/article/51818/antfin-1000-billion-cny（最後瀏覽日：2019 年 12 月 31 日）。

印度 IT-BPM 資訊外包產業介紹(二之一)，台灣經貿網，2015 年 8 月 24 日，https://reurl.cc/pDekxZ（最後瀏覽日：2020 年 1 月 13 日）。

## 英文文獻

### 書籍

VAN DEN BOSSCHE, PETER & WERNER ZDOUC, THE LAW AND POLICY OF THE WORLD TRADE ORGANIZATION: TEXT, CASES AND MATERIALS 333 (3rd ed. 2013).

Aaditya Mattoo,Thomas Cottier(eds.),Petros C. Mavroidis(eds.), REGULATORY BARRIERS AND THE PRINCIPLE OF NON-DISCRIMINATION IN WORLD TRADE LAW 2 (2000).

### 期刊

Jan Philipp Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. L. REV. 288, 287-289 (2016).

Aaditya Mattoo, Joshua P. Meltzer, *International Data Flows and Privacy: the Conflict and Its Resolution* 21 J. INT. ECON. LAW 769, 779 (2018).



DOI:10.6814/NCCU202000087

Shin-yi Pent, 'GATS and the Over-the-Top (OTT) Services—A Legal Outlook', Journal of World Trade 50 (1), at 10-13.

R. Fefer, S. Akhtar &W. Morrison, *Digital Trade and US Trade Policy*, CONGRESSIONAL RESEARCH SERVICE (Nov. 5, 2018), https://fas.org/sgp/crs/misc/R44565.pdf.

Usman Ahmed, *The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade*, 18 WORLD TRADE REVIEW, 99-120 (2019).

Andrew D Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data Driven World: How WTO Law Can Contribut*e 22 J. INT. ECON. LAW, 3 (2019).

Meltzer, Joshua, *The Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & THE PACIFIC POLICY STUDIES 90, 90-102 (2013).

官方文件

OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).

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).

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, 2016 O.J. (L 119).

Draft Report on the Proposal For A Regulation of The European Parliament and of the Council on the Protection of Individual With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (COM(2012)0011–C7-0025/2012–2012/0011(COD)), EUR PARL. DOC. PE501.927V02 (2012).

Opinion of the Committee of the Regions on 'Data protection package', Dec. 18, 2012, 2012 O.J. (C391)127, at 127–133.

Executive Summary of the Opinion of the European Data Protection Supervisor on 'Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability', Feb. 20, 2016, 2016 O.J. (C67)13, at 13–15.

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.0, Adopted on12 November 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf [hereinafter Article 3 Guidelines].

Article 29 Data Protection Working Party, Guidelines on Consent under Regulation



DOI:10.6814/NCCU202000087

2016/679, Adopted on 28 November 2017, as Last Revised and Adopted on 10 April 2018, WP259 rev. 01

Article 29 Data Protection Working Party, Adequacy Referential (updated), Adopted on 28 November 2017, WP254.

2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539).

Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance, Dec. 29, 2014, O.J. L 385, at 74–84.

2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance), Feb. 12, 2010,O.J. L 39, at 5–18.

Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, Adopted on 11 April 2018, WP263 rev.01, at 1.

Group of Negotiations on Services, Uruguay Round, *Services Sectoral Classification List*, Note by the Secretariat, MTN.GNS/W/120, 10 July 1991WTO Committee on Specific Commitments, Report of the Meeting Held on 18 September 2014, Note by the Secretariat, S/CSC/M/71.

Comprehensive Economic and Trade Agreement Between Canada and the European Union and its Member States, Annex 9-B.

Privacy Shield Framework, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/welcome.

判決文件

Judgment of the Court (Grand Chamber), 13 May 2014.Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Request for a preliminary ruling from the Audiencia Nacional. Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8. Case C-131/12.

Case C-108/09, Ker-Optika bt v. ÀNTSZ Dél-dunántúli Regionális Intézete, 2010



DOI:10.6814/NCCU202000087

E.C.J. I-12213, ¶¶ 22, 28.

Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. Request for a preliminary ruling from the High Court (Ireland). Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities. Case C-362/14, ¶¶ 73, 74.

Panel Report, *United States-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 6.285–87, WT/DS285/R (Nov. 10, 2004).

Appellate Body Report, *United States— Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 215, WT/DS285/AB/R (April 7, 2005).

Appellate Body Report, *United States — Import Prohibition of Certain Shrimp and Shrimp Products*, ¶ 150, WTO Doc. WT/DS58/AB/R (Oct. 12, 1998).

Appellate Body Report, *Canada — Certain Measures Affecting the Automotive Industry*, WTO Doc. WT/DS139/AB/R (adopted June 19, 2000).

226 *Justice K S Puttaswamy v Union of India and Ors*, Supreme Court of India, Writ Petition (Civil) No. 494.

Panel Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc. WT/DS27/R/ECU (adopted on May 22, 1997).

Appellate Body Report, *European Communities - Regime for the Importation, Sale and Distribution of Bananas*, WTO Doc. WT/DS27/AB/R (adopted on Sept. 25, 1997).

Panel Report, *China - Certain Measures Affecting Electronic Payment Services*, ¶ 7.699, WTO Doc. WT/DS413/R (adopted on Aug. 31, 2012)

Appellate Body Report, *Argentina - Measures Relating to Trade in Goods and Services*, WTO Doc. WT/DS453/AB/R (adopted on May 9, 2016).

Panel Report, *European Economic Community - Imports of Beef from Canada*, ¶ 4.2-4.3, WTO Doc. L/5099 (Mar. 10, 1981).

網頁資料

Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, THE NEW YORK TIME (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-



DOI:10.6814/NCCU202000087

campaign.html?module=inline.

EUROPEAN COMMISSION, *Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Dec. 31, 2019).

EUROPEAN COMMISSION, *Binding Corporate Rules (BCR) Corporate rules for data transfers within multinational companies*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (last visited Dec. 31, 2019).

EUROPEAN COMMISSION, *List of companies for which the EU BCR cooperation procedure is closed*, EUROPEAN COMMISSION, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=61384 (last visited Dec. 31, 2019).

Forbes Technology Council, *15 Unexpected Consequences of GDPR*, FORBES, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#2770880794ad (last visited Dec. 31, 2019).

Daniela Fabian Masoch, *Why Should Companies Invest in Binding Corporate Rules*, ICLG, https://iclg.com/practice-areas/data-protection-laws-and-regulations/3-why-should-companies-invest-in-binding-corporate-rules (last visited Dec. 31, 2019).





DOI:10.6814/NCCU202000087