國立政治大學國際經營與貿易學系

碩士論文

新版標準契約條款在歐盟 GDPR 下之合法性分析

Legal Analysis of the New Standard Contractual Clauses under EU GDPR

指導教授：薛景文博士

研究生：楊和潤 撰

中華民國 113 年 7 月

謝辭

回顧這三年的研究所時光，有過酸甜苦辣，但始終感謝有這個機會能夠進入這個融合法學和商學的系所就讀，有機會跳脫傳統法學院的角色，讓我能夠以商學院的角度重新看待許多事物，一路上真的看到許多以往未曾看過的風景。感謝法組四位老師——大楊老師、施老師、小楊老師、薛老師的悉心教導，也感謝國貿所其他組別的老師不厭其煩地帶領我理解商學的知識，感謝口試委員兆恬老師、小楊老師給予我許多寶貴的建議。

以及想感謝青璿、奇哥，我總是透過你們，看到更大的世界。我們是如此截然不同；卻又在某些地方保持如此相似，還有詹晉，一路上以來的音樂好夥伴，能連續在兩個城市相聚，是很棒的緣分。感謝在法組遇到的同學們，Evan、宇倫、楷勛、思妤、Jenny、家卉、語萱，我想我會一直記得我們在法學中心一起奮鬥的時光，有你們並肩作戰，對我來說也是意義非凡，還有想感謝我的家人，讓我能無後顧之憂的完成研究所的學位，謝謝你們！

最重要的還是要感謝我的指導教授薛景文老師，能夠加入您的門下撰寫碩士論文，是我的榮幸，感謝您每次 meeting 時總是給予我許多實質的建議，有時不知如何繼續的徬徨在 meeting 後總能茅塞頓開。這段時間在您的指導下收穫良多，希望未來仍能保持交流切磋。

楊和潤

誌於 國立政治大學達賢圖書館

2024 年 7 月 31 日

摘要

在現今數位爆炸之時代下，人們的日常生活已與網際網路密不可分，而現今各式新興科技之背後，均須以大量之個人資料作為其基礎與分析改善之動能，依今日網路技術之發展及全球化商業佈局之普遍程度，資料需要在許多不同國家間跨境傳輸已是無法避免之必要行為。不料歐盟法院於 2015 年及 2020 年相繼宣告美歐間《安全港協議》及《隱私盾協議》失效，使美歐間之資料跨境傳輸頓失合法依據，惟 Schrems II 案判決中，仍側面肯定以標準契約條款（Standard Contractual Clauses, SCC）進行跨境傳輸之合法性，歐盟執委會於 Schrems II 案後積極進行相關修訂，並於 2021 年 6 月正式通過新版之 SCC 條款，此一新版之 SCC 條款，整合過去三份 SCC 並加入兩種新的傳輸情境，形成依不同傳輸情境區分之四個模組（Module）的特殊規範模式，並針對 Schrems II 案中歐盟法院之擔憂於第 14 條、第 15 條新增若干義務。

不料於 2023 年，愛爾蘭資料保護委員會認為 Meta 以 2021 新版 SCC 作為合法依據之跨境傳輸不合法，並裁罰 Meta 12 億歐元。本文以此案件作為發想，惟不限於本件裁罰案討論之範疇，而係全面性之比較 2021 新版 SCC 與歐盟 GDPR 之規範差異，及透過若干歐盟法院判決、監管機關裁罰案件及指引、學者見解等，進一步分析 2021 新版 SCC 於歐盟規範架構下之合法性，最後加入若干本文自身觀點，期望能提供企業若欲選擇以 SCC 作為資料跨境傳輸合法依據者，在面對 2021 新版 SCC 可能仍無法完全解決歐盟法院於 Schrems II 案擔憂之前提下，應注意 2021 新版 SCC 有哪些法律上之重點缺失，以及得採取何種補充措施以制訂長久合法有效的資料跨境傳輸契約。

關鍵詞：歐盟一般資料保護規則、GDPR、標準契約條款、SCC、歐盟基本權利憲章、Schrems、Meta、個資保護、隱私權、跨境資料傳輸、資料跨境傳輸

Abstract

In today's era of digital explosion, people's daily lives are inextricably linked with the internet. The basis for the analysis and improvement of various emerging technologies relies heavily on large amounts of personal data. Given the current development of internet technology and the widespread extent of global business layouts, the necessity of cross-border data transfer between many different countries has become an unavoidable requirement. However, the European Court of Justice (CJEU) successively invalidated the Safe Harbor Agreement and the Privacy Shield Agreement between the U.S. and the EU in 2015 and 2020. Nonetheless, the Schrems II case still indirectly affirmed the use of Standard Contractual Clauses (SCC) as a legal basis for cross-border data transfer. Following the Schrems II case, the European Commission actively made relevant revisions and officially passed the new version of SCC clauses in June 2021. This new version of SCC integrates three previous SCCs and adds two new transfer scenarios, forming a special regulatory model divided into four modules based on different transfer scenarios. It also added several obligations in Articles 14 and 15 to address the concerns of CJEU in the Schrems II case.

Unexpectedly, in 2023, the Irish Data Protection Commission deemed Meta's cross-border transfer, which based on the 2021 new SCC was illegal and fined Meta €1.2 billion. This paper uses this case as an inspiration, but not limited to the scope of this case. This paper comprehensively compares the regulatory differences between the 2021 new SCC and the EU GDPR, further analyzes the legality of the 2021 new SCC under the EU regulatory framework through several EU court cases, regulatory authority penalty cases, and scholarly opinions, and finally adds several of the author's viewpoints. It aims to provide enterprises, intending to choose SCC as a legal basis for

cross-border data transfer, with insights into the legal shortcomings of the 2021 new SCC and suggests possible supplementary measures to formulate a long-term, legal, and effective cross-border data transfer contract.

Keywords: General Data Protection Regulation, GDPR, Standard Contractual Clauses, SCC, EU Charter of Fundamental Rights, Schrems, Meta, data protection, privacy rights, cross-border data transfer

目次

表目錄

簡稱對照表

簡稱	英文全名	中文翻譯
GDPR	General Data Protection Regulation	歐盟一般資料保護規則
Directive 95	Data Protection Directive 1995	歐盟 1995 年資料保護指令
SCC	Standard Contractual Clauses	標準契約條款
DPF	《EU–US Data Privacy Framework》	歐美資料隱私架構協定
EDPB	European Data Protection Board	歐盟資料保護委員會
EDPS	European Data Protection Supervisor	歐盟資料保護監督機構
WP29	The Article 29 Working Party	歐盟第 29 條工作小組
DPA	Data Protection Authorities	各國之資料保護機關
LSA	Lead Supervisory Authority	系爭案件主責機關
CJEU	Court of Justice of the European Union	歐盟法院
BCR	Binding Corporate Rules	拘束性企業規則
CoC	Code Of Conducts	行為準則
DPIA	Data Protection Impact Assessment	資料影響評估
TIA	Transfer Impact Assessment	傳輸影響評估

第一章 緒論

第一節 研究動機與目的

在劃時代的 Schrems I[1]及 Schrems II[2]案判決中，歐盟法院相繼宣告美歐《安全港協議》[3]及《隱私盾協議》[4]失效，使美歐間之資料跨境傳輸合法依據為何，頓時罩入難見天日的烏雲之中，惟 Schrems II 案判決中，仍側面肯定以標準契約條款（Standard Contractual Clauses, SCC）作為跨境資料傳輸之合法依據，故 SCC 普遍被認為係後 Schrems II 時期最可能通過歐盟法院合法性審查標準之希望。

考量到 SCC 上次修訂已是 2010 年，當時之歐盟資料保護法律基礎仍為歐盟 1995 年資料保護指令（Data Protection Directive 1995, Directive 95），若要以 SCC 作為跨境傳輸之主要合法依據，似有通盤檢查更新之必要，故歐盟執委會於 Schrems II 案後積極進行相關修訂，並於 2021 年 6 月正式通過新版之 SCC 條款，此一新版之 SCC 條款，不僅將法律基礎更新至歐盟一般資料保護規則（General Data Protection Regulation, GDPR），也將過往針對不同傳輸情境之三份 SCC 進行統合，並加入兩種新的傳輸情境，形成依不同傳輸情境區分之四個模組（Module）的特殊規範模式，並針對 Schrems II 案中歐盟法院之擔憂於新版 SCC 第 14 條、第 15 條進行規範，亦即第 14 條規定締約雙方須於資料傳輸前，針對資料輸入方之國內法律或實務作法是否會與此 SCC 條款相衝突；以及是否須採取其他更多

[1] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (Oct. 6, 2015) [hereinafter Schrems I].
[2] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (July 16, 2020) [hereinafter Schrems II].
[3] 2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council 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, 2000 O.J. (L 215) [hereinafter Safe Harbor].
[4] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) [hereinafter Privacy Shield].

之技術性措施或組織性補充措施以加強對資料之保護，進行資料傳輸影響評估（Transfer Impact Assessment, TIA），而傳輸行為存續之過程中，雙方亦負有持續評估、不斷更新之義務。另一方面，第 15 條則係針對第三國政府機關監控之問題所生，即當資料輸入方之政府機構向其要求提供資料主體之個人資料時，資料輸入方應於符合該國國內法要求之情況下，以資料給予最小化之原則為之。另外，於同意該公部門之要求給予資料或獲知該公部門已直接存取資料後，資料輸入方應評估該公部門之要求或行為是否確實符合該國國內法律及相關國際法標準，若於評估後有相當理由認為該公部門之要求或行為有合法性之疑慮，資料輸入方應盡力為資料主體尋求救濟或上訴。

然而，2023 年 5 月，一件由愛爾蘭資料保護委員會對 Meta Ireland 之裁罰案件卻為 SCC 作為跨境資料傳輸合法性主要基礎之未來，再度蒙上陰影[5]，本件為 Schrems II 案判決後，美歐間企業採用 2021 新版 SCC 作為資料跨境傳輸法律基礎之第一個重大案件，其指標性之意義不言可喻。愛爾蘭資料保護委員會遵照歐盟資料保護委員會（European Data Protection Board, EDPB）之裁決，認為 Meta 在 Schrems II 案判決後仍持續進行美歐間跨境資料之傳輸，且亦未具備其他能足以符合 GDPR 及歐盟基本權利憲章之合法依據，故裁決（1）Meta 須負擔 12 億歐元之罰款；（2）在六個月內停止資料處理行為及將儲存在美國之歐盟公民個人資料刪除。令人好奇的是，歐盟法院在 Schrems II 案中曾肯定使用 SCC 作為跨境資料傳輸之合法依據，又 Meta Ireland 及 Meta 間之跨境資料傳輸契約即係以 2021 新版 SCC 為基礎簽訂，何來無合法基礎之說？為何 EDPB 會認為 2021 新版 SCC 並無法作為資料跨境傳輸之合法依據，實耐人尋味。另外本件 Meta 公司已將案件提交至歐盟法院，後續歐盟法院是否將採取與 EDPB 相同之見解，值得

[5] In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited) Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation Further to an own-volition inquiry under Section 110 of the Data Protection Act 2018, Data Protection Commission Ireland (Adopted on May 12, 2023) [hereinafter Meta 2023 case].

持續關注。

本篇論文以本件愛爾蘭資料保護委員會對 Meta 之鉅額裁罰案件作為發想，惟將不以此單一案件為囿，而係擬全面性之比較 2021 新版 SCC 與歐盟 GDPR 之條文內容，輔以相關之判決、裁決，以及學者見解，審視 2021 新版 SCC 之內容於歐盟 GDPR 及相關規範架構下是否適法，進而對於 SCC 作為美歐間資料跨境傳輸合法依據之現況及未來進行釐清及評析。期望能提供企業若欲選擇以 SCC 作為資料跨境傳輸合法依據者，在面對 2021 新版 SCC 可能仍無法完全解決歐盟法院於 Schrems II 案擔憂之前提下，應注意 2021 新版 SCC 有哪些法律上之重點缺失，以及得採取何種補充措施以制訂長久合法有效的資料跨境傳輸契約。

第二節 研究方法

本篇論文擬採用「文義解釋法」、「案例分析法」及「文獻分析法」，透過將歐盟 GDPR 條文與 2021 新版標準契約條款(SCC)作一全面綜合性之比較分析，並輔以歐盟法院判決及各成員國監管機關所裁罰之案件、EDPB 及其前身歐盟第 29 條工作小組（以下簡稱 WP29）所發布之相關指引（guideline）／建議（recommendation）、其他政府機關所發布之相關文件、非營利組織提出之看法、學者所發表之期刊論文，針對法律上之規範差異、歐盟法院或監管機關之實務發展等進行觀察，以分析 2021 新版 SCC 在歐盟 GDPR 規範架構下之合法性。

第三節 研究範圍

本篇論文之研究範圍包含歐盟 GDPR 條文本身、2021 新版 SCC 條款、過去各版本之 SCC 條款沿革、EDPB 所發布之指引及建議（包含其前身 WP29 所發布者）、歐盟法院之判決（包含影響最為重大之 Schrems I 及 Schrems II 案）、歐盟各成員國所發布之重大裁罰案件，包含促使本篇論文研究緣起之愛爾蘭資料保

護委員會裁罰 Meta 12 億歐元案件。

另外，因本篇論文所著重之面向為適用於私人間之 SCC 合法性分析，故雖於相近之時間，美歐第三版資料跨境傳輸協定 DPF 正式通過施行，亦可能作為美歐資料跨境傳輸合法性依據的解方之一，同時也極有可能作為 Schrems 挑戰之對象，惟本文由於寫作方向之設定，將不著重太多篇幅討論第三版資料跨境傳輸協定 DPF 之合法性問題。另一方面，本篇論文設定之討論方向為著重在提供私部門因應方案之觀點，GDPR、DPF 與 SCC 間尚有諸多政策考量及國際關係之面向，本論文礙於篇幅及方向設定之故，無法逐一討論，可能得留待其他較為公法面向之論文進行探討，一併敘明。

第四節 研究架構

本篇論文第二章先介紹歐盟關於跨境資料傳輸之規範架構，首先釐清資料跨境傳輸之必要性及其應用範圍，再介紹歐盟 GDPR 之整體架構及相關機關之職責，接著就 GDPR 針對跨境傳輸之規範進一步介紹，包含全面資料在地化之可行性，以及各項 GDPR 所規定之例外合法事由。

第三章則為新版 SCC 及歐盟 GDPR 全面性之規範比較，首先由歷史各版本 SCC 之沿革，到 2021 新版 SCC 之內容簡介，再分別依序就資料處理原則、資料主體權利、資料管控者／處理者義務、監管與救濟等方面，將新版 SCC 之條文與歐盟 GDPR 之規範作一比較，以瞭解新版 SCC 在規範上是否與 GDPR 有所落差。

並於第四章進一步針對此些落差進行新版 SCC 及歐盟 GDPR 之合致性分析，即此些落差是否導致新版 SCC 在對於歐盟公民之保障密度上，未達到 GDPR、歐盟基本權利憲章以及歐盟法院在過往案件中揭示之保護水準，進而導致新版 SCC 具有合法性上之疑慮，並搭配最新之愛爾蘭裁罰 Meta 12 億歐元案件，以瞭

解 EDPB 對於新版 SCC 之態度及監管趨勢，最後於第五章回顧本篇論文之重點及發現，並作一結論。

第二章 歐盟跨境資料傳輸規範架構

第一節 跨境傳輸之必要性及應用範圍

第一項 資料跨境傳輸之必要

在現今資訊爆炸的數位時代，人們的日常生活已與網際網路密不可分，一天當中舉凡獲知新聞不再透過傳統的報紙而係網路新聞、有許多串流服務提供者取代舊有的有線電視、購買餐點及各種物品透過手機行動支付或信用卡等工具進行付款，而漸漸減少實體紙幣的使用率、人與人間的社交活動亦大幅度的轉移到社群媒體上等等。從商業活動的角度來看亦是如此，而得以使這些創新服務在資訊時代順利運行的一個重要因素即是資料(data)，各大公司為了提供更好的服務，必須更了解消費者或使用者的需求、使用習慣等，故需要對個人資料進行蒐集、分析，不僅是一般民眾最容易想像到的大型科技公司(如：Meta、X、Google 等)，其他各式各樣的行業如金融業、服務業、電信業、製造業...等等亦須在其提供服務的過程中蒐集各種個人資料。而當中資料的傳輸常透過雲端等方式進行傳送、儲存等，不僅現今許多跨國公司可能於業務範圍內即須將資料進行跨境傳輸，背後雲端儲存、資料傳送的過程亦可能因伺服器、儲存位置架構之不同，而將許多的個人資料，在一般民眾甚至是企業本身毫無知覺的情況下，流通經過不同的國家。依現今的網路技術發展及全球化商業佈局之普遍，資料需要在許多不同國家間跨境傳輸已是許多企業無法避免之必要行為[6]。

[6] Casalini, F. and J. López González, Trade and Cross- Border Data Flows, 220 OECD TRADE POLICY PAPERS 10 (2019).

第二項 資料是如何被跨境傳輸

在正式討論資料跨境傳輸之法制議題前，本文將先簡要介紹在事實技術面上，資料究竟是如何被跨境傳輸的。首先，每個上網的裝置都有專屬於自己的 IP 位置，每個 IP 位置都是獨一無二的，就好比是網路世界的身分證一般。當資料要進行傳輸時，這些資料會先被拆散成數個「小包裹」，這些「小包裹」中包含發信人的 IP 位置、收信人的 IP 位置，以及待小包裹抵達目的地時該如何重組的順序代碼，一旦這些資訊準備就緒，這些小包裹就會離開原始之的裝置，通過不同的網路、路徑前往目的地，在這過程中，網路會透過路由器（Routers）引導資料通過，確保他們採取最短或最不耗時的路徑。而當小包裹皆抵達目的地後，收信人的裝置即會依據前述之順序代碼將小包裹們重新組裝，還原回原始的資訊。而雖然小包裹會採取什麼路徑抵達目的地難以事先預測，但事後可以透過一定之方式追蹤到它們的傳輸路徑[7]。

第三項 資料跨境傳輸之應用範圍

如前所述，現今各行各業均有可能、或甚至是「必須」於其業務範圍內進行資料跨境傳輸。而近年許多正迅速發展中之新興技術更是如此，以 AI 相關之各種產業為例，即係以大量之資料作為其提供創新技術之背景資源，透過獲取大量使用者之個人資料，取得許多使用上之經驗及軌跡，故得以更精準地掌握現行提供之服務有何缺失之處，進一步提升服務的品質。諸如物聯網、電動車等產業，均係不斷地將裝置上之各項數據資料，回傳回母公司進行分析，並不斷優化軟體、韌體面之程式，使其符合搭配現有的硬體，帶給使用者不斷更新

[7] *Id.*

的使用體驗[8]。甚至是金融科技之各項運用亦是如此，舉凡是網路銀行的普及，許多的業務皆可以在手機上一指完成，省去跑實體銀行的等待及作業時間；API 應用程式介面，即傳統金融業者與其他領域之業者合作，使得民眾可以透過通訊軟體的 app 即完成轉帳或繳費的功能，或與其他泛金融產業如租賃業、汽車金融業合作，透過 API 即得達成「一站式」完成所有步驟，顯著地提升使用者體驗；以及近年十分火熱的群眾募資，金融科技亦在此領域提供相當之助力，蓋傳統跨境支付之流程繁瑣、時間耗費較長、亦通常會收取相當比例之手續費，金融科技之應用能有效改善傳統金融方法於此項領域之缺點[9]。而這些獲取、傳輸資料加以分析的過程，往往都會伴隨著資料跨越傳統地理疆域之跨境傳輸。

第二節 簡介歐盟資料管制架構

第一項 歐盟一般資料保護規則（GDPR）

在 2016 年正式通過之 GDPR，不僅快速攫取全球之目光，亦成為歐盟對於個資保護之最大支柱，其延續「歐盟 1995 年資料保護指令（Data Protection Directive 1995, Directive 95）」[10]之規範架構，並於此一基礎上，進一步強化歐盟對於隱私權之保障。

承前所述，在 GDPR 問世之前，在歐盟層級中針對個資保護之代表法規，即是於 1995 年訂立之 Directive 95，該法制定之時成為歐盟對於個資保護之一大創

[8] *See* Julian Schütte & Gerd Stefan Brost, LUCON: Data Flow Control for Message-Based IoT Systems, 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering, Institute of Electrical and Electronics Engineers, 1-2 (Aug., 2018).

[9] *See* GREGOR DORFLEITNER & LARS HORNUF, FINTECH AND DATA PRIVACY IN GERMANY 3-6 (2019).

[10] 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, OJ L 281, 23.11.95. [hereinafter Directive 95].

舉，其係為促進歐盟內部市場流動及調和歐盟各成員國間對於個資保護水準之不同而生。又雖其係以「指令」之方式立法，即提供一指引性之準則，供歐盟各成員國各自於國內立法形成，然其對於統一歐盟各國對於個資保護之密度及強度而言，亦有極大之貢獻，即首次形成歐盟層級之一致性最低標準。然而，Directive 95 制定之時空背景係於網際網路仍未發達之時代，隨著時間的推演，網際網路之技術不斷進步，4G、5G 通訊技術相繼問世，AI 等人工智慧應用逐步在吾人的日常生活當中普及，原先之技術背景已大幅演進，相對應之個資保護法規亦有隨之調整之必要。經過漫長之討論，歐盟理事會（Council of Europe）及歐洲議會（European Parliament）於 2016 年 4 月 27 日正式通過 GDPR，並規定於 2018 年 5 月 25 日正式施行，且由於其係以「規則」之方式立法，故無庸等待各成員國於國內立法，本規則即於歐盟境內全面生效，各成員國皆須遵守之。以下簡介 GDPR 之立法架構：

一、立法目的

GDPR 之立法目的係在個資保護（涉及隱私權）及資訊流通自由（涉及廣義之言論自由）兩大憲法基本權當中，透過適當之立法設計，謀求符合歐盟公民基本權利及福祉之最大平衡，在不過度限制資訊流通自由之前提下，對於歐盟公民之個人資料及隱私權提供適足之保障[11]。

二、適用範圍

GDPR 之所以受到全球如此廣大矚目的原因之一，即在於其不單單僅在歐盟

[11] GDPR recital 4 (“The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.”).

領域內具有拘束力，而具有「域外適用」之效力。GDPR 第 3 條第 1 項規定，只要在歐盟境內設有營業據點者，不論其對資料之處理是否於歐盟領域內進行，均須受到 GDPR 的規範；同條第 2 項即為域外適用之條款，其規定雖在歐盟領域內「無」營業據點，然對於歐盟之公民提供商品／服務或監控其行為者，亦須受到 GDPR 之拘束[12]。又，為避免適用範圍過寬，歐盟資料保護委員會（European Data Protection Board, EDPB）於 2018/3 指引文件中進一步解釋限縮域外適用之範圍，即限縮在「有意以位於歐盟市場之自然人為特定目標，排除無意或偶然之行為」，即加入主觀要素之判斷，排除僅係偶然間不慎蒐用到歐盟領域內自然人之個資，非具商業意圖之行為[13]。

三、相關主體及行為定義

（一）管控者（controller）係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關或其他機構；依照歐盟法或成員國法決定處理之目的及方法，由歐盟法或成員國法律規定管控者或其認定之具體標準[14]。

（二）處理者（processor）係指代管控者處理個人資料之自然人或法人、公務機關或其他機構[15]。

---

[12] 此處所謂「位於歐盟境內之公民」，不以具備歐盟成員國國籍者為限。GDPR arts. 3(1), (2) (“1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not; 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.”).

[13] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, Adopted on 12 Nov. 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

[14] GDPR art. 4(7) (“‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”).

[15] GDPR art. 4(8) (“‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”); 處理者和管控者可能為同一人，即管控

（三）處理（processing）係指對個人資料或檔案執行之任何操作，且不問是否係透過自動化方式為之，例如蒐集、記錄、組織化、結構化、儲存、改編或變更、檢索、查閱、使用、揭露或以其他方式使之得以調整或組合、限制、刪除或銷毀等[16]。

四、資料處理基本原則及資料主體權利

GDPR 第 5 條列出六大資料處理之基本原則，此些原則在資料蒐集利用之各階段均須遵守之，且不論資料管控者或處理者取得資料處理之合法事由為何，均不影響第 5 條基本原則的要求，有合法性、公平性與透明性原則；目的性原則；最小化蒐用原則；正確性原則；儲存時間最短化；資料完整性及保密性等[17]。

而資料主體權利方面則包含有知情權（或稱被告知權）；資料主體向資料管控者確認自己的個資是否被蒐集利用，及取得相關資訊之接近使用權；刪除權（或稱被遺忘權）；針對自動化處理程序之限制個人自動化決策與剖繪權等等[18]。

五、資料管控者與處理者義務

相對地，資料管控者及資料處理者亦負有一定之義務，諸如確保資料處理安全性；個資侵害事件之通報／通知義務；相關處理行為之紀錄義務；與監管機關合作；資料影響評估與事前諮商義務等等[19]。

六、跨境資料傳輸

者自行處理資料之情形。

[16] GDPR art. 4(2) ("'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.").

[17] GDPR arts. 5(1), (2); 張陳弘、莊植寧，新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，2 版，頁 63-67（2022 年）。

[18] GDPR arts. 12-22.

[19] GDPR arts. 24-36.

GDPR 針對資料從歐盟境內傳輸至非歐盟地區，或自非歐盟地區傳輸至歐盟境內（即合稱跨境傳輸）所採取之立場係「原則禁止，例外許可」，意即原則上禁止資料跨境傳輸，只有在符合 GDPR 所訂之幾種特殊情形下，始得例外准予進行之。而最常被使用之例外規範有以下幾種：（一）該國家取得歐盟資料保護委員會及歐盟執委會通過之「適足性認定」[20]；（二）以「雙邊協商」方式取得適足性認定，在此一方式中，申請國較似立於平等之地位與歐盟進行協商談判後，簽訂資料傳輸協定，雙方皆得在某些保護之面向或密度上互相讓步；（三）使用企業自我拘束規則（Binding Corporate Rules, BCRs）並獲得歐盟成員國個人資料保護主管機關之核准[21]；（四）使用經監管機關核准之行為準則（Codes of Conduct）[22]（五）採用歐盟執委會或成員國個人資料保護主管機關發布之標準契約條款（Standard Contractual Clauses, SCC）[23]；（六）取得當事人同意[24]等方式，始得例外進行跨境資料傳輸。

七、行政裁罰之金額

GDPR 對於行政裁罰之金額，分別依違反之規範類型，設有兩種不同之金額上限，分別是自最高一千萬歐元或企業之前一會計年度全球營業額之 2%，取其高者作為上限；以及自最高兩千萬歐元或企業之前一會計年度全球營業額之 4%，取其高者作為上限[25]。

第二項 相關機關之職責

一、各國之資料保護機關（Data Protection Authorities, DPAs）

[20] GDPR art. 45(1).
[21] GDPR art. 46(2)(c).
[22] GDPR art. 40.
[23] GDPR art. 46(2)(b).
[24] GDPR art. 49(1)(a).
[25] GDPR arts. 83(4)-(6).

在 GDPR 的架構下，歐盟各成員國均於自己國家境內設有資料保護機關（如愛爾蘭資料保護委員會、法國國家資訊自由委員會等），GDPR 第 56 條至 58 條分別就其權限（competence）、任務（task）及擁有之權力（powers）分別列有詳盡之規定，包含監控本規則於該成員國內之適用情形；對國會／政府機構立法或制定行政規則時給予建議；進行第 41 條至第 43 條所述之各項認證；對資料管控者進行調查，並命其提出調查所須之一切資訊、證據；對資料管控者進行限制禁令、乃至於依 GDPR 第 82、83 條規定進行裁罰等，均授權得由各國 DPA 為之[26]。

而在資料跨境傳輸的案件，為避免公司須在同一事件向多個歐盟成員國 DPA 進行通報之煩，或係整體考量到發生個資侵害事件時，GDPR 第 33 條規定之可行性，即資料管控者須於知悉後 72 小時內進行通報之義務，實際上難以期待在如此短的時間內，資料管控者有能力向所有涉及之歐盟成員國 DPA 完成通報，故 GDPR 及其專責機關 EDPB 設有一套「一站式紛爭解決機制（one-stop-shop mechanism）」以便管控者完成通報[27]。

以下簡述一站式紛爭解決機制之流程：（1）首先，當有資料主體提出或 DPA 依職權主動開啟一案件時，會先依據 GDPR 第 56 條之規定，即該管控者主要機構所在地之監管機關，有權作為此一跨境資料事件之主責機關（Lead Supervisory Authority, LSA），並由其主要代表其他所有 DPAs 作為此一事件之窗口[28]；（2）LSA 在充分進行調查及與其他 DPAs 交換資訊後，會草擬一份決議（decision），並詢問所有 DPAs 就此決議有無意見；（3）若有 DPA 提出附具理由之不同意見且與 LSA 僵持不下，LSA 可將案件移交給 EDPB 作成具有拘束力之裁決（binding

[26] Sofija Voronova and Anna Nichols, *Understanding EU Data Protection Policy*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE (May, 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf; GDPR arts. 52, 56-58, 82-83.
[27] GDPR art. 33.
[28] GDPR art. 56.

decision）。藉此方式使得案件中涉及之各個 DPA 均得充分表達自身之意見，又兼顧程序之一致性及迅速之效[29]。

二、歐盟資料保護委員會（EDPB）及歐盟資料保護監督機構（EDPS）

EDPB 係 GDPR 立法所設立之獨立專責機關，EDPB 主要的功能除了會定期發布關於 GDPR 之解釋指引（guidelines），以利各界更清楚了解 GDPR 法規意旨及規範範圍與適用情境。蓋 GDPR 之大部分規定均係原則性、大範圍的立法，實際適用上，亦或是特定問題上更為細緻之法規解釋，未必能在有限之法條文字中表達周全，為使各界於面對 GDPR 時得以更明確瞭解其規範內涵，EDPB 在此扮演舉足輕重的角色。

EDPB 之另一重要功能即係和歐盟資料保護監督機構（European Data Protection Supervisor, EDPS）攜手合作，協調歐盟各國 DPA 間之相互運作、以及各國 DPA 與歐盟間之合作，包含在前述一站式機制下擔任最終有權做出拘束性裁決、為紛爭暫時劃下休止符的角色[30]。

而 EDPS 則有以下三大功能：（1）監督歐盟機構、歐盟各政府機關之行為是否遵守隱私權及個資保護之相關規定，此一功能使得 EDPS 可說是歐盟這個組織本身的 DPA。（2）擔任歐盟政府於個資保護方面的智庫角色，提供歐洲理事會、歐盟執委會、歐洲議會等機構關於個資保護相關問題之諮詢（consultation）對象，其中亦包含針對各式日新月異的新型技術出現，歐盟應採取何種行動因應，以確保個資保護之強度及方式得以跟上科技之最新發展。（3）和 EDPB 一起促進協調各 DPA 間之運作，如 EDPS 甚至須指派秘書（secretariat）至 EDPB，確保雙方溝通聯繫的管道維持順暢[31]。

---

[29] *Tasks and Duties*, EUROPEAN DATA PROTECTION BOARD, https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en (last visited Jan. 18, 2024).
[30] *Id.*
[31] *About Us*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/about/about-us_en;

第三節 GDPR 針對跨境傳輸之規範

早在 GDPR 實施前，其前身 Directive 95 即有針對跨境傳輸設有明文規範，如 Directive 95 第 25 條第 1 項規定：「因資料處理而傳輸至第三國，或擬傳輸至第三國進行處理的個人資料，成員國應確保第三國在資料保護上已具「適足性水準」，始能將個人資料由歐盟傳輸至境外[32]。」同條第 2 項並規定歐盟執委會有權確認資料接收國／地區的保護水準是否已達適足性之要求[33]。

而來到 GDPR 時代，GDPR 在延續 Directive 95 的基礎下，針對資料之跨境傳輸亦設有相關之規範，延續「原則禁止、例外許可」的態度，並僅有在滿足若干例外規範時始得進行跨境資料傳輸，如：適足性認定、雙邊協商、拘束性企業規則（BCR）、行為守則（CoC）、標準契約條款（SCC）、取得當事人同意等。

另外，有論者亦提出，在 Schrems II 案後全球是否應朝向所謂「資料在地化」之立法模式，要求資料均在地儲存、減少跨境傳輸之行為。本章將首先分析為何資料在地化之立法模式於今日國際社會並不可行，再針對各個例外事由之規範進行介紹。

Frequently Asked Questions, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/frequently-asked-questions_en (last visited Jan. 18, 2024).

[32] Directive 95 art. 25(1) ("The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.").

[33] Directive 95 art. 25(2) ("The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.").

第一項 資料在地化

在全球矚目之美歐《安全港協議[34]》及《隱私盾協議[35]》等雙邊適足性協商相繼於 Schrems I 案[36]、Schrems II[37]案中被歐盟法院宣告失效時（此部分介紹待本章第二項第二款後述），縱使仍有 SCC 可暫時作為美歐資料跨境傳輸之替代方式，然歐盟法院的這兩個判決似乎已形成歐盟單邊決定的資料硬疆界，有論者亦提出是否應採取所謂「資料在地化」作法之論點，以及資料在地化之立法是否適合作為目前全球資料法制之新趨勢[38]。

首先，提倡資料在地化者多提倡資料在地化模式有以下好處，如便利國內執法，涉及不同國家間跨境資料之刑事案件，內國執法機關僅能透過司法互助協議等方式，請求其他國家之合作以調查儲存於境外伺服器之資料或相對應之資料庫，過程十分繁雜且有時成效不彰，若資料強制被儲存或留存一份相同的副本在境內，將可大大改善執法上之效率。其他亦有回應 Schrems II 案中保障公民隱私避免受到他國監控者，蓋儲存於境外之資料，係受到該地（即第三國）之內國個資保護法保護及影響，然世界上不同地方之個資保護立法密度及品質不一，若公民遭遇其他國家行政機關之監控時，未必能尋獲適當之救濟管道以進行救濟，類似之擔憂亦可從歐盟法院於 Schrems II 案中一再強調美國情報單位對歐盟公民之監控

[34] 2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council 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, 2000 O.J. (L 215) [hereinafter Safe Harbor].

[35] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) [hereinafter Privacy Shield].

[36] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (Oct. 6, 2015) [hereinafter Schrems I].

[37] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (July 16, 2020) [hereinafter Schrems II].

[38] Anupam Chander, *Is Data Localization a Solution for Schrems II*, 23(3) JOURNAL OF INTERNATIONAL ECONOMIC LAW 771 (2020).

行為，及缺乏正當程序救濟管道看出[39]。

次按所謂「資料在地化」之概念實則有兩種表現方式，(1)「要求公司將資料儲存於境內」: 如網路伺服器之位置、自建機房擺放儲存網路伺服器、亦或是使用雲端運算技術者，將資料儲存於雲端運算服務提供者所建置的資料庫亦屬之；(2)「限制資料傳輸至境外」: 而限制資料傳輸至境外之方式，亦是另一廣義的資料在地化樣態，蓋其透過限制資料跨境傳輸之立法，造成資料難以在國與國之間流通，間接形成資料在地化之效果[40]。

歐盟於 Directive 95 時期即採取「原則上禁止資料跨境傳輸、例外許可」之態度，而到現代之 GDPR 亦延續這樣的精神，明顯偏向上述第二種方式，而這樣的情況在 Schrems II 案後更為明顯，甚至可能造成資料鎖國化、不利國際經貿發展的後果。

然而，本文認為資料在地化之立法不僅無法正面回應歐盟法院所擔憂之情形，且於今日國際經貿往來頻繁、科技快速發展的社會，資料在地化之立法可能僅存在於理想之間，於現實並不可行，理由分述如下：

一、為何資料在地化無法解決歐盟法院的擔憂

（一）無法真正解決美國政府情報單位監控之問題

美國進行國際監控的方式、來源已十分多樣，即使強制要求資料需儲存於歐盟境內，外國機關仍可透過在國外設定惡意軟體、內部人員攻擊和其他種種方式，以達成獲取目標情報之結果，是以限制資料跨境傳輸未必能根本解決美國國家監控的問題[41]。

---

[39] 郭戎晉，論資料在地化之立法，臺灣科技法學叢刊，第 3 期，頁 84-88（2020 年）。
[40] 同上註，頁 89-92。
[41] Anupam Chander, *supra* note 38, at. 778.

（二）實際上資料跨境傳輸在今日社會係無法避免

如前所述，在現今社會中，國際間經貿往來已在世界上幾乎每一處不斷發生，不論是貨品貿易亦或是服務貿易均如是，其中涉及跨越國界的跨境資料傳輸、移轉，事實上係無可避免的必要過程，殊難想像能達到所謂百分之百之資料在地化或是資料鎖國之情形於今日社會中發生，舉例言之，如某些位於歐盟境外的航空業者、旅宿業者對歐盟公民提供服務，即勢必仍須獲取其相關個人資料，是其行業之性質及服務上之必要所使然，若硬要形成資料在地化的規範及使該些資料不得傳輸至境外的服務提供業者，難以期待這樣的服務仍能正常運行[42]。

二、資料在地化本身會造成其他問題

（一）更易遭受網路攻擊

資料若過度集中於特定位置反而更易於被有心人士鎖定，境外網路伺服器或資料中心如採取分散式架構，將相關資料分散儲存在異地，反而具有較高的安全性。

另外，跨國大型雲端運算公司具有較大的能力與資源致力於安全措施之提升，同時於問題發生時原則上亦具有較快的應變速度及防堵災害擴大之能力，但若被資料在地化相關立法所限制，企業可能被迫只得選擇安全性較低、資源力較少的本國服務提供業者[43]。

（二）對於中小企業造成過大的成本

若要達成資料在地化，所要付出之成本對於中小企業來說可能過於昂貴，資料在地化要求在多個司法管轄區經營業務的公司，在每個司法管轄區內皆建置資

[42] See *Id.* at. 781.
[43] 郭戎晉，前揭註 39，頁 113-114。

料基礎設施已進行儲存、處理等，這將是一個昂貴的過程，可以想見許多中小型企業可能無力負擔這樣的額外成本，因而選擇退出歐盟市場[44]。

而當越來越多的國家面臨到上述的情況，該些國家可能也將祭出相關的法令，以限制歐盟或世界對於該國之資料傳輸，形成所謂「資料鎖國化」之現象。很難想像在今日國際經貿往來快速、許多資訊串流服務發達之社會下，若形成各國不再跨境傳輸資料的情況，會對國際社會造成如何巨大的影響，不僅有違國際自由貿易經濟效益最大化的基本原則，也會重大減損全球公民的福祉[45]。

（三）影響國際經貿發展並與 GDPR 前言第 101 點所揭櫫的理念背道而馳

按 GDPR 前言第 101 點指出：「個人資料來自或移轉到歐盟以外國家或國際組織，對於國際貿易和國際合作的擴展是必要的。然而，當個人資料從歐盟移轉至第三國或國際組織的管控者、處理者或其他接收者，本規則所確保的歐盟境內公民之保護水準不應因此降低。無論如何，對於第三國和國際組織的移轉，必須完全遵守本規則的規定，只有在資料管控者或處理者符合本規則有關將個人資料轉移到第三國或國際組織條款的情況下，始得進行轉移。」本條前言重申 GDPR 許多重要概念，如適足性保護水準相當、對於跨境傳輸採原則禁止、例外許可等，更重要的是，本條亦揭櫫 GDPR 之立法目的之一亦是想要在保護歐盟公民資料隱私權之前提下，促進國際貿易之流通。換言之，完全資料在地化的作法亦可能與 GDPR 之立法精神相互違背[46]。

---

[44] Anupam Chander, *supra* note 38, at. 782.
[45] *Id.* at. 783.
[46] GDPR recital 101("Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation.… However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined.... In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.").

（四）可能違反 WTO GATS 相關規定

GDPR 保障關於個人資料的隱私，其中包含前述提及的跨境個人資料傳輸，於國際經貿法領域可能被歸類為提供服務，而有《服務貿易總協定（General Agreement on Trade in Services, GATS）》之適用。有論者認為，GDPR 之規定有違反最惠國待遇（MFN）及國民待遇原則（NT）等不歧視義務，以及可能違反市場准入等相關規定[47]。

蓋歐盟針對不同國家，要求其先取得適足性認定，或透過 SCC、BCR 等方式始得將其資料傳輸至歐盟境內，即有可能違反最惠國待遇及市場准入等規定。而非歐盟成員國之國家除了自身國內個資或隱私法規外，尚須額外負擔歐盟 GDPR 的法令遵循成本，甚至是相關修正，亦可能導致其他國家相較於歐盟成員國處於競爭上之不利地位，因而有違反國民待遇原則之疑慮[48]。

然此部分由於 GATS 之適用範圍、電信附件談判未果等原因，WTO 爭端解決體系未必能對這個美歐跨境傳輸的問題提供適當的解決，就算真的落入 GATS 之範圍，亦被認定有違反上述義務，歐盟也可能主張 GATS 第 14 條之例外抗辯，只要能夠證明其手段及目的之關聯性，並通過必要性標準之檢測，就能夠例外排除最惠國待遇、國民待遇等規定之適用，而 GDPR 所欲保障者，是歐盟基本權利憲章中所明文規定之隱私權，具有受歐盟憲法所保障基本權之崇高地位，只要歐盟相關機關在適用 GDPR 時合乎目的性地適用相關規定，歐盟在受到其他國家質疑 WTO 法律之適法性時，有不小可能得以透過此項例外條款來排除[49]。

綜上所述，目前似僅能認為 GDPR 有違反 GATS「之虞」，然目前尚無此方面之實際案件，實務將如何發展，仍有待 WTO 爭端解決小組或未來重新調整後

[47] 薛景文，從 Schrems I & II 論美歐隱私權保障落差對於自由貿易規範之影響，第 21 屆國立政治大學國際經貿法學學術發展研討會論文集，頁 529-532（2021 年）。
[48] 同上註。
[49] 同上註，頁 532-534。

的上訴機構發表見解。

三、小結

資料在地化於今日社會似並不可行，蓋其既無法真正解決歐盟法院在 Schrems I 及 Schrems II 案中對於美國情報單位監控之擔憂，且亦可能造成資料過度集中存放不利資安防護、造成中小企業過高之基礎設施成本及可能違反 WTO GATS 協定等更多衍生問題，甚至就本質上而言，亦與 GDPR 立法精神背道而馳，並不利於國際經貿流通發展。

第二項 例外合法事由

承上所述，蓋現今國際經貿環境下，難以全面採用「資料在地化」之立法模式，在 GDPR 對於資料跨境傳輸採取「原則禁止，例外允許」之前提下，在全球不同國家／地區之間，仍有尋找跨境傳輸資料合法依據之必要，即只有符合 GDPR 所規定例外事由的情況下，資料才能合法地進行跨境傳輸，以下將分別介紹數種 GDPR 條文中最常見之合法事由。

第一款 適足性認定——以日本為例

在所有之合法事由當中，適足性認定可說是得讓合法效力涵蓋的範圍到最廣、最一勞永逸之方式，按 GDPR 第 45 條規定，若一位於歐盟以外之第三國能夠通過歐盟之適足性認定，則兩國間之資料傳輸就如同在歐盟境內傳輸一般，能夠具備合法性地自由流通，然該第三國對於個資保護之水準（包含個資相關法制、憲法對於基本權之最低要求、刑法、救濟途徑之完善性等）須達到和歐盟幾乎相同

之水準，歐盟才會認為符合給予適足性認定之要求[50]。

然而在各個國家法制不盡相同之背景下，若本身之內國法對於個資隱私之規範先天上即與歐盟之 GDPR 存有相當之落差，或是憲法對於基本權保障所側重之面向有所不同，該如何取得歐盟之適足性認定？判斷是否通過適足性認定的標準為何？對手國是否得與歐盟進行協商，若為肯定，得進行何種程度之協商？均不無疑問。換言之，適足性認定之給予與否似乎係歐盟得決定准駁結果之單方面行為，歐盟在決定是否給予適足性認定之標準上，於 GDPR 條文中僅見上述符合法制保護水準一致性、完整救濟途徑等較原則性之說明，歐盟實際在作成決定之過程中，真正決定性之因素有哪些，均未能從 GDPR 條文中直接得出答案。

個資法制及憲法背景與歐盟有不小差異之日本，於 2019 年正式通過歐盟之適足性認定，也或許為世界各國建立起示範之標準。蓋隱私權及個資保護均為歐盟憲法上所明文規定之基本權，不容協商妥協，在歐盟眼中，此類基本權之保障亦毫無疑問地應優先於商業利益；相對地，日本在憲法中並未明文承認隱私權及個資保護為基本權，僅有部分實務案例間接承認。另外日本主要之個資法規——日本個人資料保護法[51]（Japan Act on the Protection of Personal Information, APPI）更直接定調個資具有商業價值，適當地進行利用可以增進全體經濟福祉，較肯定個資所帶來之經濟商業效應，對於隱私、個資保障的範圍較為限縮[52]。

而日本面對雙方個資法制上之差異，修法之方式主要係以在 APPI 之基礎上另外新增獨立附件的方式完成，其重點主要有以下兩點：（1）將性傾向等資訊及勞工是否加入工會等個資分別挑選出來，並將之歸類為敏感性個資；（2）特別針

[50] GDPR art. 45.
[51] Kojin joho no hogo nikansuru horitsu [Amended Act on the Protection of Personal Information], Law No. 57 of 2003, translated in PERS. INFO. PROTECTION AMENDED ACT ON THE PROTECTION OF PERSONAL INFORMATION (TENTATIVE TRANSLATION), VER. 2 (2016) [hereinafter Amended APPI].
[52] Flora Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 HARV. J. L. & TECH. 661, 668-670 (2020).

對來自歐盟的個資依據歐盟之標準處理，即使超出日本法本身對於個資的保護密度（即特別針對歐盟傳輸之跨境個資分流處理）[53]。

歐盟原先對於日本個資法制的擔憂有二：首先為日本採用大量的指引（guidelines）作為法源依據，由於在歐盟法制下指引（guidelines）是非拘束性（non-binding）的，故以「指引」作為法源依據之作法曾受到歐盟之質疑；然而在日本的社會風氣下，不遵守指引會被企業或人民認為是不誠信的行為，法院判決也多會採用指引中所揭示的準則，所以指引在實際的效果上其實已經非常接近法律（law）或規則（regulation）。這給了日本政府在政策工具上有更多的彈性，在某些難以在短時間通過立法的政策，首相透過頒布指引的方式實質上也能夠達到類似於立法之效果。而透過協商溝通上述特殊之實務作法，日本成功說服歐盟接受此種法制文化上的差異[54]。

另一方面為，日本的個資主管機關 PPC 和日本企業間的關係較偏向合作、互動式的關係；和歐盟 EDPB 較偏向以強力的裁罰手段規制歐盟企業的方式有所不同。有論者即質疑日本此種軟法（soft law）性質的手段可能並不足以符合歐盟之標準，惟亦有論者指出，考量到日本特殊的社會文化及監管機關軟硬導向之差異，以軟法手段規制已足以實質上達到近似於歐盟對於個資的保護水準。其後歐盟執委會及 EDPB 在觀察日本法院的相關判決，及考量整體日本社會風氣後所形成的法之整體觀察，認為日本這樣的立法模式係足以達到與歐盟相一致之保護水準[55]。

值得注意的是，從歐盟傳輸至日本之資料適用前述調整過的較高標準；而從日本傳輸至歐盟之資料，由於並未落入 GDPR 的管制範圍當中，則仍維持日本原先之低密度保護水準，故日本與歐盟間之跨境資料傳輸形成一雙軌制的規範模式，

[53] *Id*. at. 670-674.
[54] *Id*. at. 674-676.
[55] *Id*. at. 676-678.

蓋係日本政府考量到國內文化與歐盟間之差異，在能夠通過歐盟適足性認定之前提下，選擇以改動面向最少之方式為之，期在經濟發展及人民接受程度當中取得一適度平衡[56]。

總結來說，透過日本取得歐盟適足性認定之過程，為其他欲申請適足性認定之國家首開先例，提供若干足供參考之資訊，吾人至少可以獲得以下幾點啟發：（1）歐盟對於決定是否給予適足性認定，並非要求必須完全修法至與 GDPR 完全相同，就算使用之立法模式與歐盟大相徑庭，在考量到整體社會文化規制力量及其他綜合考量下，亦可能達成與歐盟「本質上」相同之保護水準；（2）各國仍得在保有自身特色及需求之情況下，滿足歐盟在意之保護面向，以更動最小化之方式進行修法以完成適足性認定，甚至可以透過如日本的雙軌制模式，兼顧自身國內民情文化與國際貿易經濟發展；（3）就算並非如同美國透過雙邊協商之方式完成資料傳輸協定（詳後述），而係透過一般申請適足性認定之方式為之，可以在日本的例子中看到，雙方政府仍有許多協商互動、說服彼此瞭解雙方差異之空間，不論是法制上、文化上等均如是，並非謂透過一般申請適足性認定之程序，即完全任由歐盟單方面准駁。惟實際談判協商之過程，可以想見仍會因申請國之國力及經貿地位而有所差異，自不待言。

第二款 雙邊協商

在取得適足性認定的名單中，尚有以「雙邊協商」方式取得適足性認定者，在此一方式中，申請國較似立於平等之地位與歐盟進行協商談判，雙方皆得在某些保護之面向或密度上互相讓步，而非如一般情形取得適足性認定時歐盟立於絕對優勢之地位。而目前能與歐盟透過雙邊協商方式完成資料跨境傳輸協議（歐盟適足性認定）的國家僅有美國[57]。

---

[56] *Id*. at. 676-678.

[57] European Commission, *Adequacy decisions*, https://commission.europa.eu/law/law-topic/data-

在歐盟較重視隱私保護、美國較重視保障自由的背景下，美歐雙方在 20 世紀末期選擇透過 Directive 95 第 25 條第 4 項及第 5 項規定，以「雙邊協商」之方式，完成適足性之認定[58]，即《安全港協議（Safe Harbor Framework）[59]》及其後之《隱私盾協議（EU-US Private Shield）[60]》，然而在分別經過 Maximillian Schrems v. Data Protection Commissioner（以下簡稱 Schrems I 案[61]）及 Data Protection Commissioner v. Facebook Ireland Ltd （以下簡稱 Schrems II 案[62]）後，前述之安全港協議及隱私盾協議相繼被歐盟法院（Court of Justice of the European Union, CJEU）以與 GDPR 保護之程度不相符為由宣告失效後，美歐間資料跨境傳輸的合法基礎究竟為何，即陷入一混沌不明的狀態。

一、Schrems I 案

首版資料傳輸協定《安全港協議》於 2000 年獲歐盟執委會通過，不料在順利運行十餘年後，一位奧地利公民 Schrems 認為 Facebook 在註冊時要求用戶揭露過多之個人資料，將位於歐盟之公民的資料，以安全港協議作為基礎，傳輸至美國之 Facebook 總部。Schrems 認為美歐安全港協議之內容，可能有違反 Directive 95 對個資保障程度之虞，遂於愛爾蘭法院對 Facebook 提起訴訟。

愛爾蘭高等法院為求慎重，選擇中止訴訟並將案件提交至歐盟法院，歐盟法院判決的重點摘要如下：

（一）釐清「適足性保護水準」

按透過雙邊協商之方式達成協議，實際上仍須對手國對於個資保護之密度及水準達到與歐盟保護密度相一致之水準，僅係於實際談判之過程，可能考量雙方

protection/international-dimension-data-protection/adequacy-decisions_en#high-level-meeting-on-international-data-flows (last visited Jan. 18, 2024).

58 Directive 95 arts. 25(4)(5).

59 Safe Harbor, *supra* note 3.

60 Privacy Shield, *supra* note 4.

61 Schrems I, *supra* note 1.

62 Schrems II, *supra* note 2.

對於隱私權及其他憲法上基本權，所著重保護之面向不同，故得於某些部分進行調整，或搭配相關之配套措施，而非謂兩國個資保護水準差異極大的國家，得以藉由雙邊協商之方式，完全架空原應進行適足性認定之程序與其基本精神。

故所謂適足性保護水準，應為資料接收國根據其內國法，立法方式或作法與 Directive 95 或許有所不同，惟可確保其針對基本權及自由的保護水準，實質上之保護程度與歐盟並無二致而言[63]。

（二）安全港協議於 Directive 95 下之合法性

安全港協議之相關原則僅適用於美國私部門（即公司等），即若為美國公部門對歐洲人民進行隱私干預或做出違反規定之行為者，並不包含在此規範內，此一部分對於受侵害之歐盟公民而言，亦欠缺適當之救濟管道及程序[64]。再者，歐盟法院指出歐盟執委會於 2000 年通過安全港協議時，實際上並未實質審查美國國內個資立法及安全港協議隱私原則之內容，即認其已達到 Directive95 第 25 條第 6 項所要求的適足性保護水準，尚嫌速斷[65]。

（三）對美國國家監控行為的擔憂

此外，判決中亦指出，美國常會基於自身國家安全考量為由，對歐盟境內公民蒐集個人資料，美國雖以國家安全及公共利益等原因作為例外合法事由，然實際上是否違反 Directive95 之保護精神，不無疑問。且該些行為甚至可能涉及違反歐盟基本權利憲章（Charter of Fundamental Rights of the European Union）之層級[66]，如第 7 條規定所保障之隱私權、第 8 條個資保護權利、第 47 條所規定之訴訟權等基本權[67]。

---

[63] Schrems I para. 73.
[64] *Id.* paras. 82, 89.
[65] *Id.* paras. 96-98.
[66] *Id.,* paras. 86-88, 94-95.
[67] Charter of Fundamental Rights of the European Union arts. 7, 8, 47 (“7. Everyone has the right to

綜上所述，歐盟法院認為安全港協議有違反 Directive95 及歐盟基本權利憲章相關規定之虞，且不符合歐盟對於個資保障之水準，故判決安全港協議失效。

二、Schrems II 案

於安全港協議被歐盟法院宣告失效後，美歐雙方政府即迅速著手討論新版之資料傳輸架構，並於 Schrems I 案判決作成不到一年後，歐盟執委會即於 2016 年通過《隱私盾協議》，即美歐間第二版之資料跨境傳輸協議。

另一方面，Schrems 於安全港協議失效後，亦再針對 Facebook 改採用 SCC 進行跨境資料傳輸的權宜之計提起訴訟，愛爾蘭法院受理後亦中止訴訟並將之提交至歐盟法院，並一併詢問 2016 年甫完成之隱私盾協議是否符合歐盟資料保護的要求，當中隨著時間遞嬗，經過 2018 年 GDPR 正式施行，故 Schrems II 判決之法律基礎亦轉變為以 GDPR 作為基準。

（一）隱私盾協議無效

隱私盾協議相較於前版之安全港協議，主要改善之處係在雙邊之合作執行機制等程序面向，對於實質保障內容之修改實則有限，針對歐盟法院最擔憂之美國國家監控行為之問題，隱私盾協議新增一行政監察專員機制（Ombudsperson Mechanism），回應 schrems I 案中，歐盟法院認為安全港協議違反歐盟基本權利憲章第 47 條訴訟權保障要求之部分。

惟歐盟法院於 schrems II 案中指出，歐盟基本權利憲章第 47 條所欲保障之

---

respect for his or her private and family life, home and communications.; 8. (1) Everyone has the right to the protection of personal data concerning him or her.; 47. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.”); 郭戎晉，論個人資料跨境傳輸與數位經貿之互動與規範設計─以歐盟法院 Schrems 案影響為觀察對象，收於：王震宇編，2021 數位貿易政策論壇－科技．人文．數位貿易，頁 224-226（2021 年）。

程度係為使資料主體應具有明確、公正進行司法救濟之程序，隱私盾協議之行政監察專員機制與司法救濟仍屬有別，無法滿足第 47 條所保障之歐盟公民基本權[68]。綜合來說，美國情報單位對歐盟公民進行個人資料蒐集之行為已逾越合法目的關聯所必要之程度，違反比例原則，使得美歐對於個人資料保護之密度及程序上皆未符合「本質上相同」之最低限度要求，隱私盾協議仍有違反歐盟基本權利憲章多項規定之虞，最終歐盟法院再次判決美歐間隱私盾協議失效[69]。

（二）肯認 SCC 為一有效之機制

而針對 SCC 方面，歐盟法院認為，在評估採取 SCC 方案是否符合 GDPR 及歐盟基本權利憲章時，除了檢視所提供之保護水準是否滿足與歐盟個資保護「本質上相同」之要求外，亦須考量當跨境傳輸行為有違反 SCC 情形時，資料主體是否得有適切之管道進行法律救濟，並應設計有責機關具有權力暫停或禁止資料傳輸，於此部分，歐盟法院認為 SCC 尚符合上述要求[70]。

至於 SCC 本身的有效性部分，SCC 的重要特色之一為其本質上仍屬契約，只能拘束締約雙方，本判決雖肯認 SCC 之合法性，惟 SCC 僅拘束私人公司，無法解決第三國國家政府監控之問題，故仍需有其他之額外措施進行搭配，以填補 SCC 效力範圍之不足。然而，這些額外措施的內涵和形式為何，本判決並未清楚指明，有待後續釐清[71]。

三、後 Schrems II 時期

（一）SCC 似為目前最具合法性之方式

在安全港協議及隱私盾協議等雙邊適足性協商相繼被歐盟法院宣告失效，且

---

[68] Schrems II para. 191.
[69] Schrems II para. 201.
[70] Schrems II paras. 128-130.
[71] *See* 董芃旻，台灣跨境資料傳輸——聚焦以契約方式作為隱私保障工具，國立政治大學法律學系碩士學位論文，頁 35-38（2022 年）。

Schrems II 案又暫時肯定 SCC 之合法性後，SCC 應係短期內美歐資料跨境傳輸最具合法性希望之方式。

又 Schrems II 案判決後不久，EDPB 隨即於 2020 年 11 月針對所謂「額外補充措施」發布相關建議[72]，而其後歐盟執委會亦參酌 Schrems II 案之判決內容及此份 EDPB 建議，於 2021 年 6 月通過新版 SCC[73]，作為各企業訂立之參考標準。本文後續將進一步討論此一新版 SCC 之內容、其是否能夠解決歐盟法院所擔憂之問題，以及後續若面對相關社會團體再次提起訴訟，是否能通過歐盟法院之審查，在歐盟基本權利憲章對基本權之保護及 GDPR 方面均通過合法性檢驗，成為跨境資料傳輸長久穩定、有效之解決方案。

（二）美歐第三版資料傳輸協定

另一方面，美國政府及歐盟執委會仍不放棄以雙邊協商之方式繼續進行第三版美歐雙邊資料傳輸協定之可能性，畢竟如前所述，SCC 僅為企業所採用個案性質之契約條款，真正一勞永逸之方式，仍為美國與歐盟簽訂資料傳輸協定並得以通過歐盟法院之檢驗，使雙方企業均得放心地進行資料跨境傳輸。歷時近三年之討論協商，歐盟執委會於 2023 年 7 月正式通過《歐美資料隱私架構協定（EU–US Data Privacy Framework, DPF）[74]》，即美歐間第三版之雙邊資料傳輸協定。

而美國本次針對歐盟法院所擔憂之美國情報機關監控問題，主要係以拜登政府於 2022 年 10 月通過之行政命令 EO 14086，取代舊有之歐巴馬政府行政命令

[72] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[73] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31 [hereinafter 2021 SCC].

[74] Commission Implementing Decision (EU) of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118 [hereinafter DPF].

PPD-28，作為回應之法源依據[75]，而雖然新的 EO 14086 有針對許多隱私原則作出重申及微幅調整，但從中不難看出美國做出的實質讓步實則有限。有論者提出以下兩大缺失：（1）新的 EO 14086 仍未針對哪些行為會落入本命令所規範之「情報活動」做出明確定義；（2）再者，新的 EO 14086 並無法修改美國 FISA 法之內容，特別是一直為人詬病之 702 條款[76]。

而在救濟制度方面，EO 14086 創設一新的雙層救濟機制：第一層級由國家情報總監辦公室的公民自由保護官（Civil Liberties Protection Officer, CLPO）就申訴之具體案件作行政調查；第二層級則由此行政命令授權設立之新「資料保護審查法院（Data Protection Review Court）」，對前述公民自由保護官作成之行政決定進行如第二審般、具有拘束力之複審。而資料保護審查法院的法官不得為美國政府公務員或同時擔任政府職位，並需具備資料隱私法律方面之專長，其獨立審判之職權如同一般法院，不受其他行政或立法之干預[77]。

雖然美歐政府間迅速達成共識，順利通過第三版跨境資料傳輸協定 DPF，並於 DPF 進行若干隱私原則之重申及文字上之微幅調整，亦針對 Schrems II 案中歐盟法院認為違反歐盟基本權利憲章第 47 條訴訟權之部分，以新設計的雙層救濟機制（包含新設資料保護審查法院）作為回應，惟此一協定相較於前版之隱私盾協定，改變之幅度及內容是否已達到歐盟法院所要求之標準，不無疑義。Max Schrems 及其所屬之公民團體已表態將對 DPF 繼續向歐盟法院提起訴訟，其等認為 DPF 僅係微幅作文字上詞藻之修飾、甚或進行若干換湯不換藥之改動，無異是隱私盾協議之翻版，一樣無法滿足歐盟基本權利憲章之保障密度[78]。後續訴訟

[75] Executive Order (EO) 14086 of 7 October 2022, on Enhancing Safeguards for United States Signals Intelligence Activities [hereinafter EO 14086]; Presidential Policy Directive 28 – Signals Intelligence Activities, 17 January 2004 [hereinafter PPD-28].
[76] 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871; Sergi Batlle and Arnaud van Waeyenberge, *EU–US Data Privacy Framework: A First Legal Assessment*, EUROPEAN JOURNAL OF RISK REGULATION 1, 4-6 (2023).
[77] EO 14086 sec. 3(E).
[78] NOYB, *European Commission Gives EU-US Data Transfers Third Round at CJEU* (July 10, 2023) https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

之發展及歐盟法院之看法如何，甚值持續關注。

第三款 拘束性企業規則（BCR）

若無法取得一般性之適足性認定或透過雙邊協商的方式完成資料傳輸協定，GDPR 另有設計其他方法，達成個案性取得例外性合法事由之依據，如：拘束性企業規則（Binding Corporate Rules, BCR）、行為準則（Code Of Conducts, CoC）、標準契約條款（Standard Contractual Clauses, SCC）[79]。其中最為重要、目前也最被廣泛使用者為 SCC，其合法性在 Schrems II 案中受到歐盟法院側面肯定，已如前述。SCC 之部分，詳細介紹留待後述第五款作說明。

BCR 主要係用於跨國企業集團旗下各母子公司間傳輸個人資料所用，蓋某些跨國企業之母公司或部分子公司可能係位於未取得適足性認定之國家／地區，此時企業集團間若欲進行客戶等資料主體之個人資料流通，可能即有適法性之疑慮，BCR 制度之設計即係為解決此一問題，使企業集團得以透過制定 BCR 並得到監管機關批准之方式，取得例外合法事由。惟須注意的是，BCR 之制定仍須符合 GDPR 所揭櫫的各項基本原則，並賦予受影響之資料主體適當的申訴及進行救濟之管道[80]。

第四款 行為準則（CoC）

CoC 則較近似於各行業別之公會自行提出其如何落實 GDPR 要求之一套自發性標準，通常係適用在特定行業別，如科技業或具特定技術之行業，為了其業務範圍可能涉及個資保護之適法性疑慮，於公會討論、制定出一套該行業皆能接受並得以遵守的同業標準。

---

79 GDPR art. 46(2).
80 GDPR arts. 46(2)(b), 47(2).

和 BCR 相似，CoC 必須經過監管機關之批准後，始得成為具有效力之跨境資料傳輸例外合法事由[81]。又 CoC 雖得依其行業別之特性，在資料處理之公平性要求、透明性要求，甚或是資料主體之救濟方式做出符合該行業特色且符合經濟之規範模式，惟其中所有之內容亦須符合 GDPR 之各項基本原則，自屬當然[82]。附有說明者為，和 BCR 以及 SCC 不同的是，CoC 本身規範之法條座落於 GDPR 第 40 條，亦即第四章「管控者及處理者之義務」，蓋行為準則並非專為解決資料跨境傳輸合法依據之用而設，此為 GDPR 法條編排上略為特殊之處。

故在實際使用上，管控者或處理者可依據已通過監管機關核准之 CoC，作為其跨境傳輸個人資料之準則，如此即便欲傳輸至其他尚未取得歐盟適足性認定之地區時，也因為符合例外事由而具備合法性。

第五款 標準契約條款（SCC）

SCC 係廣泛地得被使用在任何資料管控者／處理者之間，透過將歐盟執委會已發布之 SCC 條款，納入資料管控者／處理者間之契約中，並藉由利益第三人條款，使資料主體成為受益第三人之方式[83]，透過契約之方式使分別位於歐盟境內及境外之資料管控者／處理者對於個資保護之水準達到一致，如此一來，即使兩國間並未透過雙邊協商簽訂資料傳輸協定，或取得歐盟適足性認定，個別企業仍可藉由使用 SCC 的方式，取得將資料主體之個資進行跨境傳輸之合法依據[84]。

惟企業若欲在 SCC 條款納入與資料主體間之契約時對條款的內容進行調整，僅得以新增獨立附件之方式為之，而不得逕行修改歐盟執委會已頒布之 SCC，新增獨立附件之內容亦不得與 SCC 條款及 GDPR（舊時期則為 Directive 95）之基

[81] GDPR art. 46(2)(e).
[82] GDPR art. 40.
[83] 2021 SCC arts. 3,10-12.
[84] GDPR art. 46(2)(c).

本原則相衝突[85]。

歷史上目前僅有頒布過四份 SCC，分別是三份在 Directive 95 時代即已作成之 SCCs（以下簡稱舊版 SCC）[86]，以及本文所欲著重探討之 2021 年新版 SCC（詳第三章述）[87]。在舊版 SCC 中，前兩份針對「歐盟境內之資料管控者」將資料傳輸至「歐盟境外之資料管控者」作規範，第三份則係針對「歐盟境內之資料管控者」將資料傳輸至「歐盟境外之資料處理者」作規範。

累積前三份之 SCC 條款雖已有針對不同之面向作設計，然而由於歐盟個資法制進入到 GDPR 時代後，GDPR 之適用範圍不僅較 Directive 95 而言來得更廣，規範之若干原則及其範圍、密度均有顯著提昇。再者，資料傳輸科技之進步日新月異，已出現諸多 Directive 95 時代所未能設想到之傳輸情境，導致舊版之 SCC 已逐漸無法滿足現今之需求。又因 Schrems II 案中對於 SCC 合法性之側面肯定，使得 SCC 成為後 Schrems II 時期中，一前景較為明亮之跨境傳輸合法工具，故歐盟執委會亦一併將 Schrems II 案之判決內容納入考量，於 2021 年 6 月正式頒布新版 SCC，2021 新版 SCC 則一改以往之立法方式，以模組化（Module）之方式分別對應規範四種不同之傳輸情境。

而新版 SCC 賦予已依舊版 SCC 為架構所簽訂之契約 18 個月之緩衝期，於 2022 年底開始，舊版 SCC 全面失效。換言之，若係依據舊版 SCC 所簽訂之資料跨境傳輸契約，其合法性自此失所附麗，故可以想見有許多已作成／使用中之跨

---

[85] European Commission, *New Standard Contractual Clauses - Questions and Answers Overview*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (last visited Jan. 24, 2024).

[86] 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, 2001 O.J. (L 181) 19 [hereinafter 2001 SCC]; 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 transfer of personal data to third countries, 2004 O.J. (L 385) 74 [hereinafter 2004 SCC]; 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, 2010 O.J. (L 39) 5 [hereinafter 2010 SCC].

[87] 2021 SCC, *supra* note 73.

境資料傳輸契約有重新簽訂、調整之必要[88]。

第六款 同意（Consent）

而取得資料主體之同意(Consent)係作為最後一種資料管控者／處理者取得合法依據之手段。取得同意和其他方式最為不同的地方在於，資料管控者／處理者並未取得上述適足性認定、SCC 等任何一種資料跨境傳輸之例外合法事由，惟既然資料主體自願在其基本權利上做出讓步（通常為事前同意），則即使資料管控者／處理者並未取得上述任一例外合法事由，立法者仍賦予管控者／處理者得將資料主體之資料進行跨境傳輸之權[89]。

而同意之內涵及範圍究何所指，不無疑問，資料主體對於同意之後果所瞭解的程度、其同意的範圍是否應有界線、取得同意的方式等問題，在學理上多有爭論，本文由於主題及篇幅之限制，於此部分僅就 GDPR 本文及前言之內容，輔以部分論者之意見作成歸納。

GDPR 對於同意之內涵為何，分別於前言第 32 點、第 42 點、第 43 點、本文第 7 條有所規範，而就其規範內容，可整理出以下幾種「同意」所包含之面向[90]：

---

[88] 2021 SCC recital 24 (“Decision 2001/497/EC and Decision 2010/87/EU should be repealed three months after the entry into force of this Decision. During that period, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, still be able to use the standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU. For an additional period of 15 months, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, be able to continue to rely on standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU for the performance of contracts concluded between them before the date of repeal of those decisions, provided that the processing operations that are the subject matter of the contract remain unchanged and that reliance on the clauses ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679. In the event of relevant changes to the contract, the data exporter should be required to rely on a new ground for data transfers under the contract, in particular by replacing the existing standard contractual clauses with the standard contractual clauses set out in the Annex to this Decision. The same should apply to any sub-contracting to a (sub-)processor of processing operations covered by the contract.”).

[89] GDPR art. 49(1)(a).

[90] GDPR recitals 32, 42, 43; art. 7 (“(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the

（1）基於資料主體的自由意志下明確給予

資料主體必須是在清楚了解到其給予同意將會造成何種後果，亦即對於其權利將會造成何種影響有清楚的認知，且同意之給予並非出於受強迫或另負有負擔之方式。

作成同意之方式必須具體明確，方式包含書面同意、電子簽章或口頭承諾，惟資料主體單純沈默或默示同意，則並不能得出資料主體已對此表達同意之結論。另外，若管控者對於同意的取得係與其他權利告知事項一併進行，則須能夠確保資料主體有針對同意之部分明確表達接受的意思，包裹式的一鍵式同意或將同意的選項直接預設為勾選的方式無法符合 GDPR 之要求。

（2）同意之撤銷必須如給予時同等容易

資料主體為同意後非不得撤銷之。換言之，資料主體得於作成同意後，隨時向資料管控者撤銷同意，惟撤銷同意之效力不溯及既往，自不待言。GDPR 前言

processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided; (42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment; (43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.).

與本文皆揭示同意之撤銷方式必須如同給予時同等容易且不會遭受不利益，若否，或是資料主體於作成同意前並無從得知撤銷亦一樣容易，則應推定其所為之同意並不具備自主性要件。

（3）對於同意之取得管控者須負擔舉證責任

在一般民事或行政訴訟上，當法院窮盡所有證據調查方法及綜合全辯論意旨後，仍對部分陷入真偽不明之事實無法作成判斷時，多會依據程序法或實體法對於舉證責任之分配，判決須負擔舉證責任之一方承擔不利判決之結果。而在 GDPR 中，若對於同意之取得與否陷入爭議不明時，GDPR 第 7 條第 1 項明確規定，對於同意之取得與否，舉證責任之分配上，係由資料管控者就已取得資料主體完整、無上述瑕疵之同意負擔舉證責任[91]。

第三項 SCC 作為例外合法事由之定位與功能

雖同為資料跨境傳輸之例外合法事由工具，SCC、BCR 及 CoC 有著定位及功能上之若干差異。首先，蓋 SCC 係由歐盟執委會所發布，故其不若 BCR 及 CoC 係由企業或行業公會自行提出，須再經歐盟執委會核准通過，SCC 經過締約雙方合意簽署後即可直接施行（包含雙方在不違反 SCC 本身及 GDPR 之前提下以新增附件之方式進行修改），成為資料跨境傳輸之合法性基礎[92]。

再者，SCC 與前述 BCR 及 CoC 最大的不同之處在於，BCR 適合用於母子公司遍佈歐盟／非歐盟地區之企業集團、CoC 較近似於特定類別行業公會所提出之標準守則，而 SCC 之適用上則不受到特定行業別之限制，不論任何產業之

[91] Stephen Breen et al., *GDPR: Is your consent valid*, 37(1) BUSINESS INFORMATION REVIEW 19, 21-23 (2020).
[92] Nicole Beranek, *SCCs and CoCs and BCR – Untangling the Web and Spotting the Difference*, INPLP (Nov. 26, 2021), https://inplp.com/latest-news/article/sccs-and-cocs-and-bcr-untangling-the-web-and-spotting-the-difference/.

兩個資料管控者／處理者，皆得藉由簽訂 SCC，獲得資料跨境傳輸之例外合法基礎[93]。

SCC 之一般性通用特質，亦使其被普遍認為能夠提供未能取得歐盟適足性認定之國家，仍得與歐盟進行資料跨境傳輸之合法工具。如在目前歐美間欠缺適足性認定或確定有效之雙邊資料傳輸協定的狀態下，SCC 可望成為歐美間主要之跨境資料傳輸合法工具，EDPB 亦於 Schrems II 案判決後隔年即推出新版本之 SCC 條款，並於條文中明訂新版 SCC 相較於舊版 SCC 及以舊版 SCC 為基礎所簽訂之資料傳輸契約，具有優先效力[94]。本文第三章及第四章將接續進行新版 SCC 之合法性分析，礙於目前歐盟法院尚未有專門針對 SCC 於 GDPR 下之適法性疑義的案件，故本篇論文參照過往歐盟法院在面對其他跨境資料傳輸合法工具（即 Schrems I、II 案針對雙邊資料傳輸協定）於 GDPR 下適法性疑慮之案件，歐盟法院係將雙邊資料傳輸協定之內容與 GDPR 進行分析比對的作法，亦將於後述章節先進行 2021 新版 SCC 與 GDPR 之重點規範比較，並進一步進行新版 SCC 與 GDPR 之合致性分析。

[93] *Id.*
[94] 2021 SCC Annex §5.

第三章 新版 SCC 與 GDPR 之規範比較

第一節 新版 SCC 規範簡介

第一項 各版本 SCC 歷史沿革

如前所述，舊版三個版本的 SCC 係分別於 2000-2010 年間制訂，歷經十年有餘，科技環境、網路雲端技術之迅速發展；GDPR 的制訂施行；Schrems II 案判決等因素，皆推使 SCC 須進行一次大幅度之更新。

一、2001 年版 SCC 與 2004 年版 SCC

舊版 SCC 僅針對兩種不同的傳輸面向作成規範，前兩份係針對「歐盟境內之資料管控者」將資料傳輸至「歐盟境外之資料管控者」者，2001 年版 SCC 中即確立簽訂 SCC 之契約主體為分別位於境內及境外之資料管控者，並透過使資料主體成為「受益第三人」之方式，達成對資料主體隱私權、個資保護權利之保障[95]。並明訂資料輸出方（此處為位於歐盟境內之資料管控者）具有以下義務：（1）若欲將特定類型的個資傳輸至在此方面未能提供適當保護之第三國，須在傳輸前通知資料主體。（2）使資料主體要求 SCC 契約之副本時易於取得。（3）當資料主體或監管機關對於資料輸入方處理資料有所疑問時，資料輸出方亦須能夠在合理的時間內給予回應[96]；資料輸入方（此處為位於歐盟境外之資料管控者）具有以下義務：（1）當資料主體或監管機關對於資料處理有所疑問時，作適當地處理，並積極配合監管機關之要求。（2）依照資料輸出方之要求提供資料處理之設備作為資料輸出方或監管機關稽核審查之用。（3）使資料主體要求 SCC 契約

[95] 2001 SCC Annex §3.
[96] *Id*. Annex §4.

之副本時易於取得，並於其上標明主責救濟程序之機關[97]。另外，附件第 2 條規定締約雙方須將締約雙方之資訊、傳輸目的、可能受影響之資料主體、被傳輸之資料類型等資訊於 Appendix 1 載明[98]。

關於責任歸屬方面，附件第 6 條規定，若資料主體得依利益第三人條款主張其權利因資料輸出方或資料輸入方因違反此 SCC 條款，而有受損害，除非資料輸出方及資料輸入方均能證明其對於 SCC 條款之違反係不可歸責，否則資料輸出方及資料輸入方須共同負擔對資料主體權利受有損害之賠償，意即對資料主體負擔連帶責任[99]。爭端解決及救濟程序則於附件第 7 條有簡要之規範，即當資料主體對於輸出方或輸入方的回應或處理不滿意時，資料主體得（1）透過公正獨立之第三人或監管機關進行調解；（2）在資料輸出方之所在地法院提起訴訟（此處即為歐盟法院）；（3）若資料主體係針對資料接收者，且資料接收者所在國亦為紐約公約簽約國，則亦可透過仲裁之方式解決紛爭[100]。

2004 年版 SCC 亦係針對「歐盟境內之資料管控者」將資料傳輸至「歐盟境外之資料管控者」之情境作規範，其基本上係以 2001 年版 SCC 為基礎，於各部分再做條文上更細緻之規範，惟其基本精神及規範方向上並無重大不同，可將此版 SCC 視為 2001 年版之「2.0 版本」。改變幅度較大的地方有以下兩處，其一為不再依 2001 SCC Annex 第 5 條分別搭配 Appendix 2 及 Appendix 3，依情況適用兩套不同之個資處理原則，而係統一成 Annex A 一種（即 2001 SCC 中 Appendix 2 之保護強度）[101]；另一為在 Annex 第 7 條明訂雖締約雙方均不得修改 SCC 條款，惟得在不違反其精神及 Directive 95 之原則下，新增其他商業條款（commercial clause）進雙方之契約當中[102]。特別的是，2004 SCC 並未廢止 2001 SCC，而係透

[97] *Id*. Annex §5.
[98] *Id*. Annex §2.
[99] *Id*. Annex §6.
[100] *Id*. Annex §7.
[101] 2004 SCC Annex §2, Annex A.
[102] *Id*. Annex §7.

過修改「decision」條文之方式，將 2001 SCC 稱作「set 1」、2004 SCC 稱作「set 2」，供欲使用之管控者自行選擇要使用哪一版本之 SCC[103]。

二、2010 年版 SCC

而舊版之第三份 SCC 則於 2010 年施行，與前兩份不同，其係針對「歐盟境內之資料管控者」將資料傳輸至「歐盟境外之資料處理者」。其規範體例及若干原則均與前兩份相似，資料輸出方（此處為境內資料管控者）之義務在此份 SCC 中略有微幅調整，惟基本之大方向不變[104]。此份 SCC 特別之處在於明定資料輸入方（此處為境外資料處理者）之義務如下：（1）在遵守 Directive 95 及此 SCC 之原則下處理個資，若發生無法遵守之情形，須於適當時間迅速通知受影響之資料主體，此時資料主體可與資料輸出方協調，資料輸出方有權停止資料傳輸或終止契約；（2）須於 Appendix 2 列明其所採取之資料處理之技術性／組織性措施以確保資料處理之安全性；（3）在其國內執法機關依據國內法要求其揭露資料主體資訊、發生任何未經授權之資料存取，或在接收到資料主體直接要求時，在回應前，須通知資料輸出方；（4）而其他配合資料輸出方及監管機構的要求、提供資料處理之設備以供稽核審計之用、取得 SCC 條款及複委託處理契約條款副本（若有商業機密資訊，則得刪除該商業資訊或作成總結版本後提交之）等義務則與前兩版之原則大同小異[105]。

第 6 條係針對責任之分配作規範，綜觀之可發現，資料輸出方須對資料主體負擔絕對之責任，而在無法對資料輸出方請求之情形，始得對資料輸入方進行請求；又祇在無法對資料輸出方及資料輸入方進行請求之情形，始得始得對資料複委託處理者進行請求，惟資料複委託處理者須負擔之義務以其在條款下進行處理

[103] 2004 SCC arts. 1(1), 1(4).
[104] 2010 SCC Annex §4.
[105] *Id*. Annex §§5(a)-(g).

行為之範圍為限[106]

另外由於處理行為是否包含「複委託處理」，其效果及資料複委託處理者之義務如何，不無疑問，2010 SCC 主要係將此規範在第 11 條，而於其他若干條文中對此亦設有規範，主要係複委託處理須得資料輸出方之「事前書面同意」始得為之、資料複委託處理者進行處理行為時係立於近似資料輸入方之地位，其所遵守之規範等均與資料輸入方相同，另外資料輸入方須確保資料複委託處理者進行處理行為時亦須在遵守此 SCC 條款的原則下為之[107]。

第二項 2021 新版 SCC 條文內容概覽

如前所述，在 Schrems II 案判決美歐隱私盾協議失效，並側面肯定 SCC 作為資料跨境傳輸選項之合法性後，歐盟執委會於 2021 年 6 月正式通過新版之 SCC 條款[108]，此版 SCC 條款一改過去散落於三份 SCC 條款之規範情境，以模組（Module）之方式針對不同之傳輸情境，在同一份 SCC 中分別作成規範，即整合舊有之「位於歐盟境內之資料管控者傳輸至位於歐盟境外之資料管控者」、「位於歐盟境內之資料管控者傳輸至位於歐盟境外之資料處理者」，並新增「位於歐盟境內之資料處理者傳輸至位於歐盟境外之資料處理者」、「位於歐盟境內之資料處理者傳輸至位於歐盟境外之資料管控者」兩種以往所未規範到的傳輸樣態，換言之，即形成「位於歐盟境內之資料管控傳輸至位於歐盟境外之資料管控者」、「位於歐盟境內之資料管控者傳輸至位於歐盟境外之資料處理者」、「位於歐盟境內之資料處理者傳輸至位於歐盟境外之資料處理者」、「位於歐盟境內之資料處理者傳輸至位於歐盟境外之資料管控者」等四種模組之新規範模式[109]，並延續一貫採用以利益第三人條款使資料主體成為契約之受益第三人模式，使受影響的資料

106 2010 SCC Annex §6.
107 *Id*. Annex §5(h)-(j), §11.
108 2021 SCC, *supra* note 73.
109 2021 SCC Annex §§8-18.

主體雖非契約之締約方，亦得根據此契約主張其權利[110]。

而於新版 SCC 條款之規範架構上，可大致分為兩大部分，第一部分為不論四種模組之哪一種均相同適用之基礎條款[111]；第二部分始針對各項細節進行四種模組之模組化條款設計[112]，透過以下圖表概覽新版 SCC 各條款規範重點：

Annex	
Section 1 (一般原則)	
§1	目的與範圍
§2	不得直接修改 SCC 條款本身，但在不違反 SCC 條款及對資料主體基本權保障之前提下，得另以附件之方式新增條款。
§3	利益第三人條款
§4	關於此 SCC 的名詞、原則之解釋須與 GDPR 一致。
§5	此新版 SCC 相較於先前已訂立之契約，具有適用上之優先性。
§6	傳輸雙方之資訊、傳輸資料類別及目的須列明於 Annex I.B。
§7	對接條款（Docking Clause）
Section 2 (模組化設計)	
§8	資料處理原則
§9	複委託處理者
§10	資料主體之權利；以及面對資料主體之請求，資料輸入方得否自行回應。
§11	救濟
§12	責任歸屬
§13	監管
Section 3 (對第三國國內法及政府部門存取資料之因應)	

[110] *Id*. Annex §3.
[111] *Id*. Annex §§1-7.
[112] *Id*. Annex §§8-18. 惟第 14 條至第 16 條明文規定四種模組皆有適用，故其性質實質上較為近似基礎條款，特此敘明。

§14	資料傳輸影響評估
§15	第三國政府存取個人資料之因應
Section 4 (最後條款)	
§16	終止條款
§17	準據法
§18	約定管轄法院

表 1　2021 新版 SCC 各條款規範重點

一、 第一部分——基礎條款

此部分多延續前三版 SCC 所逐漸形成之若干原則，如第 2 條規定締約雙方不得直接修改 SCC 條款本身之內容，僅得以新增補充條款等方式為之，且新增之補充條款不得與此 SCC 所規範之原則相衝突[113]；利益第三人條款規範於第 3 條[114]；第 6 條規定將資料傳輸各方之資訊、所傳輸資料之種類等資訊須列明於 Annex I.B 中等等，如上表中所述[115]。而新版 SCC 主要變化重點如下：

（一）第 7 條 對接條款（Docking Clause）

非締約之第三方得在任何時候，取得所有締約方之同意後，以資料管控者或資料處理者的身分成為締約方。此條款因應現今複雜之傳輸樣態中，可能不只一位資料管控者或一位資料處理者，將對接條款明文化得省去重複締約之繁瑣及不必要之時間浪費，亦可使資料傳輸過程中，所有參與者之權利義務更加清楚明確，甚值贊同[116]。

[113] *Id*. Annex §2.
[114] *Id*. Annex §3.
[115] *Id*. Annex §6.
[116] *Id*. Annex §7; Marcelo Corrales Compagnucci et al., *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, 2021(2) NORDIC JOURNAL OF EUROPEAN LAW 37, 44 (2021).

（二）第 14 條 資料傳輸影響評估（Transfer Impact Assessment, TIA）

雖第 14 條至第 16 條之位置座落於第二部分模組化條款中，惟本條至第 16 條條文中皆有明文規定 Module 1 到 Module 4 皆有所適用，合先敘明之。

本條係為因應 Schrems II 案之判決內容所設立，締約雙方必須於傳輸前進行資料傳輸影響評估，內容包含就資料傳輸過程中各方、傳輸目的、所涉及之資料種類等，以確保：（1）資料輸入方之國內法律或實務作法是否會與此 SCC 條款相衝突；（2）是否須採取其他更多之技術性措施或組織性補充措施以加強對資料之保護，並將資料傳輸影響評估之結果作成書面，送交主管機關[117]。

又雙方必須在傳輸之過程中持續地確保資料傳輸影響評估之結果，若資料輸入方之國內法律進行修改或實務作法有所更動等，資料輸入方有義務向資料輸出方進行通知；另外，若因資料輸入方之國內法律修改或其他因素，使資料輸出方有相當理由認為資料傳輸行為已不再符合此 SCC 條款，則資料輸出方應採取適當之技術性或組織性補充措施，使資料傳輸行為能夠再次符合此 SCC 條款，若資料輸出方認為採取若干補充措施仍無法符合 SCC 條款之標準，則應中止資料傳輸行為[118]。

（三）第 15 條 第三國政府存取個人資料之因應

本條明顯係為試圖回應歐盟法院在 Schrems II 案中，展現對於美國國家情報機關對歐盟公民監控之擔憂所設，第 15.1 條規定，在「收到資料輸入方公部門（包含司法機關）依該國國內法律，要求提供該等跨境傳輸之個人資料」或「獲知資料輸入方公部門（包含司法機關）依該國國內法律，已直接取得該等跨境傳輸之個人資料」時，資料輸入方應通知資料輸出方，並於可能的情況下亦通知資

[117] 2021 SCC Annex §14; Marcelo Corrales Compagnucci et al., *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, 2021(2) NORDIC JOURNAL OF EUROPEAN LAW 37, 44 (2021).
[118] 2021 SCC Annex §14.

料主體[119]。

而資料輸入方於提供個人資料於公部門時，應在符合該國國內法要求之情況下，以資料給予最小化之原則為之。另外，於同意該公部門之要求給予資料或獲知該公部門已直接存取資料後，資料輸入方應評估該公部門之要求或行為是否確實符合該國國內法律及相關國際法標準，若於評估後有相當理由認為該公部門之要求或行為有合法性之疑慮，資料輸入方應盡力尋求救濟或上訴之途徑，並應尋求以臨時措施中止該等資料存取行為[120]。上述各項通知、救濟程序等，資料輸入方均應詳實紀錄，以便日後提供予資料輸出方或相關監管機關[121]。

二、第二部分——模組化條款

首先，第 8 條係規定關於資料處理之原則，其規範均與 GDPR 所揭示之原則大同小異，惟規範密度上略有差異[122]。另值注意者為，第 9 條複委託處理；第 10 條面對資料主體之請求，資料輸入方是否得自行回應；第 11 條關於救濟途徑等規範。

（一）第 9 條 複委託處理

1. 僅有在模組二、模組三，即資料輸入方為資料處理者之情形，始有適用本條資料複委託處理之可能，合先敘明之。而欲進行資料複委託處理，有以下兩種方式：

（1）明確事前授權

一般情形下，若資料輸入方欲將資料處理之任務進行複委託，須得到資料輸

[119] *Id*. Annex §15.1.
[120] *Id*. Annex §15.2.
[121] *Id*. Annex §§15.1, 15.2.
[122] *Id*. Annex §8.

出方／模組三中為資料管控者之明確書面授權始得為之。資料輸入方須在進行複委託行為前之合理期間，向資料輸出方／模組三中之資料管控者提交授權之請求，並提供資料輸出方／模組三中之資料管控者決定是否給予授權所需之一切資訊[123]。

（2）一般性書面授權

資料輸出方／模組三中之資料管控者得預先就資料複委託處理行為，就合格之資料複委託處理者擬有一份事前同意清單，資料輸入方始得逕就該清單上之人選，直接進行複委託。而若嗣後資料輸入方欲就該名單之人選進行變更，須在進行複委託行為前之合理期間，以書面形式通知資料輸出方／模組三中之資料管控者其欲改動之人選，使資料輸出方／模組三中之資料管控者有充足的時間考慮拒絕或接受。並須提供資料輸出方／模組三中之資料管控者決定拒絕或接受所需之一切資訊[124]。

2. 進行複委託處理時，資料輸入方須與複委託處理者以契約約定，資料複委託處理者須負擔如同資料輸入方在此 SCC 下之義務，包含利益第三人條款等。換言之，一旦資料複委託行為成立，資料複委託處理者即係等同於立於資料輸入方之地位進行資料處理，故須遵守此 SCC 之所有規範。惟資料輸入方須就資料複委託處理者之資料處理行為負責，於其有違反 SCC 條款之行為時通知資料輸出方[125]。

3. 資料輸入方與資料複委託處理者間需簽訂利益第三人條款，內容為使資料輸入方實體上消失、於法律上清算或解散時，資料輸出方有權力終止複委託處理契約，並指示資料複委託處理者刪除或返還其經手處理之個人資料[126]。

---

123 2021 SCC Annex Module 2 §9(a), Module 3 §9(a).
124 *Id*.
125 2021 SCC Annex Module 2 §§9(b)-(d), Module 3 §§9(b)-(d).
126 2021 SCC Annex Module 2 §9(e), Module 3 §9(e).

（二）第 10 條 個資主體之權利，以及面對資料主體之請求資料輸入方是否得自行回應

第 10 條則係規範當資料主體提出請求時，資料輸出方及資料輸入方之權利義務，僅在模組一（管控者傳輸至管控者），資料輸入方面對資料主體所提出之請求，得自行回覆資料主體，資料輸出方僅須提供適當之協助即可；但在模組二（管控者傳輸至處理者）及模組三（處理者傳輸至處理者）之情形，資料輸入方應通知資料輸出方，不得逕自回覆資料主體之請求；模組四（處理者傳輸至管控者）之情形則係雙方須相互配合協助，共同回覆資料主體[127]。

（三）第 11 條 救濟

此部分留待本章第二節第三項說明。

（四）第 12 條 責任歸屬

另第 12 條責任歸屬方面，基本上資料輸出方與資料輸入方須對資料主體負連帶責任，於發生損害時，資料主體得自行選擇其欲向何者請求損害賠償，而先負擔損害賠償者得再對實際造成損害之一方，或傳輸過程中實際造成損害之其他第三人為請求，自不待言。另外，資料管控者不得以損害係資料處理者或複委託處理者所造成，與其無涉等語作為有效之抗辯；資料處理者亦不得以損害係複委託處理者所造成作為有效之抗辯，亦屬當然[128]。

（五）第 13 條 監管

此部分留待本章第二節第三項說明。

[127] 2021 SCC Annex §10.
[128] *Id*. Annex §12.

第二節 新版 SCC 和 GDPR 保護規範之比較

本節擬整理 GDPR 所揭櫫之各項基本原則及資料主體得主張之權利，以及監管救濟途徑，與 2021 新版 SCC 中之規範有何異同之處。換言之，即本文雖於前述第二章已就 GDPR 之基本架構做過初步介紹，惟本節以下將更進一步針對其中各項原則、各方權利義務之保護密度及實務發展，以及監管及救濟途徑等層面是否有所差異，作更深入之比較。簡要整理表格可先參見下表 2。

<table>
<tr><td>GDPR</td><td>2021 SCC
模組一</td><td>2021 SCC
模組二</td><td>2021 SCC
模組三</td><td>2021 SCC
模組四</td></tr>
<tr><td colspan="5">資料處理原則</td></tr>
<tr><td>透明性原則與資料主體知情權</td><td colspan="3">✓
（有準用條款）</td><td>✕</td></tr>
<tr><td>目的性原則</td><td colspan="3">✓</td><td>✕</td></tr>
<tr><td>最小化蒐用原則與正確性原則</td><td>✓</td><td colspan="2">Δ
Module 2, 3 僅有正確性原則</td><td>✕</td></tr>
<tr><td>儲存時間最短化</td><td colspan="3">✓</td><td>✕</td></tr>
<tr><td>資料完整性及保密性</td><td colspan="4">Δ
內涵仍不清楚</td></tr>
<tr><td colspan="5">資料主體權利</td></tr>
<tr><td>知情權</td><td colspan="4">N/A，整合進透明性原則中一併討論</td></tr>
<tr><td>接近使用權</td><td>✓</td><td colspan="3">Module 2~ Module 4 ✕</td></tr>
<tr><td>更正權</td><td>✓</td><td colspan="3">Module 2~ Module 4 ✕</td></tr>
<tr><td>刪除權（被遺忘權）</td><td>Δ
適用情境較 GDPR 條文少</td><td colspan="3">Module 2~ Module 4 ✕</td></tr>
<tr><td>限制使用權</td><td colspan="4">✕</td></tr>
</table>

資料可攜權	✕	
拒絕權	**Δ** 僅規範「當個資係被用於市場行銷目的時，個資主體得隨時拒絕」	Module 2~ Module 4 ✕
限制個人自動化決策及剖繪權	**Δ** 僅規範限制自動化個人決策	Module 2~ Module 4 ✕
資料管控者／處理者義務		
確保資料處理安全性	✓	
關於設計階段及預設的個資保護（by design and by default）	✕	
個資侵害事件之通報、通知義務	✓	
處理活動之紀錄、與監管機關合作	✓	
資料影響評估與事前諮商義務	✕，和 2021 SCC 第 14 條的 TIA 目的不同	
監管		
監管	✓（不影響 GDPR 所規範監管機關之權利義務）	✕
救濟		
救濟	✓（不影響 GDPR 所規範監管機關之權利義務）	
圖示說明：		

✓: 與 GDPR 規範無明顯實質落差； Δ: 規範密度低於或範圍小於 GDPR 規定； ✕: 無規範。

表 2　GDPR 與 2021 SCC 四個模組之規範比較

第一項　資料處理原則與資料主體權利

蓋資料主體權利之內容多有與資料處理原則相互對應者，故本文於比較 2021 新版 SCC 與 GDPR 之規範差異時，將資料處理原則與資料主體權利一併於第一項討論之。

第一款　透明性原則與資料主體知情權

透明性原則及資料主體之知情權（受告知之權利）係 GDPR 中非常重要之基本原則及資料主體權利，其精神貫串整部 GDPR，於 GDPR 後面之章節，亦可看出其他條文亦常考量透明性要求及資料主體知情權是否受到滿足。

一、GDPR 規範

GDPR 第 5.1 條（a）項係規定資料處理須合乎合法性、公平性、透明性之原則。合法性之部分，實際上 GDPR 各條款中對於各項權利義務均有詳細之規範，GDPR 第 5 條中所謂資料處理須符合合法性原則，僅為一總體性之規範，實際資料處理行為之內涵合法與否，仍須視其是否遵守其他各條項規定觀之。公平性之概念則著重於消除資料管控者與資料主體間資訊不對稱，或對於專業上之知識落差，具體之消除方式係透過達成透明性之要求來完成，故許多概念上與透明性要求相輔相成[129]。

較具討論性之處在於透明性規定之要求，蓋 GDPR 第 5 條雖規定資料處理

[129] GDPR art. 5(1)(a).

均須符合透明性要求，惟卻未給予其明確之定義，僅於前言第 39 點中對於透明性要求之內涵有些許描繪，其稱：「透明性要求係指任何關於個人資料處理之資訊，須易於接近使用，且以清楚、直白的用語使其容易理解。此項要求特別係針對受影響之資料主體，其得向資料管控者要求取得關於其個人資料被處理之相關資訊，以符合 GDPR 所謂公平性及透明性要求之資料處理原則[130]。」

另外，透明性要求亦常與 GDPR 第 12 條以下規範之資料主體知情權（或稱受告知權）相互連結，第 12 條為原則性之規範，其第 1 項規範：「資料管控者應採取適當措施，以簡潔易懂、透明且易於接近使用之格式，並採用清楚直白之語言，提供第 13 條及第 14 條所定任何資訊及資料主體基於第 15 條至第 22 條及第 34 條之權利，提供針對資料主體所進行之處理行為的內容[131]」。

第 13 條則接續地具體規範「直接蒐集」時，從資料主體蒐用有關其個人資料時，資料管控者應於取得個人資料時，提供資料主體下列所有資訊，即於第 1 項及第 2 項洋洋灑灑規範許多應提供予資料主體之資訊，包含：管控者之身分及聯繫方式；資料保護長（或稱資料保護專員）之聯繫方式；所欲處理之個人資料之處理目的及該處理之法律依據；處理之合法依據係依同法第 6 條第 1 項第 f 點者，該管控者或第三人所追求之正當利益；個人資料之接收者或接收者的類型；若欲將其個人資料移轉至第三國或國際組織，是否具執委會通過之適足性認定，或於例外傳輸合法事由所定得傳輸之情形者，告知採取何等適當之保護措施及取得該副本之方式；個人資料將被儲存之期間，或如告知確切之期間實際上不可能者，如何決定該期間之標準；處理係依據第 6 條第 1 項 a 款或第 9 條第 2 項 a 款者，資料主體有隨時撤回其同意之權利；向監管機關提起申訴之權利；個人資料

[130] GDPR recital 39 ("…The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…").
[131] GDPR art. 12(1).

之提供係法定義務或契約要求，或係訂立契約之必要要件，以及資料主體是否有義務提供個人資料，以及未提供該些資料的可能後果；重申其他資料主體得依第 15 條至第 22 條主張之權利[132]。

第 14 條則係針對「間接蒐集」時，資料管控者須盡到之通知義務，其規範內容前 2 項與第 13 條之內容大致相同，較大之差別在於第 14 條第 5 項對於告知義務設有較多之例外規定，不僅於資料主體早已得知該些資訊之情況下得免除（此部分第 13 條亦然），另外尚規範如提供該些資訊實際上係不可能或花費過鉅，尤其是為了實現公共利益、科學、歷史研究目的或統計目的，或本條第 1 項所定義務可能使該處理目的無法實現或嚴重損害者，於此情形，管控者應採取適當保護措施以保護資料主體之權利及自由，代替向資料主體提供資訊[133]。

二、新版 SCC 部分

（一）新版 SCC 第 8 條資料處理原則

1. 模組一規範

蓋透明性要求常會與資料主體之受告知權相互連結，已如前述。2021 新版 SCC 在四個模組中對於透明性要求之規範，均無如第 12 條先為一總則性之規範，而係直接以 GDPR 第 13 條、第 14 條之規範架構作模板，作成相類似之規範。

2021 SCC 在模組一第 8.2 條之規範中，對於透明性要求之規範採用與 GDPR 第 13 條、第 14 條相似之架構，其規定資料輸入方（在模組一中為境外之資料管控者）須通知個資被蒐用之資料主體，關於資料輸入方身份、聯絡資訊、個資主體被蒐用資料之類型、其得要求 SCC 條款副本之權利、若該資料主體之個資有進一步被傳輸至其他第三方，該第三方之類別以及為進一步傳輸至其他第三方之

[132] GDPR arts. 13(1), (2).
[133] GDPR art. 14(5).

目的等[134]。

除非係資料主體已從資料輸出方處得知上述資訊，或進行上開通知將對資料輸入方構成不符比例原則之負擔或難認通知係可能，始得例外免除資料輸入方之通知義務。惟在資料輸入方例外免除通知義務之情形，資料輸入方仍須以大眾皆可取得之形式發布相關之隱私公告。而若提供資料主體 SCC 條款完整之副本（包含 Appendix）將損害雙方之商業秘密（business secret）或其他機密性資訊，則資料輸入方得先將 Appendix 中之資訊進行編輯後再進行交付，以維護上述商業機密。惟須提供予資料主體進行編輯之摘要（須對於資料主體而言係有意義）及在不損及相關商業機密之前提下，提供資料主體為何須進行編輯之理由[135]。

雖 2021 SCC 在此部分之條文長度及內容較 GDPR 第 13 條、第 14 條來得短，惟 2021 SCC 在模組一第 8.2 條第（d）項特別明文規範，同條第（a）項至第（c）項不排除資料輸出方在 GDPR 第 13 條、第 14 條中所須遵守之義務。換言之，2021 SCC 模組一雖僅針對資料輸入方進行規範，表面上與 GDPR 之規範略有落差，惟其實質上並無與 GDPR 作成不同密度之保護原則，而係和 GDPR 之義務及解釋原則相互一致[136]。

2. 模組二規範

關於透明性要求之條文，模組二係規範在第 8.3 條，在模組二第 8.3 條之規範即相較模組一第 8.2 條精簡許多，僅規範如模組一第 8.2 條（b）項，原則須依資料主體之要求，提供 SCC 條款完整之副本及例外；以及若涉及損害商業機密之情形時，可先經編輯後始提供等，此係模組二中之資料輸入方為資料處理者，故不適用 GDPR 第 13 條、第 14 條之規定所致。另外於條文最後亦規定本條不

[134] 2021 SCC Annex Module 1 §8.2(a).
[135] *Id*. §§8.2(b)-(c).
[136] *Id*. §8.2(d).

排除資料輸出方在 GDPR 第 13 條、第 14 條中所須遵守之義務[137]。

3. 模組三規範

模組三第 8.3 條之規範與模組二第 8.3 條之差別，僅在於模組三無規定「本條不排除資料輸出方在 GDPR 第 13 條、第 14 條中所須遵守之義務」等文字，蓋模組三之締約雙方為「歐盟境內之資料處理者傳輸至位於歐盟境外之資料處理者」，此時資料輸出方並非資料管控者，因而造成上述規範上之差異，亦不難理解[138]。

4. 模組四規範

模組四對於透明性要求並無規範。實際上，若縱覽 2021 SCC 模組化之各條文，會發現模組四之規範強度及密度明顯低於其他三類模組，甚至在多個條文中，模組四係直接被排除適用（無任何規範），此情形是否係因模組四之傳輸路徑係相對單純地由歐盟境內之資料處理者將已處理完成之資料，傳輸至歐盟境外之資料管控者，故立法者認為無庸加以過多之管制所致，不無疑問。因本節許多條文皆有同樣之問題，由於章節編排之故，此部分之探討本文擬留至後續章節一併討論之。

（二）新版 SCC 第 15 條面對第三國政府存取個人資料之因應

按新版 SCC 第 15.1 條規定，在「收到資料輸入方所在地公部門（包含司法機關）依該國國內法律，要求提供該等資料主體之個人資料」或「獲知資料輸入方所在地公部門（包含司法機關）依該國國內法律，已直接取得該等跨境傳輸之個人資料」時，資料輸入方應通知資料輸出方，並於可能的情況下通知資料主體

137 2021 SCC Annex Module 2 §8.3.
138 2021 SCC Annex Module 3 §8.3.

[139]。本條僅規定資料輸入方於上述情形發生時，有通知資料輸出方之絕對義務，然僅於「可能的情況下」始須通知資料主體，而非「應」通知資料主體，如此規範方式是否符合 GDPR 資料處理透明性原則以及資料主體知情權，不無疑問。

三、統整

雖然 2021 SCC 於模組一至模組三對於知情權通知義務之規範較 GDPR 第 13 條至第 14 條來得短，然模組一與模組二由資料管控者作為資料輸出方之樣態均設有「上述規定不排除資料管控者在 GDPR 第 13 條、第 14 條之義務」之文字，具有準用條款之意味，綜上所述，撇除模組四規範密度明顯低於其他三類模組之問題（此問題留待後述討論），於透明性要求之方面，2021 SCC 第 8 條與 GDPR 之規範於實質上並無顯著差異，惟在第 15 條面對第三國政府存取個人資料之因應部分，可能有對資料主體權利保障不周之虞。

第二款 資料完整性與保密性原則

資料完整性與保密性原則可說是資料保護之最核心原則，蓋所謂「資料保護」之最核心內涵即在於使資料主體之個人資料得受到適當之保護，不會遭受無合法權源之第三人任意取得或破壞；換言之，若資料無法受到完整且嚴密之保護，使無合法處理蒐用權利之人亦得任意使用、甚至進行刪除、竄改等行為，則其他關於資料保護之規範及處理原則恐淪為空談，蓋有合法權源始得蒐用處理個資之此一法制前提已蕩然無存，更遑論其他如資料處理之透明性、公平性等要求，由此可見，維持資料之完整性及保密性係資料保護最重要的課題之一。

一、GDPR 規範

按 GDPR 第 5 條第 1 項 f 款：「以確保個人資料適當且安全的方式進行處理，

[139] 2021 SCC Annex §15.

包括防止未經授權之處理、非法處理，以及意外遺失、毀損或破壞，並採取適當的技術性或組織性措施[140]。」

二、新版 SCC 條文規範

雖 2021 SCC 之四個模組均對資料完整性與保密性於第 8 條設有規範（按：模組一第 8.5 條、模組二／模組三第 8.6 條、模組四第 8.2 條）

1. 模組一至模組三規範

內容包含：(1)以確保個人資料適當且安全的方式進行處理，包括防止未經授權之處理、非法處理，以及意外遺失、毀損或破壞，並採取適當的技術性或組織性措施；(2)資料輸入方應確保經手資料處理之人員均負有法定的或契約上的保密義務；(3)當發生資料侵害事件時，資料輸入方應採取適當措施以減輕對資料主體的影響，並應立即通知資料輸出方、監管機關及資料主體，惟若資料輸入方已採取相當措施降低風險、或對資料主體進行通知實際上不可能或花費過鉅時，得以公告等方式代替通知[141]。

2. 模組四規範

模組四則係規範將上述(2)、(3)之義務人訂為資料輸出方，應係考量模組四之傳輸性質所定，此部分並無太大問題[142]。

三、統整

綜探上述內容，均僅係聲明資料輸出方及資料輸入方應於傳輸過程「採取適當之技術性及組織性補充措施」，以避免資料之毀損滅失、竄改、外洩等，以及

[140] GDPR art. 5(1)(f).
[141] 2021 SCC Annex Module 1 §8.5, Module 2 §8.6, Module 3 §8.6.
[142] 2021 SCC Annex Module 4 §8.2.

發生侵害事件時之通報義務等，並無將前述 EDPB 2021 年所發布之建議的內容完整明文化，意即將技術性與補充性之內涵具體化於條文當中，或如該份建議於附件進行若干之例示[143]。如此之結果，將導致資料輸出方及資料輸入方應進行何種行為，始得符合所謂「適當之技術性及組織性補充措施」，以達成保護資料之完整性及保密性原則，仍陷於一混沌不明之狀態。

本次 2021 新版 SCC 無將 Schrems II 案判決中之一大伏筆，即技術性及組織性補充措施之具體內容作成更明確之規範，實屬可惜，不確定歐盟執委會是否認為不適當於 SCC 條文中將該等標準一錘定音，或有何其他考量不得而知，惟目前可以確定的是，對於技術性及組織性之具體形式及內涵，可能得先參考 EDPB 於 2021 年所發布之建議之例示及內容，惟實務是否將全盤接受此等標準，仍有待觀察。

第三款 其他資料處理原則

其他基本原則如目的性原則、正確性原則、儲存時間最短化原則等[144]，2021 SCC 模組一至模組三之規範文字雖或有與 GDPR 些微不同之處，其保障之力度及精神尚可稱與之無明顯實質差異，惟除模組二及模組三不知何以特意排除最小化蒐用原則之適用[145]，此部分原因並不明確，不知歐盟執委會於制定之初有何考量，本文認為似無特意排除最小化蒐用原則規定之必要。

第四款 刪除權

一、GDPR 規範

資料主體之刪除權，亦多有稱之為「被遺忘權」者，蓋其概念係在 GDPR 施

143 EDPB, *supra* note 72.
144 GDPR arts. 5(1)(b), (d), (e).
145 2021 SCC Annex Modules 1-4 §8.

行前即由一著名之歐盟法院判決——Google Spain v. AEPD 案所確立[146]。按所謂被遺忘權，係指每個人對於其不願意被搜尋到之個人資料，有請求資料管控者刪除，或以適當之方式進行屏蔽、防止一般大眾輕易獲知之權利。

其後進入到 GDPR 時代，學者多認為 GDPR 第 17 條刪除權之規定中，已將過往歐盟法院實務肯認之被遺忘權，正式明文化納入之[147]。並於第 17.1 條規定，在符合個資於蒐用目的下已不再需要（即 Google Spain v. AEPD 案中申請人想被遺忘之情形）、資料主體撤回同意，且管控者無其他合法蒐用事由、資料主體行使 GDPR 第 21 條之拒絕權等其中一項要件時，資料主體得向資料管控者行使刪除權[148]。

二、新版 SCC 規範

惟 2021 SCC 模組一第 10 條（b）款（iii）目中僅規範「當資料主體之個人資料，被以違反本契約利益第三人條款之各條款之方式處理，或資料主體撤回其同意時，資料主體得向資料輸入方行使刪除權[149]」，規範之要件事由樣態明顯少於 GDPR 規範者，如 Google Spain v. AEPD 案中所確立之當「個資於蒐用目的下已不再需要」時，單純被遺忘之權利；以及與 GDPR 第 21 條拒絕權之配套措施均付之闕如[150]，且模組二至模組四對刪除權均無設有任何規範。

---

146 Case C-131/12, Google Spain v. AEPD and Mario Costeja González (May 13, 2014).
147 郭戎晉，論區塊鏈技術與歐盟一般資料保護規則之衝突，臺大法學論叢，50 卷 1 期，頁 69，頁 114（2021 年）。
148 GDPR art. 17.1.
149 2021 SCC Annex Module 1 §10(b)(iii) ("erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.").
150 GDPR arts. 17.1(a), (c) ("1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed… (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2).").

第五款 拒絕權與限制個人自動化決策及剖繪權

拒絕權之部分，2021 SCC 在條文上之規範密度即與 GDPR 不同，蓋 GDPR 係規範「（1）當資料管控者之合法蒐用事由係依據執行公共任務或權衡條款時；（2）當個資係被用於市場行銷目的時，個資主體得隨時拒絕[151]」。惟 2021 SCC 模組一第 10 條（c）款僅規範「當個資係被用於市場行銷目的時，資料主體得隨時拒絕[152]」要件上相較 GDPR 有所缺乏，且模組二至模組四對此亦均無規範，2021 SCC 之規範完整度明顯較為不足。

在限制個人自動化決策及剖繪權亦有類似之問題，因「剖繪」與「個人自動化決策」行為雖常接續發生，惟其本質上係兩個不同之行為，無必然之伴隨關係或先後順序，GDPR 針對「個人自動化決策」及「剖繪」均設有限制[153]，而 2021 SCC 模組一第 10 條（d）款完全未針對「剖繪」方面設有任何規範[154]，保障亦明顯低於 GDPR。又模組二至模組四在此之規範亦為空白一片。

---

[151] GDPR art. 21.

[152] 2021 SCC Annex Module 1 §10(c).

[153] GDPR art. 22 ("1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.").

[154] 2021 SCC Annex Module 1 §10(d) ("(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter: (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.").

第六款 其他資料主體權利

GDPR 於第三章規範之資料主體權利，尚有接近使用權、限制使用權及資料可攜權等權利，於此些部分，2021 SCC 條文與 GDPR 存有規範上之落差，或為部分權利僅在模組一中設有規範，或係在整部 2021 SCC 均未見其規定。

（一）接近使用權及更正權之部分[155]，分別於 2021 SCC 模組一第 10 條（b）款（i）目及（ii）目中有所規範，且規範之力度與 GDPR 條文之規範尚稱一致，並無明顯之實質上落差[156]，惟模組二至模組四對此均無規範。

（二）而限制使用權及資料可攜權則係於 2021 SCC 均無規範，四種模組均然[157]。

---

[155] GDPR arts. 15, 16 ("15. (1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; 16. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.").

[156] 2021 SCC Annex Module 1 §§10(b)(i), (ii) ("(b) In particular, upon request by the data subject the data importer shall, free of charge: (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i); (ii) rectify inaccurate or incomplete data concerning the data subject").

[157] GDPR arts. 18, 20 ("18. (1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or

第二項 資料管控者／處理者義務

第一款 關於設計階段及預設的個資保護（by design and by default）

一、GDPR 規範

按所謂關於設計階段之個資保護(by design)即指，在服務的設計構想階段，對於個資保護之方式或欲形成之個資保護密度而言；預設（by default）即指如網站或社群媒體上對於隱私保護設定之預設值或選項預設[158]，雖 GDPR 第 25 條條文本身在此部分多係重申整部 GDPR 所揭示之個資保護原則，如規定「考量到執行成本及處理之性質、範圍、內容與目的，以及該處理行為對當事人之權利及自由產生之諸多可能的嚴重性風險，在設計處理方式時，管控者即應實施適當之技術性及組織性措施，以實踐 GDPR 所揭示之資料處理原則，並採取有效之方式將必要的保護措施納入處理程序，以符合 GDPR 保障資料主體權利之要求」、「管控者應實施適當之技術性及組織性措施，以確保在預設情況下，僅依特定之處理目的於必要範圍內處理個人資料。該義務包含所蒐集之資料數量、處理之程度、儲存之期間及其可接近使用性，以及確保個人資料不會因他人之不當干預而受不特定之人得接近使用之」等[159]。

二、新版 SCC 對此無規範

defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject; 20. (1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.").

[158] GDPR art. 25.

[159] *Id.*

GDPR 於第 25 條將其明文化之用意，可能係在於提醒資料管控者等人於產品或服務之設計預設階段，即應對個資保護有所認識，並設定符合 GDPR 原則之個資保護水準。然而，在 2021 SCC 條文中，並無針對設計階段及預設的個資保護（by design and by default）作規範，此部分是否可能產生規範上之漏洞，不無疑問。

第二款 資料影響評估與事前諮商義務

一、GDPR 規範

按 GDPR 第 35 條規定，在使用新科技進行資料處理，可能對資料主體之權利造成侵害有高度風險之可能時，資料管控者應於進行資料處理行為前，先進行資料影響評估（Data Protection Impact Assessment, DPIA）。評估所應考量之重點應有：（1）對預期將進行之處理行為及處理目的之系統性描述，包括管控者者所追求的合法利益為何；（2）處理行為與處理目的間之必要性及比例原則；（3）對本條第 1 項所提及之資料主體之權利及自由的風險評估；（4）為處理可能之風險的應對措施，包含保護措施、保密性措施和確保個人資料保護及考量到資料主體及其他人之合法利益下，證明資料處理遵守 GDPR 之要求等[160]。而若評估之結果確為「高風險」，則資料管控者必須向監管機管進行事前諮商程序[161]。

二、新版 SCC 對此無規範

而雖 2021 SCC 第 14 條有規範「資料傳輸影響評估（TIA）」者[162]，惟 DPIA 及 TIA 之內涵及所欲達成之目標並不相同，蓋 DPIA 係在應對當新興科技出現，資料管控者若欲將之應用於資料處理，必須先對其是否將對資料主體之權利及自由造成不當侵害進行事前評估；而 TIA 則係著重於，跨境資料傳輸之契約雙方必

[160] GDPR art. 35.
[161] GDPR art. 36.
[162] 2021 SCC Annex §14.

須共同確保資料輸入方之當地國法律或實務作法並不會對資料主體之隱私權造成不當之干預。雖兩者之名稱近似，惟所側重之面向截然不同，反觀 2021 SCC 並未設有 DPIA 之規定或事前諮商程序，與 GDPR 之保護存有落差。

第三款 其他資料管控者／處理者義務

其他如資料管控者之一般義務及資料處理者之一般義務，及諸如確保資料處理安全性、處理活動之紀錄、與監管機關合作義務、當發生個資侵害事件時之通報／通知義務等[163]，則分別於 2021 SCC 四個模組之各條文中均設有規範[164]，保護密度與 GDPR 規定於此些部分並無不同。

[163] GDPR arts. 28-34 (30. (1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
(2) Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
31. The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.
33. (1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. (2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
34. (1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.).

[164] 2021 SCC Annex Module 1 §§8.5, 8.9, 13; Module 2 §§8.6, 8.9, 13; Module 3 §§8.6, 8.9, 13, Module 4 §§8.1, 8.2, 8.3.

第三項 監管與救濟

第一款 監管

一、GDPR 相關規範

按 GDPR 條文中關於監管機關之規範，以第六章規範前述「一站式紛爭解決機制」及各監管機關之相互合作，並於第 57 條、第 58 條明確規範監管機關之職責與擁有之權力[165]。

其中第 57 條明訂監管機關之職責包含：監控及執行 GDPR 之適用；與其他監管機關合作，包括分享資訊及互助，以確保本規則適用與執行之一致性；監控將會影響個人資料保護之發展情形，特別是資訊與通訊科技及商業實務上之發展；於資料影響評估與事前諮商程序發揮積極作用等[166]，並於 GDPR 其他部分之條文中亦可看到與監管機關有關之規範，如第 30 條關於資料保存義務應使監管機關需要時得以取得、第 31 條與監管機關之一般合作義務、第 33 條規定發生資料侵害事件時，資料管控者／資料處理者對監管機關之通報義務等均如是[167]。

第 58 條則明訂監管機關擁有以下三大面向之權力：

1. 調查之權力：

命資料管控者／處理者，或其代表提供任何監管機關履行其職責所需之資訊；當有申訴聲稱其因資料管控者／處理者違反 GDPR 之行為而受有損害時，通知資料管控者／處理者；在不違反歐盟法或成員國程序法之前提下，得進入管控者

165 GDPR arts. 51-59.
166 GDPR art. 57.
167 GDPR arts. 30, 31, 33.

／處理者之任何辦公處所，包含近用資料處理之設備及處理方法[168]。

2. 糾正之權力：

當資料管控者／處理者之行為可能違反 GDPR 時，給予其警告；命資料管控者／處理者遵循資料主體依據 GDPR 所提出之請求；命資料管控者／處理者於一定期限內以適當方法使資料處理符合 GDPR 之要求；發布暫時或永久性之資料處理禁令等等[169]。

3. 授權或給予建議：

如第 36 條所規定之事前諮商程序給予資料管控者建議；依請求或主動對資料保護相關之議題發布建議性質之意見；針對 CoC, BCR, SCC 進行核准等[170]。

茲有附言者，第 58 條第 6 項更規定各成員國之國內法得授予該國監管機關上述範圍以外之權力。另一方面，歐盟法與成員國國內法應規定監管機關行使上述權力應有適當的救濟管道，俾符合歐盟基本權利憲章所規定之司法救濟及正當程序要求[171]。

二、新版 SCC 條文規範

考量到 SCC 僅為私人間契約之性質，故 SCC 的制定理論上並不影響 GDPR 關於監管機關權利義務之規範，新版 SCC 對於監管之條文僅於第 13 條以兩項簡短規範，(a) 項規定係以資料輸出方之身分決定監管機關為何人，即當資料輸出方位於歐盟境內時，資料輸出方之監管機關應列為附件 I.C 的主責監管機關，以及當資料輸出方非位於歐盟境內，但落入 GDPR 第 3 條第 2 項域外效力適用之

[168] GDPR art. 58(1).
[169] GDPR art. 58(2).
[170] GDPR art. 58(2).
[171] GDPR arts. 58(4)-(6).

範圍內，並依第 27 條指定代表人時，應如何擇定附件 I.C 的主責監管機關；(b) 項則係規定原則上資料輸入方須負擔主要與監管機關互動及配合調查之責任，如回覆監管機關之詢問、提交稽核審計資料、遵照監管機關之指示進行救濟或補償措施[172]。

此部分關於監管機關之認定，模組四未作任何規定，是否係因模組四之傳輸路徑相對單純，故直接以 GDPR 作為依據，以歐盟成員國之主管機關作為主責之監管機關，不得而知，在此於 SCC 條款中未作任何規範，是否易生責任歸屬之問題及監管上之真空，亦不無疑問。關於模組四規範密度明顯低於其他三種模組之傳輸模式，於新版 SCC 中反覆發生，關於此部分立法妥適性之評析，留待本文後續章節詳述之。

第二款 救濟

一、GDPR 相關規範

按 GDPR 第八章為救濟及行政罰鍰之規定，明確規定資料主體有向監管機關提出申訴、尋求司法救濟之權利，即資料主體若認為和其有關之資料處理行為違反 GDPR，則其有權向其住所地、工作地或侵害行為地之成員國監管機關提出申訴。而若監管機關未於三個月內作成申訴結果或向資料主體報告申訴處理之進度，資料主體得逕向該監管機關所在地之成員國法院提起訴訟。資料主體亦得於資料管控者／處理者之所在地法院，直接對資料管控者／處理者提起訴訟[173]。

二、新版 SCC 條文規範

關於救濟之部分，新版 SCC 並未對此設有新的救濟途徑或方式，亦僅係重

[172] 2021 SCC Annex §13.
[173] GDPR arts. 77-79.

申若干基本原則如下：如四種模組均有適用之第 11 條第（a）項規定，資料輸入方須以符合透明性要求及易於接近使用之格式，將有權處理相關爭議之機關的聯絡資訊通知資料主體，以個人通知或公開在其網站之方式在所不問。（a）項並設有一選擇性之條款供契約雙方自行決定是否加入：「若有其他免費之獨立爭端解決機構，資料主體亦得利用之。資料輸入方應通知資料主體另有如此之爭端解決機制可利用，惟資料主體對於欲進行何種爭端解決程序具有程序選擇權[174]。」

以及僅模組一至模組三始有適用之（b）項至（f）項，主要係規範當資料主體僅認為契約雙方之一方構成違約時，契約雙方應隨時使彼此了解救濟處理進度，於適當時，雙方應通力合作解決紛爭；當受影響之資料主體援用此 SCC 第 3 條利益第三人條款時，資料輸入方須同意資料主體向其所在地／工作地之歐盟成員國監管機關或依此 SCC 第 13 條之監管機關提出救濟，或向第 18 條所約定之管轄法院提出訴訟等[175]。

第三節 小結

按經過上述 GDPR 及新版 SCC 之綜合比較後，我們可以發現在：

（一）資料處理之六大基本原則部分，雖兩邊使用之文字或有些許不同，或涵蓋之範圍用語上有細小之差異存在，惟就前五大原則之保障精神觀之，新版 SCC 與 GDPR 間可說在規範密度上尚無實質明顯之落差。可惜的是，可說是為了回應 Schrems II 案判決結果而生之新版 SCC，在關鍵之資料完整性及保密性原則中，亦即所謂「技術性與組織性補充措施」之內涵究竟為何，要使用何種類型之技術性措施、做到何種程度均未於此份新版 SCC 中規範，可預期後續吾人將持續在此爭論不休。

174 2021 SCC Annex §11(a).
175 *Id*. Annex §§11(b)-(f).

（二）資料主體權利之部分，接近使用權與更正權於新版 SCC 之模組一有達到與 GDPR 相一致的保護水準，惟模組二至模組四於此部分卻付之闕如；刪除權、拒絕權、限制個人自動化決策及剖繪權之部分則係不僅模組二至模組四同樣形成規範真空，模組一之規範強度亦不如 GDPR 完整；限制使用權及資料可攜權則是於新版 SCC 中未見相關規定。

資料管控者／處理者的義務方面，關於設計階段及預設的個資保護（by design and by default）及資料影響評估與事前諮商義務均未於新版 SCC 中規範，對資料主體個人權利之保護恐有所不周。

（三）至於監管與救濟之部分，考量到 SCC 本身究屬私人間契約之性質，於監管及救濟方面本可想見不會有過多之著墨。新版 SCC 關於監管方面之規定僅係規範何者為負責之監管機關；於救濟方面則僅多重申 GDPR 之規定，亦無其他不合理之新規範，其餘部分應仍係依照 GDPR 之規定。

第四章 新版 SCC 與 GDPR 之合致性分析

第一節 歐盟 EDPB 對新版 SCC 之審查標準——以愛爾蘭資料保護委員會裁罰 Meta Ireland 12 億歐元案件為觀察

一、案件背景

2023 年 5 月，一件由愛爾蘭資料保護委員會對 Meta Ireland 之裁罰案件再度震驚全球，其一為本件裁罰金額高達 12 億歐元（時值約等同於 13 億美金）[176]，打破原先 2021 年 Amazon 被裁罰 7.46 億歐元之最高紀錄[177]；另一更深層的影響為，本件為 Schrems II 案判決後，美歐間企業採用 2021 新版 SCC 作為跨境傳輸法律基礎之第一個重大案件，對於美歐跨境資料傳輸法律動態上，具有指標性之意義。

愛爾蘭資料保護委員會透過前述一站式紛爭解決機制（one-stop-shop mechanism）[178]，在本件中作爲 LSA（主責監管機關）與其他歐盟各成員國之 DPA 未能取得一致之想法後，尋求 EDPB 作成具拘束力之裁決。愛爾蘭資料保護委員會遵照 EDPB 之裁決，認為 Meta 在 Schrems II 案判決後仍持續進行美歐間跨境資料之傳輸，且亦未具備其他能足以符合 GDPR 及歐洲基本權利憲章之合法依據，故裁決（1）Meta 須負擔 12 億歐元之罰款；（2）在六個月內停止資料處理行為及將儲存在美國之歐盟公民個人資料刪除[179]。Meta 則回應：歐盟法院在 Schrems II 案中曾肯定使用 SCC 作為跨境資料傳輸之合法依據，又 Meta Ireland 及 Meta 間之跨境資料傳輸契約即係以 2021 新版 SCC 為基礎簽訂，又何來無合

[176] Meta 2023 case, supra note 5.
[177] Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, EDPB (Adopted on Jul. 28, 2021), https://www.edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf [hereinafter WhatsAPP case].
[178] GDPR recital 127,128.
[179] Meta 2023 case at. 11, 213.

法基礎之說[180]？

雖然本裁決係一個案性質之 EDPB 裁決，並非一般性之立法或判例，惟仍然有高度可能將會對美歐間資料跨境傳輸立下一重大指標，可以想見美歐間數以萬計之企業間均會十分關注此一案件。以下將就為何 EDPB 會在 Meta 已採用 2021 新版 SCC 作為其法律依據之情形下，仍以違反 GDPR 第 46 條第 1 項跨境資料傳輸之規定作出如此鉅額裁罰、本件裁罰與 Schrems II 案之判決結果是否有所衝突、未來可能之發展等進行分析。

二、裁決內容簡析

在愛爾蘭資料保護委員會依照「一站式紛爭解決機制」規則，遵照 EDPB 具拘束力之判斷作成裁決，其裁決文件對於 2021 新版 SCC 合法性，係以歐盟法院 Schrems II 案之判決內容為主軸，去解釋 SCC 之定性及合法性問題，其審查架構為：(1)美國國內法律是否提供與 GDPR 及歐盟基本權利憲章相同之保護；(2)若否，2021 SCC 本身是否能填補美國法律與歐盟法律間之落差；(3)若否，本案中 Meta 所採取之其他補充性措施是否足以用來填補美國法律與歐盟法律間之落差[181]。

(一)關於層次一：美國國內法律是否提供與 GDPR 及歐盟基本權利憲章相同之保護

答案應相當明確是否定的，蓋美國對於隱私權之著重面向與歐盟截然不同，美國較著重貿易之自由；歐盟則較看重基本權之保障，這導致美國及歐盟在國內個資法制上有著難以調和的落差，故美歐雙方原先始透過《安全港協議》及《隱私盾協議》等雙邊協商之方式取得適足性認定，作為跨境傳輸之合法性基礎，已

[180] Nick Clegg and Jennifer Newstead, *Our Response to the Decision on Facebook's EU-US Data Transfers*, META (May 22, 2023), https://about.fb.com/news/2023/05/our-response-to-the-decision-on-facebooks-eu-us-data-transfers/.
[181] Meta 2023 case at. 61-62.

如前述[182]。

另外，歐盟法院在 Schrems II 案中最擔心者，即為美國情報法規及情報單位監控之問題，蓋 FISA 第 702 條允許檢察總長和國家情報主管在取得批准後聯合授權，對位於美國境外之非美國公民進行監控，並作為 PRISM 和 UPSTREAM 監控計劃之法律基礎。在 PRISM 計劃及 UPSTREAM 計劃中，美國國家安全局有權向網路服務提供商要求提供所有與系爭對象相關的通訊，其中部分內容也會傳送給 FBI 及 CIA，或向傳輸所經之電纜、交換機和路由器網絡的電信公司要求允許國家安全局進行複製及過濾網路流量，以獲得非美國公民之通訊內容[183]。

EO 12333 則係允許美國國家安全局近用過境美國之資料，如只要通過大西洋海底下之水下電纜均屬之，在該些資料抵達美國前蒐集並保管該些資料，並落入 FISA 之適用範圍，且依據 EO 12333 進行之活動不受司法審查[184]。由此亦清楚可見美國國內法律與歐盟之個資保障規範及基本權利憲章第 7 條、第 8 條、第 47 條之保障水準有非常大之差異。

（二）關於層次二：2021 SCC 本身是否能填補美國法律與歐盟法律間之落差

EDPB 緊抓著 Schrems II 案中之判決段落，即「因此，縱使在某些情況下，根據相關第三國國內法律和實務作法，跨境傳輸的接收方僅基於 SCC 條款即可達確保資料保護的必要程度，但在其他情況下，SCC 的內容可能不足以實質上有效保護傳輸到第三國的個人資料，特別是在該第三國的國內法律允許其政府機關干涉與該些資料相關的資料主體權利時[185]。」EDPB 認為歐盟法院已於 Schrems

[182] *Id*. at. 67.
[183] *Id*. at. 68.
[184] *Id*. at. 68.
[185] Schrems II para. 126 (“Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of

II 案判決中明確表示，當第三國的國內法律允許其政府機關對資料主體之個人資料及權利進行干預（當然包含情報監控在內）時，SCC 本身已無法有效保證資料主體基於歐盟基本權利憲章下之權利，蓋 SCC 僅拘束契約雙方，並無法拘束第三國政府單位[186]。

當然 Schrems II 判決當時之法律基礎為 2010 SCC 而非 2021 SCC，惟 EDPB 認為，探究 2021 SCC 之內容，雖其新增若干之模組化傳輸樣態、某些程序規範上之優化更新、以及引人注目的第 14、15 條新設之義務，然於填補美國國內法律與歐盟保護水準之落差，並無實質上的新貢獻，蓋不論是依新版 SCC 第 14 條進行傳輸影響評估，或是依第 15 條要求資料輸入方應「盡力為資料主體權利尋求救濟」，都僅為程序上之微幅優化，均無法改變美國政府機關得透過 FISA 702 條款或 EO 12333，得不經司法審查地對非美國公民進行監控行為，因第 14 條 TIA 之義務僅為進行評估，若欲進行資料傳輸，評估之結果亦勢必通過，很可能僅流於形式；第 15 條要求資料輸入方應「盡力為資料主體權利尋求救濟」，暫且撇除「應盡力尋求」之解釋問題，美國國內法規即規定上述監控行為不受司法審查，資料輸入方亦求助無門[187]。

（三）層次三：本案中 Meta 所採取之其他補充性措施是否足以用來填補美國法律與歐盟法律間之落差

EDPB 首先指出，該等「補充性措施」於填補兩國間法律落差之程度上，應不僅是「只要有所填補」即為已足，而係須使 SCC 搭配補充性措施後之結果，能達到與歐盟之保護水準相一致，這樣的論述亦符合 Schrems II 案中一再強調的，不論是適足性認定或其他跨境傳輸例外合法事由，均須符合與歐盟 GDPR 及歐

ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.").

186 Meta 2023 case at. 91-92.

187 *Id*. at. 93-94.

盟基本權利憲章之內涵達到「本質上相同」而言[188]。

進一步言之，裁決文件中說明，其認識到 Meta 確實採取包含「隱私揭露政策、通知政策、資料接近使用政策、Facebook 透明性報告等等」之組織性措施；與包含「採用符合業界標準之加密演算法與協定，使個人資料不會在未經 Meta 允許之情況下發生破壞或外洩之情事；亦針對硬體裝置、員工設備及基礎設施之全面資安保護」等技術性措施，該些措施固然可展現 Meta 維護個人資料之安全性，於資料主體間、資料主體與 Meta 間、Meta 各子公司間皆能在符合行業標準下安全地進行傳輸，惟無法解決 Meta 係受到美國政府情報單位監控之實體，且相關情報單位得依據 FISA 法案或 EO12333 任意對境外公民之活動進行監控等事實，美歐間在個資保護上法制之差距，並未因上述 Meta 所採取之額外補充措施成功彌補[189]。

從 EDPB 之上述裁決內容，可以發現 EDPB 認為 Meta 所採取之相關措施及政策，均符合 2021 新版 SCC 之內容，惟按 Schrems II 案中所謂「對 SCC 作為跨境傳輸合法依據之側面肯定」，並非是只要採取 SCC 作為合法依據，即可直接推論其跨境傳輸行為一定符合歐盟資料保護之水準，而係依據 GDPR 前言第 108 點之原則，即於資料跨境傳輸之情境，資料輸出方應採取「適當措施」以補足雙方在法律保障密度上可能存在之差距[190]。換言之，當單純採取 SCC 並不足以填

---

[188] *Id*. at. 95; Davinia Brennan et al., *EU-US Data Transfers Back in the Spotlight Following Record €1.2bn Fine*, MATHESON LLP (May 24, 2023), https://www.matheson.com/insights/detail/eu-us-data-transfers-back-in-the-spotlight-following-record-1.2bn-fine.

[189] Meta 2023 case at. 94-100.

[190] GDPR recital 108 ("In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a

補兩國間國內法律之落差時，尚須以其他「補充性措施」來搭配 SCC 使用，並須達到與歐盟保護水準本質上相同之程度始能符合合法之跨境資料傳輸。

而今 Meta Ireland 及 Meta US 針對雙方之資料跨境傳輸行為縱採用最新之 2021 SCC 作為跨境傳輸之法律基礎，且已合力採取諸多補充性措施，Meta 之作法仍不足以符合歐盟對於其公民資訊隱私權及訴訟權等基本權利之保障，蓋不論是 2021 SCC 或 Meta 所採取之補充措施，均無法防止美國情報單位不受司法控制地對歐盟公民之進行監控，故綜合 Meta 基於 2021 SCC 所制定之契約及所採取之補充性措施，並不符合歐盟資料保護之水準，即非符合 GDPR 第 46 條規定之合法傳輸。

（四）其他事項

另外應值注意的是，裁決文件中針對其他例外合法事由也一併提出意見，其指出除了適足性認定及 SCC 外，確實仍有如「取得資料主體之明確同意」等例外合法事由[191]，惟其認為此等例外事由不應適用於例行性(routine)的資料傳輸，蓋其同意須針對「將發生之資料傳輸行為」為之，已發生之資料傳輸行為並不包含在內，也不得用一次性的包裹式同意為之，故若屬於例行性、有持續發生可能性之資料跨境傳輸行為，在性質上即不適合以此種方式作為唯一之合法依據。且考量到歐盟基本權利憲章第 47 條訴訟權保障之精神，美歐間之資料跨境傳輸若欲使用「取得資料主體之明確同意」作為例外事由，則須明確揭露以下內容使將受影響之資料主體，使其清楚了解到：（1）此等資料跨境傳輸行為將不受到歐盟基本權利憲章第 7、8 條之保護；（2）美國之國內情報法係不符合歐盟基本權利憲章第 47 條訴訟權之保護；（3）其他資料主體可能受到之風險及不利影響。唯

memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.”).

[191] GDPR art. 49.

有在這樣的情況下取得同意，始得謂已取得資料主體明確之同意[192]。

可見 EDPB 亦認為 Meta 等公司或許會利用「取得資料主體之明確同意」作為合法依據，不僅在裁決文件中發表其對於以明確同意作為合法依據之看法，將何謂「資料主體已知悉風險且明確作成同意」之門檻提升至非常高的水準，甚至直接表示「明確同意」不適合用在例行性的資料跨境傳輸行為，實質上等同於已明確表示將「取得同意」作為跨境資料傳輸之主要合法依據並不可行。

Meta 目前已將案件上訴至歐盟法院，尋求救濟以中止愛爾蘭資料保護委員會之裁決，惟其訴訟策略係以爭執程序及權限等事項為主軸，並未直接針對實體事項異議[193]。雖本件愛爾蘭資料保護委員會遵照 EDPB 意見所作成之裁決係依照個案情狀所作成，惟對於美歐間資料跨境傳輸在 Schrems II 案判決後之發展，無疑具有一般性之指標作用。特別是針對原本被廣泛認為是後 Schrems II 案時代中，最具合法性希望之 2021 新版 SCC，被作成違法、不足以作為資料跨境傳輸合法依據之裁決，甚至一併否定以 GDPR 第 49 條取得資料主體同意作為長期合法依據之可能性，值得注意。

第二節 資料處理原則及資料主體權利之落差部分

Meta 案主要係針對技術性與組織性補充措施，及 2021 新版 SCC 當中之第 14、15 條進行分析，惟後續於其他案件中，2021 新版 SCC 之其他條文，能否符合 GDPR 及歐盟基本權利憲章之原則，亦不無疑問，故本章第二節以下將接續依第三章之順序，進行整部新版 SCC 及 GDPR 之合致性分析。

[192] Meta 2023 case at. 121-124.
[193] Court of Justice, Application (OJ) of 16 Feb, 2024, case T-8/24, Meta Platforms Ireland v European Data Protection Board.

第一項 透明性原則與資料主體知情權

第一款 WP29 指引

在 GDPR 公布到施行之緩衝期間內，時任第 29 條工作小組（WP29）曾發布一關於透明性要求之指引文件[194]，其亦指出 GDPR 關於透明性要求之規範，除了第 5 條資料處理原則之一般性規範外，如第 12 條以下資料主體之知情權，亦為透明性要求之具體展現，或可提供吾人一探透明性要求具體內涵之參考依據[195]。第 12 條條文中之用語，可以作為如何具體判斷是否達成透明性要求之判斷標準[196]：

（一）簡潔易懂的用語

所謂「簡潔」的方式係指資料管控者必須清楚地區分涉及隱私權相關之資訊／與隱私權無關之其他契約資訊，避免造成資料主體認知上之混淆。以網路或網站呈現條款之形式為例，可讓資料主體迅速找到他們所希望獲得資訊之分層次設計隱私權政策聲明，使資料主體省去爬梳數十頁冗長之內文或花費大量時間搜尋，直接以分門別類的連結，立即找到他們所期望獲得的資訊，可能會是較為理想的方式[197]。

而以何等程度的文字得符合「易懂」的語言，則須視該等資料主體之平均智

194 Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, as last Revised and Adopted on 11 April 2018, https://ec.europa.eu/newsroom/article29/items/622227.
195 *Id*. at. 6.
196 GDPR art. 12(1) (“The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.”).
197 Article 29 Working Party, *supra* note 194, ¶ 8.

識水準而言，蓋一般情況下，資料管控者應對其進行蒐用個資之資料主體群體有所認識或分析，故其應得對該等資料主體得瞭解何種程度或何種類型之專業用語，有範圍上之大致了解。舉例而言，若該等資料主體係以某行業別之專業人士為主要組成，則其對艱深文字或專業術語之瞭解程度，應會對比以學齡階段青少年為資料主體主要組成之群體來得高出許多[198]。

（二）使用清楚直白的文字

資料管控者使用之文字除了簡潔易懂外，另須具備「清楚」不模糊之要件，例如應避免使用「可能（may、might、probably）、某些（some）」等用語，盡量使用語及所欲形成之意思具體，避免抽象空泛、有過多不確定法律概念或須透過解釋的空白空間。指引中舉例若干常見之隱私權利告知方式其實均未符合上述要求，例如：「我們可能將您的個人資料用於開發新產品或服務」、「我們將用您的個人資料提供個人化之服務」等，蓋這樣的告知並未說明將會蒐用資料主體何種資料、蒐用之範圍，及蒐用目的仍不夠具體化的問題。若能具體至如「蒐用之種類為購物資料、瀏覽過之品項」等，並將目的具體至「提供更精準之商品折扣或改善網頁之設計方式」等，則較能符合上述之要求[199]。

（三）易於接近使用

而「易於接近使用」與簡潔方式之概念有些類似，均是須使資料主體得直接獲取他們所欲得知之資訊，指引中舉例如透過設立分層分項之連結、以 Q/A 專區之方式解答曾被頻繁詢問之問題或模擬一般大眾可能會詢問之情境、或設計聊天機器人之方式提供資料主體在搜尋資訊時可獲得即時之協助，均是其推薦之作法[200]。

198 *Id.* ¶ 9.
199 *Id.* ¶¶ 12-13.
200 *Id.* ¶ 11.

第二款 WhatsApp 裁罰案

以愛爾蘭資料保護委員會於 2021 年 9 月裁罰 WhatsApp 2.25 億歐元案件為例，該案件中愛爾蘭資料保護委員會透過前述一站式紛爭解決機制（one-stop-shop mechanism）[201]，在本件中作爲主責監管機關（LSA），因與其他歐盟各成員國之 DPA 未能取得一致之想法，故尋求 EDPB 之意見作成具拘束力之裁決。

其裁決結果認為 WhatsApp 未能遵守 GDPR 第 5 條第 1 項（a）款之透明性要求、第 13 條第 1 項多款關於資料主體知情權之要求，包含未清楚揭露處理之合法依據及處理目的（c 款）、將應提供之資訊分散於數個地方提供之作法，無法使資料主體輕易地清楚瞭解資料接收者之資訊或其類別（e 款）、僅以「如果有適足性認定可用之情況下，將會以適足性認定作為資料跨境傳輸之合法基礎」揭示其跨境傳輸合法依據（f 款），其內容多有引用前述 WP29 指引文件中對於透明性要求所揭示之具體化解釋及例示，顯見實務之發展與 WP29 指引文件中解釋之方向一致，該指引文件不僅對於企業該如何具體遵守抽象之透明性資料處理原則有所幫助，在實務上亦具有相當之參考價值[202]。

綜觀本件愛爾蘭資料保護委員會對 WhatsApp 之裁罰案，可以看出實務上在考量資料管控者是否符合資料處理透明性原則及資料主體知情權之要求時，不僅是考量揭露行為之與否，揭露之方式亦十分重要，即相關之資訊必須對於資料主體而言係易於接近使用、隱私權相關之資訊須與非隱私權相關之資訊分開存放，並位於資料主體合理預期得以找到的地方，須達到資料主體不需付出大量努力就能獲取上開資訊，且不會對於其是否已經取得所有可取得之資訊存有疑問之程度

[201] GDPR recital 127,128.
[202] WhatsAPP case, *supra* note 177.

始足當之[203]。

第三款 新版 SCC 第 15 條於此保障可能不足

按 2021 SCC 第 15.1 條規定資料輸入方於第三國政府機關向其要求提供資料主體之個人資料，或向資料輸入方說明其已取得資料主體個人資料時，資料輸入方對於是否須通知資料主體具有裁量權，僅於「可能的情況下」始須通知資料主體，而非「應」通知資料主體，若依前述 WP29 之指引及實務見解之發展，對於資料處理透明性原則及資料主體知情權之解釋，即使資料管控者已提供資料主體完整之資訊，惟只要存放之位置無法使資料主體輕易存取、或將應整合成一份之資料分散於數份文件中、抑或是提供之方式不夠清楚易懂，都很可能被認定為不符合資料處理透明性原則及資料主體知情權之要求，依舉輕以明重之法理，若當資料主體之個人資料已被第三國政府機關存取，而資料輸入方於知情後，竟可自由選擇是否告知資料主體，亦即資料主體可能因資料輸入方單方面之決定而對於自身之個人資料遭第三國政府存取仍毫不知情，殊難想像如此規定如何得以通過監管機關或歐盟法院對於資料處理透明性原則及資料主體知情權之嚴格標準，故本文認為，新版 SCC 第 15.1 條之規定，有極高之可能違反 GDPR 對於資料處理透明性原則及資料主體知情權。

第二項 資料處理之完整性與保密性原則

承續前述，在 Schrems II 案判決中，歐盟法院雖側面肯定 SCC 作為跨境傳輸工具之合法性，惟歐盟法院亦指出 SCC 本質上係屬私人間契約，在面對兩國法律條文或法律環境之落差，該如何填補雙邊之落差（以美歐為例，歐盟法院最在意者為如何避免美國國家政府監控之問題），有時仍需搭配其他額外之「技術

[203] Davinia Brennan, WhatsApp decision considers scope of transparency obligations under the GDPR, A&L GOODBODY LLP (Sep. 24, 2021), https://www.techlaw.ie/2021/09/articles/data-protection/whatsapp-decision-considers-scope-of-transparency-obligations-under-the-gdpr/.

性、組織性補充措施」，可惜的是，歐盟法院並無就補充措施之內涵及形式要求作進一步之闡述。在近期愛爾蘭資料保護委員會對 Meta 裁罰 12 億歐元的案件中，EDPB 亦根據 Schrems II 案，重申上述概念，並於裁決書中認定 Meta 所依據 2021 SCC 作成之契約及補充性措施仍不足以符合歐盟個資保護之水準。

其實在 Schrems II 案判決後未久，EDPB 即針對此一問題發布建議（recommendation），即針對「補充措施」之內涵進行更多闡述，及舉例若干技術性、組織性措施的例子，在 2020 年 11 月發布第一版（version 1.0），並於 2021 年 6 月更新第二版（version 2.0）並定稿之[204]，或可提供企業在擬定補充性措施時作為參考，故以下將簡介該份 EDPB 建議之大致內容，及此建議對於釐清技術性、組織性補充措施之內涵層面，有何實質影響。

第一款 EDPB 發布之建議

EDPB 所發布之建議，首先指明於資料跨境傳輸時，實踐資料保護應採取之六個步驟，分別為：1. 了解傳輸途徑；2. 確認所使用之傳輸工具為何；3. 確認接收方（第三國）當地之法律及實務作法；4. 於需要時採取補充措施；5. 如有採取補充措施，則進行相對應符合 GDPR 規範之正當程序；6. 於合理期間定期檢視資料保護水準[205]。其中 1, 2, 5, 6. 僅為較偏向原則性之重申，3. 之精神於其後被明文化成為 2021 SCC 第 14 條（TIA），4. 關於補充措施之部分即是此建議後半例示部分欲揭示之重點。

在此份建議之附件 2（Annex 2）中，EDPB 將補充性措施區分為以下三種，分別為技術性補充措施、契約性補充措施以及組織性補充措施，並例示若干具體

[204] EDPB, supra note 72.
[205] EDPB, supra note 72, at. 8-26.

情狀說明是否符合資料保護之水準：

（一）技術性補充措施[206]

按所謂技術性補充措施即係指透過現代資訊科技，如加密、假名化（pseudonymization）等方式，使第三國政府或其他未具合法使用權源之人，無法蒐用相關資料。又技術性補充措施係三種補充性措施中最根本之方式，蓋其係唯一在科學技術層面上阻斷非法蒐用可能性之補充措施，其他如契約性補充措施及組織性補充措施，係透過契約之債之效力，或組織內部之規範（內部規則）等，降低非法蒐用之可能性及提高其行為成本而已，常仍須搭配技術性補充措施始得形成完足之保護。

在此份建議中，EDPB 舉例如資料備份或資料跨境傳輸時，若資料之加密符合一定要件，如所使用之加密技術符合高強度、最新性、無已知之後門或弱點；且考量到第三國（資料輸入國）擁有之資源及技術能力，無法輕易破解該等加密；加密之密鑰僅由資料輸出方妥善保存等，則可認為此際之加密係一有效之技術性補充措施，以確保資料保護之完整性及填補兩國法律上可能存在之落差。

而於假名化之部分，EDPB 則指出，在無額外資訊（即可將假名化後之資料還原之相關技術或資訊）下，假名化後之資訊已無從辨識出原本之資料主體；同時該還原之技術或資訊係由資料輸出方單獨掌握；且考量到第三國（資料輸入國）擁有之資源及技術能力，無法在未經過資料輸出方之前提下，自行破解之，此時亦可認為假名化係一有效之技術性補充措施，其判斷標準與加密類似。

另外尚可利用將資料分割與多個處理者進行處理之方式（split or multi-party processing），如能確保多個處理者間無法透過相關技術或相互合作，拼湊出完整之資料主體資料，且第三國政府亦無權力得取得足夠部分之資料以拼湊出完整資

[206] EDPB, supra note 72, at. 28-36.

料，而資料輸出方係唯一得將多個分散之資料重新組合還原之人，則於此前提下，亦可認為此一分割處理方式亦係有效之技術性補充措施。

（二）契約性補充措施[207]

EDPB 此處特別指出之所謂「契約性補充措施」，僅係說明締約雙方可在不牴觸 GDPR 及 SCC（若雙方跨境資料傳輸之基礎選擇採用 SCC 者）之前提下，透過新增契約條款之方式，增加雙方之權利義務負擔，或使其間之分配更加明確化。此處不少 EDPB 所舉例之內容，日後均有被明文納入 2021 SCC 中，故本文將不另行重複說明之，惟 EDPB 此處之舉例，有一未被納入 2021 SCC 者本文認為其確有可參考價值，即「金絲雀安全聲明[208]」，所謂金絲雀安全聲明係指，在第三國國內法允許之前提下，契約雙方得約定，資料輸入方應定期（如最少一天一次）以加密方式向資料輸出方傳送「其於此段時間內並未接收到揭露個人資料之要求」，換言之，若無收到此一安全訊息，則可推定資料輸入方已收到來自某方要求其揭露關於資料主體之個人資料。

（三）組織性補充措施[209]

組織性補充措施係透過契約組織優化其內部控制或公司治理，達到更有效的符合法律義務之作法，如資料輸出方及資料輸入方雙方皆設置專責人員進行相關紀錄義務之工作，並透過公司內部規則，規定當確實發生政府部門要求蒐用資料主體之個人資料時，且該等蒐用有高度可能性不合法時；或平時資料主體就其基本權進行相關請求時，公司應對之標準流程建立，或主動將國際標準組織 ISO 資安相關規範、歐盟資安規範、或同業標準等主動納入公司內規當中，提昇資料保護之安全層級等。

---

207 EDPB, supra note 72, at. 36-43.
208 EDPB, supra note 72, ¶ 116.
209 EDPB, supra note 72, at. 43-46.

第二款 本文見解

本次 2021 SCC 新版修正並未將 Schrems II 案判決中之一大伏筆，即技術性及組織性補充措施之具體內容作成更明確之規範，如此之結果，將導致資料輸出方及資料輸入方應進行何種行為，始得符合所謂「適當之技術性及組織性補充措施」，以達成保護資料之完整性及保密性原則，仍陷於一混沌不明之狀態，未來相關監管機關或歐盟法院在判斷上，是否會以前述該份 EDPB 於 2021 年所發布之建議為依歸，作為判斷系爭案件之技術性及組織性補充措施之標準，即留下疑問。

在技術性與組織性補充措施之內涵仍不清楚之情況下，管控者應採用假名化、加密或何種技術性補充性措施，須達到何種程度仍不得而知，管控者縱已採取自認為相當之技術性補充措施加強保障以 SCC 作為基礎之資料跨境傳輸行為，仍無法確定其是否符合資料處理之完整性及保密性原則，本文認為，在 EDPB 所發布之建議中，「金絲雀安全聲明」可能係在有更清楚之歐盟法院判決或相關法規實務發展之前，私人公司做為資料管控者或可考慮採用之模式，蓋所謂「金絲雀安全聲明」係契約雙方得約定（在第三國國內法允許之前提下），資料輸入方應定期以加密方式向資料輸出方傳送「其於此段時間內並未接收到揭露個人資料之要求」，若無收到此一安全訊息，則可推定資料輸入方已收到來自某方要求其揭露關於資料主體之個人資料[210]。若於雙方之 SCC 契約中，另以附件加入之方式新增金絲雀安全聲明條款，則可相當程度補足原先 2021 新版 SCC 於此規範不足之問題，蓋如此之作法，不僅可使資料主體於一定之期間內就得知自己之資料可能已遭他人存取，亦不至於與 GDPR 或新版 SCC 之內容相衝突，可作為目前資料管控者為達成資料完整性與保密性原則、資料透明性原則及保障資料主體知情

[210] EDPB, supra note 72, ¶ 116.

權之暫時作法。

第三項 刪除權

第一款 Google Spain v. AEPD 案

Google Spain v. AEPD 案之背景及重點摘要如下：西班牙公民 González 因欠繳社會保險費用，以至於其不動產進入扣押、拍賣程序，該拍賣之新聞由西班牙政府委託當地報社進行報導並刊登於該報社之網站，該網站之連結同時亦由 Google Spain 所收錄。而在拍賣程序完成之數年後，該西班牙公民 González 偶然間發現自己之不動產遭拍賣的新聞仍可輕易地於 Google 引擎中被搜尋到，遂請求該報社網站撤除該連結以及 Google Spain 於其搜尋引擎中除去該連結[211]。

歐盟法院在判決中指出：Google 係以「網路爬蟲」之技術大幅減少一般人於網際網路搜尋資料之時間，而此技術背後對於個人資料之處理、副本、搜尋，該當 Dirctive 95 第 2(b)條「處理」之定義，且 Google Spain 在此過程中對於個人資料的管理權限係基於「資料管控者」之地位[212]。而歐盟法院亦正式肯認資料主體對於其不欲他人所輕易得知之內容，有權要求資料管控者刪除或以適當之方式限制之，意即首次正式肯認資料主體具有被遺忘權之權利。而 Google Spain 收受歐盟法院判決後之作法為，於歐盟地區屏蔽該則連結，故歐盟地區之使用者無法輕易透過 Google 搜尋引擎查找到該資訊，然其他地區之使用者則不受影響[213]。

---

211 Case C-131/12.
212 Case C-131/12, ¶¶ 73-75.
213 陳靜怡，隱私權新觀點：走過不留下痕跡？淺談被遺忘權與大數據，NCC NEWS，8 卷 11 期，頁 16，頁 18-19 （2014 年）。

第二款 新版 SCC 於刪除權之部分可能有違歐盟 GDPR

上述歐盟法院之判決係立於 Directive 95 之年代，惟通說均認為刪除權（被遺忘權）已於 GDPR 第 17 條確立且明訂，且為 GDPR 資料主體之重要權利之一，2021 新版 SCC 模組一第 10 條（b）款（iii）目中僅規範「當資料主體之個人資料，被以違反本契約利益第三人條款之方式處理，或資料主體撤回其同意時，資料主體得向資料輸入方行使刪除權[214]」，完全無針對 Google Spain v. AEPD 案中確立之單純被遺忘之權利設有任何規範，顯然與 GDPR 之保障有所落差，且模組二至模組四甚至對於刪除權未設有任何規範，亦形成規範上之真空，故本文認為，新版 SCC 於資料主體刪除權部分，保障密度明顯未達 GDPR 所訂之標準。

第四項 其他資料主體權利

如前第三章所述，關於其他資料主體權利之部分，新版 SCC 與 GDPR 之規範存有明顯之不足，其不足之處主要可歸納為以下三大類：

（一）模組二至模組四均有規範真空之情形：

按新版 SCC 對於接近使用權、更正權、拒絕權、限制個人自動化決策及剖繪權等部分，分別於 2021 SCC 模組一第 10 條（b）款、（c）款、（d）款中設有規範[215]，惟此些資料主體權利於模組二至模組四中卻隻字未提，此些資料主體權利應不僅限於模組一（境內管控者傳輸至境外管控者）之情形始應具備，在模組二至模組四之傳輸樣態，資料主體之上開權利亦應受到保護，雖 GDPR 條文中多規定資料主體行使其權利之對象為向管控者行使，惟在資料跨境傳輸之情形，SCC 作為得以例外地在第三國無取得適足性認定之情況下，進行資料跨境傳輸

[214] 2021 SCC Annex Module 1 §10(b)(iii).
[215] 2021 SCC Annex Module 1 §§10(b), (c), (d).

之合法依據，其內容之保障強度，應達到不減損資料主體於 GDPR 所應享有之權利而言。新版 SCC 在資料主體權利部分，多項權利均於模組二至模組四未見規範，本文猜想可能係新版 SCC 之制定者認為該些傳輸樣態之角色未必是管控者，故作成如此之差別規範，惟就資料主體權利保障及 SCC 本質之觀點來看，SCC 模組化之分類不應成為資料主權利保障之可能缺口，縱使某些傳輸樣態之角色未必是管控者，亦應使資料主體得對其行使 GDPR 中所明定之資料主體權利，始符合對資料主體權利之保障及 SCC 作為資料跨境傳輸例外合法事由之立法意旨，故本文認為現行模組化規範落差之情形，可能造成對資料主體保障不周。

（二）部分資料主體權利條文規範密度存有落差

此部分即前第三章所述如拒絕權之部分，2021 SCC 模組一第 10 條（c）款僅規範「當個資係被用於市場行銷目的時，資料主體得隨時拒絕[216]」，缺少 GDPR 所規範之另一種情形，即「當資料管控者之合法蒐用事由係依據執行公共任務或權衡條款時[217]」，保障密度及要件明顯比起 GDPR 有所缺乏。

以及在限制個人自動化決策及剖繪權之部分，GDPR 針對「個人自動化決策」及「剖繪」均設有限制[218]，而 2021 SCC 模組一第 10 條（d）款僅對「個人自動化決策」作規範[219]，考量到「剖繪」與「個人自動化決策」雖常接續出現，惟其二者間並無必然之伴隨關係，即可能僅有「剖繪」行為，而無進一步之「個人自動化決策」；或未經「剖繪」行為，即進行「個人自動化決策」，故新版 SCC 模組一第 10 條（d）款僅規範「個人自動化決策」之部分，亦對資料主體之權利保障有所不周。

（三）限制使用權及資料可攜權於新版 SCC 無規範

[216] 2021 SCC Annex Module 1 §10(c).
[217] GDPR art. 21.
[218] GDPR art. 22.
[219] 2021 SCC Annex Module 1 §10(d).

限制使用權及資料可攜權[220]則係於 2021 SCC 之四種模組均無規範，此部分與 GDPR 保障存有落差自明。

第三節 資料管控者／處理者義務之落差部分

第一項 新版 SCC 保障不足之部分

按前第三章所述，於資料管控者／處理者之義務部分，關於設計階段及預設的個資保護（by design and by default）之功能係為提醒資料管控者於產品或服務之設計或預設階段，即應對個資保護有所認識，並確保於實際處理前之設計階段，及預設階段或預設選項中，所為之行為或設定均應符合 GDPR 對處理行為之個資保護密度[221]；另外於資料影響評估與事前諮商義務中，GDPR 規定在使用新科技進行資料處理，可能對資料主體之權利造成侵害有高度風險時，資料管控者應於進行資料處理行為前，先進行資料影響評估（DPIA）[222]，而若評估之結果確為「高風險」，則資料管控者必須向監管機管進行事前諮商程序[223]，新版 SCC 在上述義務於四個模組中均無作成任何規範，不知是否係新版 SCC 之制訂者基於某種理由刻意為之，惟本文認為，資料影響評估（DPIA）及事前諮商程序均為 GDPR 條文所明定之義務，其功能亦十分清楚明確，並無與其他之義務有重疊之情形，可使管控者使用新興科技對資料主體進行資料處理行為前，多一道評估、甚至是與監管機關進行諮商之程序，又關於設計階段及預設的個資保護則具有使高密度之資料保護原則，更加延長至資料處理前行為之作用，兩者均有實際之功能與作用，不宜將之刪除，現行之新版 SCC 條文對此完全無任何規範，可能與 GDPR 之保護水準相左。

---

220 GDPR arts. 18, 20.
221 GDPR art. 25.
222 GDPR art. 35.
223 GDPR art. 36.

第二項 新版 SCC 所新增之第 14 條 TIA 之妥適性

按新版 SCC 第 14 條所設立之資料傳輸影響評估義務（TIA），於 GDPR 條文中未有相對應之章節，蓋本條係為因應 Schrems II 案之判決內容所新設立，締約雙方必須於傳輸前進行資料傳輸影響評估，內容包含就資料傳輸過程中各方、傳輸目的、所涉及之資料種類等，以確保：（1）資料輸入方之國內法律或實務作法是否會與此 SCC 條款相衝突；（2）是否須採取其他更多之技術性措施或組織性補充措施以加強對資料之保護，並將資料傳輸影響評估之結果作成書面，送交主管機關[224]。又雙方必須在傳輸之過程中持續地確保資料傳輸影響評估之結果，若因資料輸入方之國內法律修改或其他因素，使資料輸出方有相當理由認為資料傳輸行為已不再符合此 SCC 條款，則資料輸出方應採取適當之技術性或組織性補充措施，使資料傳輸行為能夠再次符合此 SCC 條款，若資料輸出方認為採取若干補充措施仍無法符合 SCC 條款之標準，則應中止資料傳輸行為，已如前述。

惟一律課與資料輸入方須持續監控資料輸入方之國內法律及實務作法發展，亦有論者表達是否將會對中小企業（SME）構成過大負擔之擔憂，蓋上開義務代表著資料輸入方須耗費相當大之法遵、行政人力以確保得持續更新資料輸入方所在地之法律及實務動態，對財星 500 大（Fortune Global 500）等級之企業可能尚屬可行，若欲賦予中小企業如此高之法遵成本，實務上恐怕難以期待[225]。

第四節 監管與救濟

第一項 監管部分

因 SCC 究屬私人間契約之性質，故 SCC 的制定理論上並不影響 GDPR 關於

[224] 2021 SCC Annex §14; Marcelo Corrales Compagnucci, *supra* note 116.
[225] En-Naoui Wissame, Transfer of personal data to third countries and the complexity of Clause 14 of the Standard Contractual Clauses at. 47 (Dec. 1, 2022) (on file with the Faculty of Law, University of Oslo).

監管機關權利義務之規範，新版 SCC 對於監管之條文僅於第 13 條規範以資料輸出方之身分決定監管機關為何人，以及原則上係由資料輸入方負擔主要與監管機關互動及配合調查之責任[226]。GDPR 所規定監管機關之職責、權利、一站式紛爭解決機制與多個監管機關之相互合作等，應不受影響，本文認為新版 SCC 關於監管之規定尚無需修改之處。

第二項 救濟部分

按新版 SCC 第 11 條係針對救濟之規範，其條文於救濟規範僅多重申 GDPR 條文之內容，已如第三章所述，惟新版 SCC 第 15 條關於第三國政府存取個人資料之因應，所規範之救濟方式，可能未達 GDPR 之要求。

按新版 SCC 第 15.2 條規定，於同意該公部門之要求給予資料或獲知該公部門已直接存取資料後，資料輸入方應評估該公部門之要求或行為是否確實符合該國國內法律及相關國際法標準，若於審慎評估後有相當理由認為該公部門之要求或行為有合法性之疑慮，資料輸入方應盡力尋求救濟或上訴之途徑，並應尋求以臨時措施中止該等資料存取行為[227]。

本條規定當面對政府部門要求提供資料主體之個人資料，或得知政府部門已經存取資料主體之個人資料時，竟並未提供資料主體任何之救濟管道，其針對第三國政府機關之資料存取行為，唯一救濟之可能竟繫諸條文中「資料輸入方應盡力尋求救濟或上訴之途徑」，何謂「盡力尋求救濟或上訴之途徑」，規範內容係不明確，資料輸入方應採取何種措施始達到「已盡力」之程度？又若資料輸入方怠於為資料主體之權利「盡力尋求救濟」，其法律效果或罰則為何？又資料主體是否有其他管道可自行提起救濟？在條文中均未見規範。如此似將資料主體權利中最核心之救濟權利，完全繫於資料輸入方之作為或不作為，對照 Schrems II 案中

[226] 2021 SCC Annex §13.
[227] 2021 SCC Annex §15.2.

歐盟法院對於資料跨境傳輸應符合歐盟基本權利憲章第 47 條對歐盟公民之訴訟權保障，加上對歐盟基本權利憲章第 47 條內涵之嚴格解釋，新版 SCC 如此之規範，很可能與歐盟法院所揭示之見解不相符[228]。新版 SCC 第 15 條係為針對 Schrems II 案中歐盟法院所擔憂之第三國國家政府監控之疑慮所設，惟新版 SCC 這樣的立法模式及強度，完全無法達到歐盟法院對於 GDPR 及歐盟基本權利憲章第 47 條之要求。

第五節 2021 新版 SCC 本身之規範架構問題

第一項 2021 SCC 第 4 條究竟是否為準用條款

按新版 SCC 第 4 條規定:「當 SCC 當中有使用 GDPR 條文中有定義之文字，則對於該名詞之解釋應與其在 GDPR 中之意義相同;本 SCC 中之條款應與 GDPR 之規定作成相一致解釋，意即本 SCC 條款不得以和 GDPR 規定之權利義務相衝突之方式進行解釋[229]」。

新版 SCC 於多處有要件或規範密度不如 GDPR 之情形，已如前述，而新版 SCC 第 4 條是否欲作為類似「本標準契約條款所未規範之事項，準用 GDPR 規定」的準用條款？如果答案係肯定，則有望可稍加解決新版 SCC 條文規範密度不足之問題，惟問題在於，「假如」新版 SCC 第 4 條設立之初之目的係為作為避免掛一漏萬之準用條款，則本條規範之意旨是否未能清楚呈現？蓋若以本條之文字觀之，僅規範本 SCC 中之條款應以 GDPR 規定相一致之原則進行解釋，並不當然代表具有「本標準契約條款所未規範之事項，準用 GDPR 規定」之意思，亦可能僅係單純表達此份 SCC 之名詞用語或原則之解釋上，不得與 GDPR 相衝突

[228] Schrems II para. 191.
[229] 2021 SCC Annex §4.

而言，若欲將其作為準用條款使用，立法者可能須以更明確之文字用語，以表明其作為準用條款之功能。本文認為，若單以現行新版 SCC 之條款進行解釋，應尚無法過度擴張其文字之解釋範圍，不宜將之逕行認定作為準用條款使用。

第二項 模組四極低規範密度之妥適性

綜觀整份 2021 新版 SCC 之條文，模組一在規範要件及密度上均屬最高者，而模組二及模組三大部分相差不大、均屬次之的等級，模組四之規範密度則明顯低於其他三個模組非常多，模組四許多條款之規範，不論在條文長度、要件種類、或規範密度上均十分精簡，甚至到了有所不足之程度，以資料處理之六大原則而言，模組四僅在資料完整性與保密性原則有所規範，其他五大原則均於模組四中未見任何規範；關於資料主體之權利，模組四完全無作成任何規範；甚至於新版 SCC 第 13 條關於監管之規定，即決定監管機關為何人及將資料輸入方作為與監管機關進行溝通之主要義務人，新版 SCC 之制定者亦刻意將模組四排除。

或許新版 SCC 之制定者係認為，模組四之傳輸樣態係處理者將其已處理好之資料回傳給位於歐盟境外之管控者，其處理行為已進行完畢且傳輸之路徑較為單純，惟如此精簡之規範方式，連資料處理六大原則中之五項都將之排除，莫非處理者將資料傳回給管控者之過程中，或若尚需進行一定之處理或作業時，完全無庸符合資料處理之其他五大原則？另一方面，若資料主體欲本於 GDPR 賦予其之權利，向資料管控者行使權利，於模組四之傳輸樣態則無法為之，如此規範是否合理，亦不無疑問。更有甚者為，關於監管之規範，雖新版 SCC 僅係擇定監管機關，為何以特意排除模組四在外，亦使人不解。新版 SCC 制定之初，立法者或許有意考量依不同之傳輸樣態，可適度調整或減輕規範之密度，惟本文認為，至少於最基本之資料處理六大原則及監管部分，應維持四個模組一致之規範強度，蓋此些部分不應依傳輸之樣態不同而有所差異，應形成對資料主體相一致之保障強度，始符合 GDPR 之精神，及歐盟法院於過往 Schrems I、II 案中對於

GDPR 及歐盟基本權利憲章中對歐盟公民隱私權及各項自由、權利之最基本保障之解釋方向。

第五章 結論

回顧前述內容，本篇論文首先介紹歐盟個資保護的規範架構、歐盟跨境傳輸之法制及現況，接著進入本篇論文欲探討之重點對象——SCC，透過將 2021 新版 SCC 與整部 GDPR 進行規範比較，再進一步討論 2021 新版 SCC 於 GDPR 下之合法性，而經過比對分析後，本文整理出若干新版 SCC 於規範上與 GDPR 之保護水準有所落差之地方，諸如新版 SCC 第 15 條可能違反 GDPR 透明性原則及資料主體知情權之內容；更重要的是新版 SCC 並未正確回應到 Schrems II 案中歐盟法院的擔憂，蓋縱使新版 SCC 增加第 14 條、第 15 條之新設義務，仍然無法解決美國政府得透過相關之情報法令，不受司法控制地對歐盟公民實施監控，侵害歐盟公民之隱私權及自由。關於資料主體之權利，在多項權利中新版 SCC 之規範密度明顯不如 GDPR，甚至有部分權利如限制使用權及資料可攜權在新版 SCC 中付之闕如。關於管控者／處理者義務之部分，亦有部分 GDPR 規範之義務如關於設計階段及預設的個資保護、資料影響評估與事前諮商義務在新版 SCC 中未被明文。關於救濟之部分，新版 SCC 於第 15 條規定當資料輸入方收到第三國政府機關之請求，或得知第三國政府機關已存取資料主體之個人資料時，條文僅規定「資料輸入方應盡力尋求救濟或上訴之途徑」，如此將資料主體之救濟權僅繫諸於資料輸入方之積極作為與否，恐並不符合歐盟法院對於歐盟基本權利憲章第 47 條訴訟權保障程度之見解。

針對 2021 新版 SCC 增加第 14 條、第 15 條新義務，以試圖回應 Schrems II 案之部分，該新增義務並無正確回應歐盟法院之擔憂，已如前述。而從另一角度觀察，本文亦質疑歐盟執委會如此立法，是否係企圖將國家監控之問題由私人企業去進行承擔？蓋依照新版 SCC 第 14 條、第 15 條之內容，企業不僅需花費大量之法遵、人力成本，不斷更新、評估第三國之國內法規及實務作法，更須於第三國政府疑似違法要求提供資料主體個人資料時，挺身對抗第三國政府，為資料

主體盡力尋求救濟，對於 Meta、Google 如此巨型企業尚有達成之希望，惟美歐間亦存在眾多之中小企業有進行資料跨境傳輸之實際需求，其是否有如此龐大之能力及資源，得對抗美國政府，答案不言可喻。因 SCC 本身性質上之先天限制，即私人間之契約難以根本地限制第三國國家政府監控行為，實際上確實難以期待私人企業獨自對抗第三國政府之國家監控行為，就現階段而言，私人企業能著力改變之處確實較為有限，歐盟法院一再堅持美國政府國家情報機關監控歐盟公民之行為會損及歐盟公民基於歐盟基本權利憲章第 7 條、第 8 條、第 47 條之權利，實際上若美國不進行相關之國內情報法規修法，不論是往後第幾版之資料傳輸協定，抑或是 SCC，都很可能會被歐盟法院認為是換湯不換藥之政策而再次判決違法。

總結而言，本文認為新版 SCC 在多處均有規範情形不如 GDPR 之情形，又現行新版 SCC 第 4 條並無法直接逕行作為 GDPR 之準用條款使用，再加上新版 SCC 雖係在 Schrems II 案後所生，惟其並未解決或正確回應歐盟法院於 Schrems II 案中提出之第三國國家政府機關監控行為之疑慮，歐美間企業之跨境資料傳輸，除了藉由日前通過之歐美第三版傳輸協定 DPF 外（可能即將受到歐盟法院之判決檢驗）[230]，若欲使用 SCC 作為跨境傳輸之例外合法事由，綜合 Schrems II 案[231]、愛爾蘭資料保護委員會對 Meta 12 億歐元裁罰案件[232]及 EDPB 於 2021 年發布之建議內容[233]，本文認為，企業除了將資料主體之個人資料盡可能以最新技術進行加密、匿名化處理之外，或可考慮在契約中加入「金絲雀安全聲明」條款，不僅可使資料主體於一定之期間內就得知自己之資料可能已遭他人存取，亦不至於與 GDPR 或新版 SCC 之內容相衝突，或許可作為搭配 SCC 之補充性措施，以適度解決上述案件中歐盟法院及 EDPB 之擔憂。

[230] DPF, *supra* note 74.
[231] Schrems II, *supra* note 2.
[232] Meta 2023 case, *supra* note 176.
[233] EDPB, *supra* note 72.

除此之外，並將上述 2021 SCC 較 GDPR 及歐盟基本權利憲章不足之部分，以附件方式新增加入自身之契約條款之中，即雖是以 2021 SCC 作為基礎制定契約，惟將保障之密度自主性地提高至與 GDPR 及歐盟基本權利憲章相一致之水準，以避免若後續 2021 SCC 之合法性被 Schrems 等人質疑而無法通過歐盟法院之審查時，契約於跨境傳輸之合致性將再次陷入違法之疑慮。

參考資料

一、中文文獻

（一）專書

張陳弘、莊植寧，新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，2 版（2022 年）。

（二）期刊論文

郭戎晉，論資料在地化之立法，臺灣科技法學叢刊，第 3 期（2020 年）。

郭戎晉，論區塊鏈技術與歐盟一般資料保護規則之衝突，臺大法學論叢，50 卷 1 期（2021 年）。

郭戎晉，論個人資料跨境傳輸與數位經貿之互動與規範設計—以歐盟法院 Schrems 案影響為觀察對象，收於：王震宇編，2021 數位貿易政策論壇－科技．人文．數位貿易（2021 年）。

陳靜怡，隱私權新觀點：走過不留下痕跡？淺談被遺忘權與大數據，NCC NEWS，8 卷 11 期（2014 年）。

薛景文，從 Schrems I & II 論美歐隱私權保障落差對於自由貿易規範之影響，第 21 屆國立政治大學國際經貿法學學術發展研討會論文集（2021 年）。

（三）碩博士論文

董芃旻，台灣跨境資料傳輸——聚焦以契約方式作為隱私保障工具，國立政治大學法律學系碩士學位論文（2022 年）。

二、英文文獻

（一）專書

GREGOR DORFLEITNER & LARS HORNUF, FINTECH AND DATA PRIVACY IN GERMANY (2019).

（二）期刊論文

Anupam Chander, *Is Data Localization a Solution for Schrems II*, 23(3) Journal of International Economic Law (2020).

Flora Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 HARV. J. L. & TECH. (2020).

Julian Schütte & Gerd Stefan Brost, LUCON: Data Flow Control for Message-Based IoT Systems, 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering, Institute of Electrical and Electronics Engineers (Aug., 2018).

Marcelo Corrales Compagnucci et al., *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, 2021(2) NORDIC JOURNAL OF EUROPEAN LAW (2020).

Sergi Batlle and Arnaud van Waeyenberge, *EU–US Data Privacy Framework: A First Legal Assessment*, EUROPEAN JOURNAL OF RISK REGULATION (2023).

Stephen Breen et al., *GDPR: Is your consent valid*, 37(1) BUSINESS INFORMATION REVIEW (2020).

（三）碩博士論文

En-Naoui Wissame, Transfer of personal data to third countries and the complexity of Clause 14 of the Standard Contractual Clauses at. 47 (Dec. 1, 2022) (on file with the Faculty of Law, University of Oslo).

（四）歐盟法院判決

Case C-131/12, Google Spain v. AEPD and Mario Costeja González (May 13, 2014).

Case C-307/22, FT v. DW (Oct. 26, 2023).

Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems.

Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (Oct. 6, 2015).

Court of Justice, Application (OJ) of 16 Feb, 2024, case T-8/24, Meta Platforms Ireland v European Data Protection Board.

（五）政府單位或國際組織文件

2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council 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, 2000 O.J. (L 215).

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, 2001 O.J. (L 181) 19.

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 transfer of personal data to third countries, 2004 O.J. (L 385) 74.

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, 2010 O.J. (L 39) 5.

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, as last Revised and Adopted on 11 April 2018, https://ec.europa.eu/newsroom/article29/items/622227.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207).

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31.

Commission Implementing Decision (EU) of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework, 2023 O.J.

(L 231) 118.

Casalini, F. and J. López González, Trade and Cross- Border Data Flows, 220 OECD TRADE POLICY PAPERS 10 (2019).

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, Adopted on 12 Nov. 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

European Data Protection Board, Guidelines 01/2022 on data subject rights - Right of access, version 1.0, Adopted on 18 January 2022, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

Executive Order (EO) 14086 of 7 October 2022, on Enhancing Safeguards for United States Signals Intelligence Activities.

In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited) Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation Further to an own-volition inquiry under Section 110 of the Data

Protection Act 2018, Data Protection Commission Ireland (Adopted on May 12, 2023).

Presidential Policy Directive 28 – Signals Intelligence Activities, 17 January 2004.

Sofija Voronova and Anna Nichols, *Understanding EU Data Protection Policy*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE (May, 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf

（六）網路資料

About Us, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/about/about-us_en; *Frequently Asked Questions*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/frequently-asked-questions_en (last visited Jan. 18, 2024).

Davinia Brennan et al., *EU-US Data Transfers Back in the Spotlight Following Record €1.2bn Fine*, MATHESON LLP (May 24, 2023), https://www.matheson.com/insights/detail/eu-us-data-transfers-back-in-the-spotlight-following-record-1.2bn-fine.

Davinia Brennan, WhatsApp decision considers scope of transparency obligations under the GDPR, A&L GOODBODY LLP (Sep. 24, 2021), https://www.techlaw.ie/2021/09/articles/data-protection/whatsapp-decision-considers-scope-of-transparency-obligations-under-the-gdpr/.

European Commission, *Adequacy decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#high-level-meeting-on-international-data-

flows (last visited Jan. 18, 2024).

European Commission, *New Standard Contractual Clauses - Questions and Answers Overview*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (last visited Jan. 24, 2024).

NOYB, *European Commission Gives EU-US Data Transfers Third Round at CJEU* (July 10, 2023) https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

Nick Clegg and Jennifer Newstead, *Our Response to the Decision on Facebook's EU-US Data Transfers*, META (May 22, 2023), https://about.fb.com/news/2023/05/our-response-to-the-decision-on-facebooks-eu-us-data-transfers/.

Nicole Beranek, *SCCs and CoCs and BCR – Untangling the Web and Spotting the Difference*, INPLP (Nov. 26, 2021), https://inplp.com/latest-news/article/sccs-and-cocs-and-bcr-untangling-the-web-and-spotting-the-difference/.

Tasks and Duties, EUROPEAN DATA PROTECTION BOARD, https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en (last visited Jan. 18, 2024).