中國大陸「數據出境安全評估辦法」施行對資料跨境傳輸之影響

文/王德瀛
資策會科技法律研究所專案經理

一、中國大陸資料跨境傳輸相關規定綜覽

中國大陸對於資料傳輸到境外的規範，主要由2021年11月1日施行的《個人信息保護法》、2021年9月1日施行的《數據安全法》以及2017年6月1日施行的《網絡安全法》等三部法律及相關的辦法或行政立法所構成。

與臺灣《個人資料保護法》對個資跨境傳輸採取「原則許可、例外限制」的規範模式不同，中國大陸對於資料跨境傳輸的態度明顯採取較為保守的立場。根據《個人信息保護法》的規定，「個人信息處理者」須具備以下條件之一，才可將資料跨境傳輸：取得國家認可的個人信息保護認證、依據國家制定的標準契約與境外接收方訂定契約（內容須包含雙方權利義務）、其他法律、行政法規或國家網信部門規定的條件，至於「關鍵信息基礎設施運營者」及「處理個資達到規定數量」的個人信息處理者，則原則上應將於境內營運所蒐集、產生的個資於境內儲存，僅於僅於業務確有需要時，才可在通過國家網信部門「安全評估」的狀況下，向境外傳輸個人[1]。而對於「關鍵信息基礎設施運營者」的境外傳輸規定，也可於《網絡安全法》找到相同的規範[2]。

《數據安全法》則主要規範對「重要數據」的管理，其要求於境內蒐集、產生「重要數據」的數據處理者，也只能在政府訂定的出境安全管理辦法的許可下向境外傳輸資料[3]。特別要注意的是，《數據安全法》所規範的不只是「個人」資料。該法所指之「數據」，包含個人及非個人之資料[4]。

本次，中國「國家互聯網信息辦公室」於2022年7月公布、9月1日施行的《數據出境安全評估辦法》即是針對上述三法規定中，對於「關鍵信息基礎設施運營者」、「處理個資達到規定數量」的個人信息處理者以及蒐集、產生「重要數據」的數據處理者等三個類別的資料處理者在資料跨境時所需完成的「安全評估」程序、要求等，所為之規定。以下，簡介此一辦法之規定，並分析其中可能尚待釐清的項目，最後則就其可能對企業造成之影響提出初步分析。

二、辦法下的安全評估程序

根據《數據出境安全評估辦法》規定，該辦法適用的數據處理者再將資料資出境前，應先完成「數據出境風險自評估」[5]。將該自評估之結果及相關資料，經由省級網信部門報送國家網信部門進行「數據出境安全評估」[6]，在通過數據出境安全評估後，才可進行資料出境。

(一) 資料出境之定義

究竟哪種資料處理的行為會構成辦法所稱的「數據（資料）出境」？無論是《個人資料保護法》等法律，或是辦法本身，其實都沒有明確的定義。不過中國國家互聯網信息辦公室指出，只要是在境內營運中所蒐集、產生的資料，無論是將其傳輸、儲存到境外，或是雖然除存在境內，但境外的組織或個人可以訪問或調用（意即境外的組織或個人可以近用該資料）者，都屬於「資料出境」的情形[7]。

(二) 適用對象

根據辦法的規定，以下4種「數據處理者」應依此一辦法的規定，透過省級網信部門向國家網信部門申報安全評估[8]：

第一，向境外提供重要數據的數據處理者。此一規定源於《數據安全法》對於重要數據之數據處理者資料出境之規定。

第二，關鍵信息基礎設施運營者。此項規定係依據《個人信息保護法》及《網絡安全法》規定而來。

第三，處理100萬人以上個資或自上年1月1日起累計向境外提供10萬人個資或1萬人以上敏感性個資。這個規定主要是把《個人信息保護法》規定的「處理個資達到規定數量之處理者」要件的內涵做更明確的規定。

第四，其他國家網信部門規定須申報安全評估之情形。

針對這四項要件，最值得討論的是第三要件的內容。首先，此處所指的是涉及的當事人數量，而非臺灣各主管機關制定之個資法子法中所常用以衡量風險高低的「資料筆數」[9]。此外，中國大陸的「敏感性」個資概念與我國個資法的特種個資概念不同。我國個資法的特種個資包含病歷、醫療（須由醫師或其他醫事人員做成）、基因、性生活、健康檢查及犯罪前科等幾種。中國大陸的敏感性個資，則採取例示的方法，將所有若洩漏或非法使用，容易導致其人格尊嚴侵害、人身或財產安全危害的個資都列為敏感性個資，其內容至少包含：生物識別資料、宗教信仰資料、特定身份資料、醫療保健資料、金融帳戶資料、行蹤軌跡資料以及未滿14歲者之個資[10]。最後，須注意的是雖然10萬人及1萬人的規定，是採取有限時間的方式（僅計算當年度及前一年度之累計），但其計算的標準是將所有提供境外的資料合併計算，若組織同時向多個境外單位提供個資，仍須整體觀察其所提供資料之累計是否超過標準。

(三) 數據出境風險自評估

根據辦法的要求，數據處理者在提出出境安全評估申報前，要先完成「數據風險自評估」。其內容應包含以下項目[11]：

- 目的、範圍及方法之合法、正當及必要：無論是資料出境此一行為本身，或境外接收方處理資料之目的、範圍、方法都須納入評估。
- 出境資料對國家安全、公共利益、個人或組織之合法權益造成的風險：須考量出境資料的規模、範圍、種類及敏感性。
- 境外接收方保護出境資料安全之能力：包含其承諾將擔負的責任義務，以及其為履行該責任義務所採取的管理及技術措施、能力是

否足以保障出境資料之安全；

●資料遭到竄改、破壞、洩漏、遺失、轉移或遭非法取得、利用之風險及其個資權益維護管道之通暢：此一風險須同時考量資料出境中及出境後可能產生之風險。

●與境外接收方之間簽訂的契約或法律文件是否涵蓋對資料安全保護之責任義務。（以契約或其他具法律效力之文件等形式做成）

其他可能影響資料出境安全之事項。

●上述的契約或其他法律文件，其內容應包含[12]：

●資料出境及境外接收方處理資料之目的、方式以及涉及之資料範圍；

●資料在境外保存之地點、期限，以及期限屆至、完成約定目的或契約中止後之資料處理措施；

●境外接收方將資料再移轉之相關規定；

●若境外接收方的實際控制權、經營範圍產生變化，或所在地資料安全保護政策、法規、網路安全環境等產生變化及其他不可抗力因素導致資料安全難以獲得保護時，所應採取的安全措施；

●違反約定之保護義務時的補救措施、違約責任及紛爭解決機制；

●出境之資料遭竄改、破壞、洩漏、遺失、轉移或遭非法取得、利用時之要求展開緊急應變及保護個人維護其個資權益的途徑及方式。

須特別注意的是，根據中國大陸《數據安全法》之規定，上述多處提及之「資料安全」的內函，不只是對當事人的權利保護，尚包含對「國家安全、公共利益」之衡量，足見中國大陸對於資料出境之考量，不只考量權利之保護，還有國家利益之考量。

(四) 數據出境安全評估

於完成上述「自評估」後，數據處理者應將此一自評估報告，與申報書、其與境外接收方之間擬簽訂的法律文件及完成安全評估所需要的其他資料，提交給省級網信部門[13]。省級網信部門應於5工作日完成資料完備性查驗；若資料完備則應報送國家網信部門、不完備時則應退回數據處理者並一次性告知須補充之內容[14]。國家網信部門在收到申報後7個工作日內，應書面通知是否受理，並視情況邀集相關部門、省級網信部門、專門機構等共同進行安全評估，並於通知受理後45日個工作日內完成安全評估並書面通知數據處理者[15]。審查中得要求數據處理者補充、更正，也可延長審查期限（但須告知預計延長之時間）[16]。對於評估結果有異議者，可於收到評估後15個工作日內申請複評，但複評結果即為最終結果[17]。

出境安全評估除針對「自評估」的內容（包含資料出境之目的、範圍、方式；出境資料對國家安全、公共利益、個人或組織之合法權益造成的風險；出境資料之安全、個資權益之保護；雙方簽訂之法律文件是否符合要求等等事項）進行評估外，尚要求對以下事項進行評估[18]：

●境外接收方所在地之資料安全保護政策、法規、網路安全環境等對出境資料安全之影響。

●境外接收方資料保護水準是否與中國大陸法律、行政法規或強制性國家標準相符。

●遵守中國大陸法律、行政法規及部門規章的情況。

●其他認為應評估之事項。

由上述內容可以看出，中國大陸在進行「安全評估」時，除針對資料出境本身是否受到足夠保護進行評估外，亦將過往的法律遵循結果（依條文內容不限於個資保護相關規範）等納入作為是否核准其出境評估的考慮項目。同時也考慮傳輸目的地國家的規範及實際執行對資料「安全」的影響。

(五) 完成評估後之效果及後續事項

通過「數據出境安全評估」後，即可執行資料出境。此一「數據出境安全評估」效期2年，處理者應於有效期限屆滿60個工作日之前重新申請評估[19]。而若出現有影響出境資料安全的情形則應申請重新評估；辦法所列之情形包含[20]：

●提供資料的目的、方式、範圍、種類改變，致影響資料安全。

●境外接收方處理資料的用途、方式改變，致影響資料安全。

●延長個資、重要資料境外保存期限。

●境外接收方的實際控制權、經營範圍產生變化，或所在地資料安全保護政策、法規、網路安全環境等產生變化及其他不可抗力因素導致資料安全難以獲得保護時。

●雙方法律文件變更。

●其他影響出境資料安全的情形。

三、辦法中尚待釐清事項

此一辦法雖然已經正式施行，惟其中對於適用範圍的部份仍有許多未臻清晰之處。有待後續實際執行後，由中國大陸的行政部門逐漸補充其實質內容。

■「數據處理者」的定義

「數據處理者」之用詞，於辦法及上述三部法律中，皆未有明確的定義。這些規範中，僅有規範「個人資料」的《個人信息保護法》，針對「個人信息處理者」進行定義。根據該法定義，「個人信息處理者」是指在個資處理活動中「自主決定」處理目的、方法的組織及個人，並未包含受託處理個資者[21]。然而在《數據安全法》及《網絡安全法》中，並未因是否「自主決定」而區分規範對象。因此，本辦法中所稱的「數據處理者」，究竟是否僅限於「自主決定」資料處理的組織、個人，其實仍存疑問。

■「重要數據」的範圍

「重要數據」為《數據安全法》下之概念。據該法規定，中國大陸將建立「數據分類分級保護制度」，由國家數據安全工作協調機制協調相關部門制定「重要數據目錄」；並由各地區、部門按照此一保護制度，建立該地區、部門、行業、領域的重要數據目錄[22]。然而迄今，中國大陸僅少數領域（如汽車業）完成「重要數據」範圍的指定，對於其他領域之「重要數據」範圍目前仍未臻明朗[23]。

■「關鍵信息基礎設施運營者」的範圍

「關鍵信息基礎設施運營者」為《網絡安全法》所定義的管制對象。根據《網絡安全法》的子法《關鍵信息基礎設施安全保護條例》的規定，「關鍵信息基礎設施」包含公共通訊、資訊服務、能源、交通、水利、金融、公共服務、電子政務、國防科技工業及「其他一旦遭到破獲、喪失功能或資料洩漏，可能嚴重危害國家安全、國計民生、公共利益」的重要網路設施、訊息系統等[24]。並須由涉及的主管部門、監督管理部門制定「關鍵信息基礎設施認定規則」，以認定「關鍵基礎設施」[25]。然而，由於該保護條例方於2021年9月1日施行，相關配套仍未完成，對於評估辦法的適用範圍，仍有待後續釐清。

四、企業應注意之影響

本辦法施行後，若屬於本辦法適用範圍，企業再將資料移轉或提供境外近用前， 應先按照辦法的規定申報「數據出境安全評估」。此一辦法的施行，企業應注意以下幾個面向的影響。

首先，如上所述，辦法在適用範圍上，仍有許多規範並不明確。若不確定自己是否適用本辦法規定，或於資料出境前，先向主管單位洽詢。同時，此一辦法的管制對象，除了個人資料外，尚包含「重要數據」，且無論是自我評估或政府機關之評估對象，都包含對「資料安全」的評估。

根據《數據安全法》對資料安全的規定，其考量的不只是個資權利的保護，還包含資料對於國家安全、國計民生等不同面向的考量。國際產業競爭日熾、資料科學發展迅速的今日，「資料」作為一種競爭的關鍵資源，其跨境流動的本身就可能被認為對於產業發展等「國計民生」甚至是「國家安全」造成影響。而此一辦法對於「安全」的概念，也不僅止於對於個人權利的保護，更往往將國家利益的項目納入評估。因此，在此一辦法的規範下，應注意是否會出現「事實上」（de　facto）對於資料在地化的要求。也就是雖然法律上並無「明文規定」資料不得出境，但實際上由於對於「資料安全」的評估，造成資料無法合法跨境傳輸的結果。企業對於涉及資料相關業務的產業活動，須評估若無法通過出境評估對於自身經營可能之影響。

第三，企業還應注意業務範圍內是否仍受到除前述提及的三法及「數據出境安全評估辦法」外的其他規範之管制。舉例而言，中國國家衛生計生委在2014年5月發布《人口健康信息管理辦法（試行）》，就規定要求醫療服務機構所產生的人口基本訊息、醫療衛生服務訊息的「人口健康訊息」僅能於境內儲存，不得儲存餘境外伺服器內，也不可以託管、租賃在境外的伺服器[26]。

最後，企業應該注意目前已經進行的資料出境行為是否受到本辦法的管理。若應受本辦法管理，則應於2023年3月1日前依辦法規定完成評估程序。

[1] 中國大陸《個人信息保護法》第38條、第40條。
[2] 中國大陸《網絡安全法》第37條。
[3] 中國大陸《數據安全法》第31條。
[4]　根據中國大陸《數據安全法》第3條第1項之規定，「數據」是指任何以電子或其他方式對訊息的紀錄。依照此一定義，其「數據」包含之範圍，並不限於個人資料。
[5] 中國大陸《數據出境安全評估辦法》第5條。
[6] 中國大陸《數據出境安全評估辦法》第4條。
[7]〈《資料出境安全評估辦法》答記者問〉，中華人民共和國國家互聯網信息辦公室，
http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm（最後瀏覽日：2022/11/14）。
[8] 中國大陸《數據出境安全評估辦法》第4條。
[9]　單一當事人可能對應到不同資料筆數。請參考：製造業及技術服務業個人資料檔案安全維護管理辦法第2條、內政部指定合作及人民團體類非公務機關個人資料檔案安全維護管理辦法第4條。
[10] 中國大陸《個人信息保護法》第28條。
[11] 中國大陸《數據出境安全評估辦法》第5條。
[12] 中國大陸《數據出境安全評估辦法》第9條。
[13] 中國大陸《數據出境安全評估辦法》第6條。
[14] 中國大陸《數據出境安全評估辦法》第7條。
[15] 中國大陸《數據出境安全評估辦法》第10條、第12條。
[16] 中國大陸《數據出境安全評估辦法》第11條、第12條。
[17] 中國大陸《數據出境安全評估辦法》第13條。
[18] 中國大陸《數據出境安全評估辦法》第8條。
[19] 中國大陸《數據出境安全評估辦法》第14條。
[20] 同前註。
[21] 中國大陸《個人信息保護法》第73條。

[22] 中國大陸《數據安全法》第21條。
[23] 證券與法律，〈一文全解《資料出境安全評估辦法》〉，網易，2022/7/11，https://www.163.com/dy/article/HC0P2TQ70519PQRV.html（最後瀏覽日：2022/11/15）。
[24] 中國大陸《關鍵信息基礎設施安全保護條例》第2條。
[25] 中國大陸《關鍵信息基礎設施安全保護條例》第8條、第10條。
[26] 中國大陸《人口健康信息管理辦法（試行）》第3條、第10條。

本文獲授權轉載自海基會《兩岸經貿網》

上稿時間：2022年11月30日

新聞來源：https://www.seftb.org/cp-4-1820-614ed-1.html

文章標籤

Copyright © 2016 STLI,III. All Rights Reserved.