國際商務仲裁中非實體聽證之資訊安全保護

摘要：

新冠肺炎疫情之流行使國際商務仲裁程序不得不考慮以非實體方式進行聽證，過程中必然涉及個人資料之處理使用與跨境移轉、網路安全等等之考量。本文參考歐盟 GDPR 規定內容，討論程序參與者於非實體聽證程序中所需面對之責任、風險與困難，以及合法處理與移轉資料之要件。同時，本文也檢視各大仲裁機構規則與國際商務仲裁社群所提出之建議，探尋國際仲裁社群中可行之作法。最後，本文試圖針對非實體聽證下的資訊安全保護提出程序執行上建議，做為我國未來跨國仲裁上與國際接軌之參考。

Due to the Covid-19 epidemic, as the in-person hearing is limited, the international commercial arbitration community has to consider proceeding procedures in a non-physical manner, which will inevitably involve data processing, cross-border transfer of data and related data protection regulations. This article refers to the GDPR to discuss the responsibilities and obligations of all participants in the remote hearing procedures, the obstacles of using data during the remote hearing procedures, and how to process and transfer involved data legally. Next, this article reviews the rules of major arbitration institutions and guidelines made by the international commercial arbitration community to explore feasible practices in the international arbitration community. Finally, this article attempts to provide suggestions for how to improve data protection and avoid related concerns in remote hearings of arbitrations for the practitioners in Taiwan to consider.

關鍵詞：國際商務仲裁（International Commercial Arbitration）、非實體聽證（Remote Hearing）、資料保護（Data Protection）、GDPR

國際商務仲裁中非實體聽證之資訊安全保護

壹、前言

新冠肺炎 (COVID-19) 疫情正在以各種方式影響仲裁[1]，許多國家的防疫措施要求社交距離並禁止集會，更增籌劃上的不確定性與困難[2]，使許多案件之實體聽證程序被迫取消或重新安排，部分則以非實體方式舉行，考慮到聽證舉行之需求，非實體聽證（Virtual Hearing，也有以遠程聽證「Remote Hearing」稱之）即成為一種選擇，國際仲裁的大多數流程皆以非實體之方式完成，包括在程序初期和（或）中期舉行的案件管理會議（通常以電話或視訊而非實際會議進行），並通過平台共享文件資料，當事人與仲裁人溝通、提交文件、證據都可能電子化處理，藉由電子郵件以及視訊會議執行程序[3]。現行仲裁程序本身即有使用電子檔案、視訊會議和電子郵件，隨著使用增加，是否符合資料保護、網絡安全等等應受到重視[4]。國際商務仲裁下之非實體聽證必然涉及個人資料之處理使用與跨境移轉、網路安全等等之考量。

歐盟一般資料保護規則（General Data Protection Regulation，以下簡稱為「GDPR」）於二〇一八年生效實施，其廣泛之管轄內容與高額罰金連帶帶動各國與企業對個人資料保護的關注甚至修改相關規範，包括國際仲裁界[5]。除此之外各大機構諸如國際商事仲裁理事會（International Council for Commercial Arbitration，以下簡稱為「ICCA」）和國際律師協會（International Bar Association，以下簡稱為「IBA」）、紐約律師協會（New York City Bar Association，以下簡稱為「NYC Bar」）等對個人資料保護發布指引與建議，可見此議題日益受重視。本文將從 GDPR 出發，而後檢視、比較各大仲裁機構於疫情發生之後所採取之應對方式，做為我國未來跨國仲裁上與國際接軌之參考。

---

[1] Ben Knowles & Maurice Kenton, *Worldwide: COVID-19 Global: Arbitration And Court Impacts*, MONDAQ (21 May 2020), https://www.mondaq.com/uk/operational-impacts-and-strategy/938420/covid-19-global-arbitration-and-court-impacts.

[2] David Geoffrey Allan Bateson, *Virtual Arbitrations: The Impact of COVID-19*, 9(1) INDIAN J. OF ARB. L. 159, 159 (2020).

[3] Sami Kallel, *Online Arbitration*, 25(3) J. of Inter'l Arb. 345, 346 (2008).

[4] Hong-Lin Yu, "Business As Usual" During An Unprecedented Time—The Issues Of Data Protection And Cybersecurity In International Arbitration, 13(1) CONTEMP. ASIA ARB. J. 45, 50, 2020.

[5] Jacques de Werra, *Using Arbitration And ADR For Disputes About Personal and Non-Personal Data: What Lessons From Recent Developments In Europe?*, 30(2) AMERICAN REV. OF INT'L ARB. , 195, 195 (2019).

貳、GDPR 規範之之影響

一、適用範圍、定義與合法之資料處理前提

GDPR 並未針對國際仲裁程序有所著墨，僅一般性規範其領土和實質範圍內的資料控管者和處理者的處理行為[6]。GDPR 之實體適用規範於第 2 條第 1 項「本規則適用於全部或一部以自動化方式處理之個人資料，且適用於其他非自動化方式處理而構成檔案系統之一部分或旨在構成檔案系統之一部分的個人資料」[7]，為了確實保護自然人的個人資料使用較為廣泛之用詞：「個人資料」和「處理」，盡可能涵蓋所有類型的個人資料處理類型，諸如姓名、地址、電子郵件地址、身份證號碼、IP 等等[8]。是以在仲裁程序中實際參與訴訟者之電子郵件地址以及其他任何作為證據所提交文件中所提及之個人資料均極易落入適用範圍之內[9]，仲裁中當事各方、仲裁庭和仲裁機構之文件資料傳遞（書面資料或通過電子郵件、案件管理平台等電子方式進行的仲裁請求、回覆、進一步的書面陳述、程序命令、仲裁判斷等），以及仲裁機構儲存其所管理各項案件之資料均有落入 GDPR 規範範圍內的可能[10]。第 2 項第 2 條規範適用上之例外並未涵蓋國際商務仲裁，參照 GDPR 前言第 20 條「本規則之適用範圍雖包括但不限於法院及其他司法機關之活動」[11]，「其他司法機關」應解釋為包括具有紛爭解決功能之仲裁庭[12]。

GDPR之領土適用規範於第3條，其適用於控管者或處理者在歐盟境內之分支機構所為之個人資料處理，不問該處理是否發生於歐盟境內；非設立於歐盟境內之控管者或處理者對於歐盟境內資料主體提供商品或服務之個人資料處理

---

[6] Emily Hay, *The Invisible Arm of GDPR in International Treaty Arbitration: Can't We Make It Go Away?*, KLUWER ARB. BLOG (Aug. 29, 2019), *https://www.kluwerarbitration.com/document/kli-ka-austrian-yb-2020-004-n?q=Chapter%20I%3A%20The%20Arbitration%20Agreement%20and%20Arbitrability%2C%20Mission(Im)Possible%3A%20Where%20GDPR%20Meets%20Commerical%20Arbitration*.

[7] GDPR Art.2(1).

[8] EUROPEAN COMMISSION, *What is Personal Data?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (last visited Dec. 25, 2020).

[9] Gaurav Natarajan Ramani, *One size doesn't fit all: the General Data Protection Regulation vis-a`-vis international commercial arbitration,* ARB. INT'L 1, 5 (2020).

[10] Martin Zahariev, *The Arbitration Agreement and Arbitrability, Mission(Im)Possible: Where GDPR Meets Commerical Arbitration*, *in* 2020 AUSTRIAN Y.B. ON INT'L ARB. 3, 5 (Christian Klausegger et al. eds., 2020).

[11] GDPR Recital 20.

[12] Zahariev, *supra* note 10, at 9.

也有所適用。是以程序中參與者為歐盟境內之資料主體、在歐盟境內進行的仲裁程序、仲裁地在歐盟境內（例如指定之機構位於歐盟境內）等等，均應受 GDPR 規範，GDPR 前言第 23 條即言「為確保當事人受本規則所保護之權利不被侵奪，凡為歐盟境內之資料主體，雖由非設立於歐盟境內之控管者及處理者進行個人資料處理，惟其處理活動涉及為該等資料主體提供商品或服務者，不問是否涉及付款，本規則仍應予適用」[13]。現今技術之發展與使用，諸如電子郵件、視訊連線、雲端平台之使用等等使跨境服務提供愈發普及，第 3 條之適用範圍也逐步擴大。

簡言之，GDPR 並不排除國際仲裁[14]，無論其主要機構和執行地點在哪裡，仲裁程序參與者都應考慮其潛在適用性**[15]**。隨著網路、電子郵件和其他形式的電子跨境通信的普及，當事人、專家、機構和仲裁員在仲裁過程中審查的資料越來越龐大[16]，其中包含有「個人資料」，諸如姓名、位置資料、網路識別碼等內容即受有規範，當事人、仲裁人或律師如果處於歐盟境內，或其所提及之資料主體為歐盟公民也落入規範範圍中（須注意者為公司之註冊碼、匿名資料等等並不視為個人資料，蓋其核心重點為「識別或可得識別」）[17]。非實體聽證中證人線上之陳述通常包含其姓名、職務等個人資料，其所提交之聲明亦包含其背景簡歷與照片，專家亦同，內部文件（例如與證人，專家和客戶的會議記錄以及與案件有關的內部電子郵件通訊）也可能包含個人資料[18]，而非實體聽證過程之錄音錄影也應屬之，相較於實體聽證含有更強之跨境因素使其更易受到 GDPR 規範。

仲裁程序中諸如個人資料之保存、閱覽、相關資料移轉與第三方（證人、專家、翻譯人員等）等等均構成 GDPR 下對個人資料之「處理」，定義範圍廣

---

[13] Recital 23.

[14] Zahariev, *supra* note 10, at 8.

[15] *Id.* at 10.

[16] Kathleen Paisley, *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, 41(4) FORDHAM INT'L L. J. 841, 862 (2018).

[17] GDPR Art.4 (1); EUROPEAN COMMISSION, *What is personal data?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (last visited Dec, 25, 2020).

[18] MARILY PARALIKA & SONIA MORTON, *COVID-19 and data protection in international arbitration*, THE IMPACT LAWYERS (July 8, 2020), https://theimpactlawyers.com/articles/covid-19-and-data-protection-in-international-arbitration.

泛[19]。國際仲裁往往具有文件密集性[20]，其跨境特性更牽涉不同地域間之資料移動，此時管理資料應更為審慎[21]。資料處理過程中核心角色為主動之「控管者」與被動之「處理者」，前者係指單獨或與他人共同決定個人資料處理目的與方法之自然人或法人、公務機關或其他機構，後者為代前者處理個人資料之自然人或法人機構[22]，兩者區隔關鍵為「**決定**個人資料處理之**目的與方法**」，確定誰應負責遵守資料保護規則，以及資料主體如何行使權利[23]。仲裁程序參與者均有機會接觸大量文件資料，依其行為可能有不同身份之重疊，觀察條文內容可見控管者承擔更多責任，明確化各自義務有一定之重要性。

第 6 條規範資料處理之合法性要件[24]。資料主體之「同意」係指資料主體基於其意思，透過聲明或明確肯定之行動，所為自主性、具體、知情及明確之表示同意處理與其有關之個人資料[25]，僅在其對於接受或拒絕條件，或拒絕時免受損害而享有真正的選擇時，才可作為適當的合法基礎[26]。然而多數情況下，同意不是處理爭端解決中個人資料的可靠依據[27]。同意之給予應涵蓋基於相同之一個或多個目的所為之全部處理活動，如個人資料之處理具有多重目的者，應為全部目的取得同意[28]，如果資料主體同意出於多種目的進行處理，其同意可以解釋為對個別特定情形下的處理，或者在整個爭端解決的流程下都符合其同意之目的[29]，惟仲裁中所涉及之資料不一定於取得當時資料主體即明確知情其資料將應用於爭端解決而得為事先同意，在仲裁中可能難以預測將如何處理

[19] GDPR Art.4(2).
[20] Lukas Wyss and Liv Bahner, *The impact of the GDPR on arbitral proceedings – a gateway for new conflicts?*, BRATSCHI (Oct. 15, 2019), https://www.bratschi.ch/de/uebersicht/detail/bratschi-arbitration-blog-the-impact-of-the-gdpr-on-arbitral-proceedings-a-gateway-for-new-conflicts.html.
[21] Ananya Bajpai & Shambhavi Kala, *Data Protection, Cybersecurity and International Arbitration: Can They Reconcile?*, 8 Indian J. Arb. L. 1, 4 (2020).
[22] GDPR Art.4 (7)(8).
[23] Opinion 1/2010 on the Concepts of "Controller" and "Processor", at 4 (Article 29 Data Protection Working Party, 00264/10/EN WP 169, 2010).
[24] GDPR Art.6 (1).
[25] GDPR Art.4(11).
[26] Guidelines on consent under Regulation 2016/679 17/EN WP259rev.01, p.3
[27] Working Document on Pre-trial Discovery for Cross Border Civil Litigation, 00339/09/EN WP 158, 2009, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, 8-9.
[28] GDPR Recital 32
[29] Ramani, *supra* note 9, at 9.

個人資料，並且每次傳輸或處理均獲得特定的同意極為困難[30]，如若涉及主體數量龐雜則更不利程序有效進行。此外，資料主體有權隨時撤回其同意[31]，對於程序中是否可以使用資料帶來極大不確定性。即使當事方之間的仲裁協議包含資料處理與移轉條款也難以涵蓋過程中可能出現的所有情形。

為此，GDPR 仍提供其他於仲裁程序中授與處理資料合法性的選擇，而不仰賴資料主體之同意，例如處理係控管者或第三者為追求正當利益（legitimate interest）之目的所必須者[32]、處理係為履行資料主體為契約當事人之契約所必須者（尤其是資料主體同時為仲裁程序當事人時，基於仲裁程序多立基於當事人同意下進行）[33]以及處理係控管者為遵守法律義務所必須[34]。

主張正當利益涉及各項利益之權衡（資料主體之權利、利益以及爭端解決本身之利益），應考慮比例性、個人資料與爭端的相關性以及對資料主體所產生之影響，當該資料保護之資料主體其利益、基本權與自由優先於該爭端解決之利益時，則無法給予仲裁程序使用合法性[35]。有主張爭端解決所為之攻防，其本身的重要性並不優先於沒有直接參與爭端解決的資料主體的基本權利，蓋原本此法條於應用上預期由法院對各項權利與利益進行衡量，然而仲裁與法院之判決不同，為當事人間基於契約所定之爭段解決手段，並且資料主體難以對程序之進行發表意見，是以仲裁庭應不具有執行利益衡平並決定基本權利的必要權限或合法性[36]。

主張「處理係控管者為遵守法律義務所必須」者，資料處理係基於控管者為遵守其法定義務所為，該處理應具備歐盟或其會員國之法律上依據[37]，按工作組（Article 29 Working Party，為歐盟之獨立工作組，至二〇一八年五月均負責處理隱私保護與個人資料之議題[38]）之意見，除非歐盟或其會員國之法律要

[30] Bajpai & Kala, *supra* note 21, at 9 .
[31] GDPR Art.7(3).
[32] GDPR Art.6(f).
[33] GDPR Art.6(b).
[34] GDPR Art.6(c).
[35] Working Document on Pre-trial Discovery for Cross Border Civil Litigation, 00339/09/EN WP 158, 2009, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, 9-10.
[36] Ramani, *supra* note 9, at 10-11.
[37] GDPR Recital 45
[38] EUROPEAN DTA PROTECTION BOARD, Article 29 Working Party, EUROPEAN DTA PROTECTION BOARD, https://edpb.europa.eu/our-work-tools/article-29-working-party_en (last visited Jan. 3, 2021).

求遵守外國法院命令，否則外國法律所施加的義務將不屬於法律義務[39]，是以除非成員國法律要求遵守仲裁庭對於個人資料處理之裁定，否則該命令將不構成法律義務[40]。另有主張國際仲裁中遵守法律義務僅涵蓋歐盟或其會員國法律規定之義務，例如法院命令，而非由仲裁庭命令所產生的法律義務。儘管如此，仲裁程序中揭露義務仍滿足 GDPR「處理係控管者或第三者為追求正當利益之目的所必須者」[41]。

二、資料主體之權利與對程序之限制

GDPR 第三章規範資料主體之權限，第 12 條賦予資料主體為行使其權利之透明資訊、溝通及管道，個人資料之蒐集、利用、商議或其他處理應向當事人公開，且應及於該個人資料所處理或將處理之程度[42]；第 13 條「蒐集資料主體之個人資料時所提供之資訊」、第 14 條「尚未自資料主體取得個人資料時所應提供之資訊」、第 15 條「資料主體之接近使用權」，資料主體應有權接近使用其所受蒐集之個人資料，並得容易地、於合理之時間間隔行使接近使用權，以知悉並核實該處理之合法性[43]。仲裁優點之一為機密性，然則於資料主體非為程序參與者時，其行使上述權利可能使其得以知悉仲裁相關訊息而損及機密性利益，也可能損及當事人程序上之防禦，如果仲裁庭滿足資料主體之接近使用權更可能違反其保密義務[44]。此外於複雜之案件，上述權利之適用可能導致大量資料控管者被要求通知大量的資料主體[45]，成本將大幅增加。又，依第 16 條「更正權」、第 17 條「刪除權」，資料主體應有更正其個人資料以及刪除其個人資料之權利，並於該個人資料就資料蒐集或另為處理之目的已無必要時、於資料主體已撤回其同意或拒絕其個人資料之處理時，資料主體享有請求不再處

[39] Working Document on Pre-trial Discovery for Cross Border Civil Litigation, 00339/09/EN WP 158, 2009, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, 9.
[40] Ramani, *supra* note 9, at 10.
[41] Natalia M. Szlarb, *GDPR and International Arbitration at a Crossroads*, NAT'L L. REV. (Dec. 4, 2019), https://www.natlawreview.com/article/gdpr-and-international-arbitration-crossroads.
[42] GDPR Recital 23.
[43] GDPR Recital63.
[44] MARTIN ZAHARIEV, DATA PROTECTION IN COMMERCIAL ARBITRATION: IN LIGHT OF GDPR 145 (2019).
[45] Zahariev, *supra* note 10, at 907.

理其個人資料之權利[46]，上述權利之行使可能影響程序中資料之使用與保存，非實體聽證中各項資料可能儲存於雲端平台共享供所有參與者閱覽使用，甚或錄音錄影審理過程以防未來對審理程序有一步爭議，仲裁庭亦應注意當事人是否可能以此為由做為反對證據提交之藉口。而對於資料主體之刪除權，立法者明確肯認為建立、行使或防禦法律上請求所必要得限制之，是以仲裁程序應不受影響[47]。第 18 條之「限制處理權」更賦予資料主體對於資料處理之限制權限，將對證據使用增添不確定性，損及仲裁程序之效率。GDPR 對上述權利行使並非無所制約，諸如「法律義務之遵守、或為了建立、行使或防禦法律上主張有所必要時[48]」，得進一步合法保留資料，為建構、行使或防禦法律上之請求而有必要者，不問係於訴訟程序或行政程序或於法院以外之程序，該等個人資料處理禁止規定亦應允許例外[49]，然而對於「必要性之認定」仍有爭議，尚待觀察[50]。此外第 23 條亦明文對上述權利之行使有所限制，仲裁程序應屬「民事請求之執行」[51]，於此情形資料控管者或處理者所遵守的歐盟成員國法律可通過立法措施限制第 12 至 22 條之義務和權利的範圍，須注意第 23 條之適用並非指資料不受有 GDPR 之適用，僅其資料主體之部分權利受到限制[52]。

由此可見資料主體之權利行使對於仲裁程序有一定程度影響，且須回歸檢視個資料主體所適用之法律是否有近一步規範，不可謂不繁雜，於程序開始前先行檢視各項資料主體權利範圍應有利於避免違反規範，以及程序中個別程序參與者之責任界定。

三、仲裁程序中參與者之責任分配與豁免

仲裁程序中，GDPR 並非適用於程序本身，而是對個別程序參與者之行為有所規範[53]。如前所述，GDPR 將處理資料之人分類為「控管者」與「處理者」

[46] GDPR Recital 65.
[47] Zahariev, *supra* note 44, at 138.
[48] GDPR Recital 65.
[49] GDPR Recital 52.
[50] Zahariev, *supra* note 10, at 906.
[51] GDPR Art.23(1)(j).
[52] Zahariev , *supra* note 10, at 858.
[53] Ajar Rab, *Do Data Protection Laws Enhance The Role Of 'Venue' In Remote Arbitration Hearings?*, L. Sch. Pol'y Rev. (Sep. 17, 2020), https://lawschoolpolicyreview.com/2020/09/17/do-data-protection-laws-enhance-the-role-of-venue-in-remote-arbitration-hearings/.

並各自有不同程度之責任範圍，其中尤以控管者最為廣泛，諸如合法處理資料之依據僅控管者而無處理者（第 6 條）、控管者應證明資料主體已同意其個人資料之處理（第 7 條）、將處理資訊告知資料主體（第 12 至 14 條)、處理資料主體依其權利所為之請求（第 15 至 22 條）、規範處理者（雲端服務提供商、翻譯人員、會計師等，第 28 條）、實施適當措施以確保所處理的個人資料的安全（第 32 條）等等[54]。

仲裁機構與仲裁庭於仲裁程序中之角色應為控管者。有論者主張機構本身並不解決爭議，而是按照其規則管理仲裁員名單和組成仲裁庭[55]，然而考量到其所處理之業務，仍應認定仲裁機構為控管者[56]。仲裁庭則應回歸個別仲裁員進行認定，為履行其職責仲裁員需考量所有當事人所提交之資料、詢問當事人與證人，可以證明仲裁員處理各種不同的個人資料而做出仲裁判斷[57]，仲裁員有權限決定是否使用、如何使用資料[58]，不受當事人左右而獨立為之，應為控管者。於非實體聽證，其需決定如何使用在非實體聽證程序中所取得之資料，故有主張應在聽證會開始前即進行整體資料保護影響評估[59]。

當事人與律師應為控管者，蓋當事人決定含有個人資料之證據資料之使用，為建立、 行使或防禦法律上請求所為，應被認為控管者[60]。律師在法庭上代表其委託人處理案件有關之個人資料，決定證據於攻防上之使用，代表的過程中處理資料時應被視為獨立的控管者[61]，因其有權限決定如何處理並且其處理是為其自身目的（例如履行委任契約）[62]，GDPR 前言第 91 條也明確肯認律師之

---

[54] Martin Zahariev, *GDPR Issues in Commercial Arbitration and How to Mitigate Them*, Kluwer Arb. Blog (Sep. 7, 2019), http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/.

[55] Zahariev, *supra* note 10, at 11.

[56] Zahariev, *supra* note 54.

[57] Zahariev, *supra* note 44, at 61.

[58] *Id.* at 62.

[59] Andreas Respondek & Tasha Lim, *Should the ICCA / IBA's Task Force on Data Protection "Roadmap" address the impact of the GDPR on Video Conferencing in International Arbitration Proceedings?*, KLUWER ARB. BLOG (July 18, 2020), http://arbitrationblog.kluwerarbitration.com/2020/07/18/should-the-icca-ibas-task-force-on-data-protection-roadmap-address-the-impact-of-the-gdpr-on-video-conferencing-in-international-arbitration-proceedings/?doing_wp_cron=1595138143.5904738903045654296875.

[60] Zahariev, *supra* note 44, at 78.

[61] 'Opinion 1/2010 on the concepts of controller and processor' 00264/10/EN at 4 (16 February 2010)—2010 WP 169 28.

[62] Zahariev, *supra* note 44, at 81.

控管者角色[63]。專家依其專業獨立準備陳述並回答問題是為了履行其程序上功能，被當事人指定並不代表其為處理者而應為控管者[64]。非實體仲裁程序中更會牽涉其他人員，例如提供視訊會議之服務供應平台、第三方服務與設備、使用特定軟體，其軟體外部維護團隊（IT maintenance）、雲端服務提供商（cloud solution）、翻譯人員等等，均為處理者，蓋其對於資料之處理並無決定之權限，僅依照控管者之要求單純為處理工作[65]，惟於 GDPR 下仍有一定之責任義務。

四、網路安全之維護

處理應以確保個人資料適當安全性之方式為之[66]，仲裁優點之一為保密性，更應注重保密措施[67]。控管者及處理者應採取適當之科技化且經組織化的措施，確保對於風險應對上有達到妥適的安全層級[68]，此為 GDPR 明文課予仲裁程序參與者之義務。現今跨國仲裁中多數程序已然電子化進行，伴隨網路攻擊（例如駭客）風險日益增加，應確保於程序進行中採取適當安全與保密措施[69]。非實體仲裁中除卻一般電子化之文件資料傳遞，更需要線上共享文件並以視訊或電話方式進行審理，程序參與者分屬各地，可能於不同的地點連線參與（諸如於房間、旅館、工作室等等地方之網路參與）更增加資料洩漏之危險。於程序中，仲裁庭多具備有廣泛之程序指揮權限，可以對資料之使用提供定程度之保護，也滿足其作為控管者之義務。選擇非實體聽證所使用之平台時，仲裁庭也應確保達到適當之資料安全（諸如加密、處理系統及服務持續之機密性、完整性、可用性及彈性之能力）[70]，非實體聽證於線上進行之緣故，仲裁庭也應當確保非受允准之人無法進入平台接觸審理相關之內容，保護聽證的機密性[71]。非實體聽證對網絡安全和資料保護措施或許可以採取以下措施：使用需要驗證

[63] GDPR Recital 91.
[64] Zahariev, *supra* note 44, at 84-85.
[65] *Id*. at 156.
[66] GDPR Art.5(1)(f).
[67] Zahariev, *supra* note 44, at 177.
[68] GDPR Art.32(1).
[69] Vanessa Naish & Maguelonne de Brugiere, *Cybersecurity in Arbitral Proceedings: How to Kick-Start the Conversation about Protecting your Clients' Data*, KLUWER ARB. BLOG (Nov. 25, 2018), http://arbitrationblog.kluwerarbitration.com/2018/11/25/cybersecurity-in-arbitral-proceedings-how-to-kick-start-the-conversation-about-protecting-your-clients-data/.
[70] GDPR Art.32 (1).
[71] Respondek & Lim, *supra* note 59.

身份的視訊軟體、使用經加密之通訊方式等等[72]。無法確保在仲裁程序中所處理的、包涵個人資料之文件資訊之安全，對於任何仲裁機構或仲裁員而言亦將影響其聲譽[73]。

五、跨國移轉之限制

國際商務仲裁必然涉及跨境資料傳輸，諸如：位於歐盟之當事人指定第三國之機構，此機構必須接受必要資訊以開始程序；當事人之一方（或更多）位於第三國，此當事人之參與將可能要求移轉個人資料至其所在地；程序中個人資料到第三國（例如因為仲裁地或程序進行地位在第三國）等等[74]，而現今疫情下之非實體聽證亦多為「受限於防疫措施而無法出國（甚至也無法州間、邦間移動）實體審理」之情況服務，含有個人資料之文件、證據需傳遞至各參與者所在之位置甚或共享之雲端平台，而當案件愈發複雜，所涉及參與者與文件資料愈多，移轉之限制亦將更為龐雜。對含有個人資料之證據如果欠缺適當保護，可能導致當事人（或非當事方之資料主體）得對證據提交有所主張而阻礙程序進行[75]。

GDPR 嚴格規範跨境資料傳輸，第五章「個人資料移轉至第三國或國際組織」中得移轉者：移轉至充足保護之國家（基於充足程度保護決定之移轉 Transfers on the basis of an adequacy decision[76]）、控管者提供適當之保護[77]以及特定情形下之例外（Derogations for specific situations)[78]。如果個人資料得移轉至已取得歐盟認定確有充足程度之保護（adequacy）之第三國或國際組織，此時之移轉並無疑慮（已取得上述認證者：安道爾、阿根廷、加拿大（商業組織）、法羅群島、 根西島、以色列、曼島、日本、澤西島、紐西蘭、瑞士與烏拉圭）

[72] Diana Sulamazra Abdul Rahman, *The Role of Arbitral Institutions in Cybersecurity and Data Protection in International Arbitration*, KLUWER ARB. BLOG (Nov. 24, 2020), http://arbitrationblog.kluwerarbitration.com/2020/11/24/the-role-of-arbitral-institutions-in-cybersecurity-and-data-protection-in-international-arbitration/.
[73] Zahariev, *supra* note 10, at 15-7.
[74] Zahariev, *supra* note 44, at 205-06.
[75] Paralika & Morton, *supra* note 18.
[76] GDPR Art.45.
[77] GDPR Art.46 (2)(a-f), (3)(a-b).
[78] GDPR Art.49.

[79]，然而渠等認證之取得非仲裁機構、仲裁員與當事人得以左右，無法作為多數情況下理想之合法依據。當需要將資料移轉至不具有充足程度保護之國家時，控管者或處理者則應為資料主體採取適當保護措施，以彌補第三國對資料保護之欠缺[80]。欠缺充足程度保護之決定或適當保護措施時，仲裁得適用之最後例外為：「資料主體於受關於因欠缺充足程度保護決定及適當保護措施，該等移轉對資料主體造成之可能風險通知後，已明確同意計畫之移轉」、「移轉對履行資料主體與控管者間契約、或依資料主體之請求執行契約前之措施為必要」、「移轉對建構、行使或防禦法律上之請求為必要」等[81]。然而承前所述，於複雜案件中一一取得個資料主體之同意有執行上困難與成本考量，亦並非資料主體均與控管者存有契約關係，最可能使用者為法律上請求之必要，而何為「必要」，仍待法院或相關機構予以定義。

六、小結

GDPR 未直接處理任何與仲裁相關的問題[82]，導致適用上不確定性。非實體聽證之執行因其允准程序參與者以遠端方式進行程序，參與者分散各處與網路之大量使用、影音之錄製，致使其法規適用上更複雜，也可能出現當事人以相關責任為由，故意拒絕非實體審理的情況，而仲裁庭能否為了公平、高效的程序，以被質疑的仲裁判斷為代價，繼續進行審理[83]，需審慎考量。

控管者和處理者皆應確保採取適當的技術和措施來保護個人資料的處理。GDPR 第 32 條指出其所要求之安全規範：「考量現有技術、執行成本、處理之本質、範圍、脈絡及目的、對當事人權利及自由之風險變動之可能性、嚴重性，控管者及處理者應執行採取適當之科技化且有組織的措施以確保對於風險之適當安全程度」並提供數項措施作為參考，「於衡量適當之安全程度時，尤其應考量因處理而造成之風險」、「控管者及處理者應採取行動，確保任何受該取

[79] European Commission, Adequacy Decision, European Commission (lasted visited May 1, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[80] GDPR Recital 108.
[81] GDPR Art.49(1)(a)(b)(e).
[82] Agata Zwolankiewicz &Anushka Sachan, *Big Data, Bigger Disruption: Is Institutional Arbitration Ready?* , Arb. Bull. 14, 19 (Dec., 2020), https://ssrn.com/abstract=3759569.
[83] Rab, *supra* note 53.

得個人資料之控管者或處理者指揮之個人不得為指示外之處理」[84]，就處理活動可能造成當事人之權利或自由有高度風險之情形，控管者應負責執行資料保護影響評估，在決定適當措施時，評估結果應納入考量[85]，一旦控管者發現個人資料侵害已然發生，即應向監管機關通報[86]，控管者應與資料主體溝通個人資料之侵害，不得無故遲延[87]。

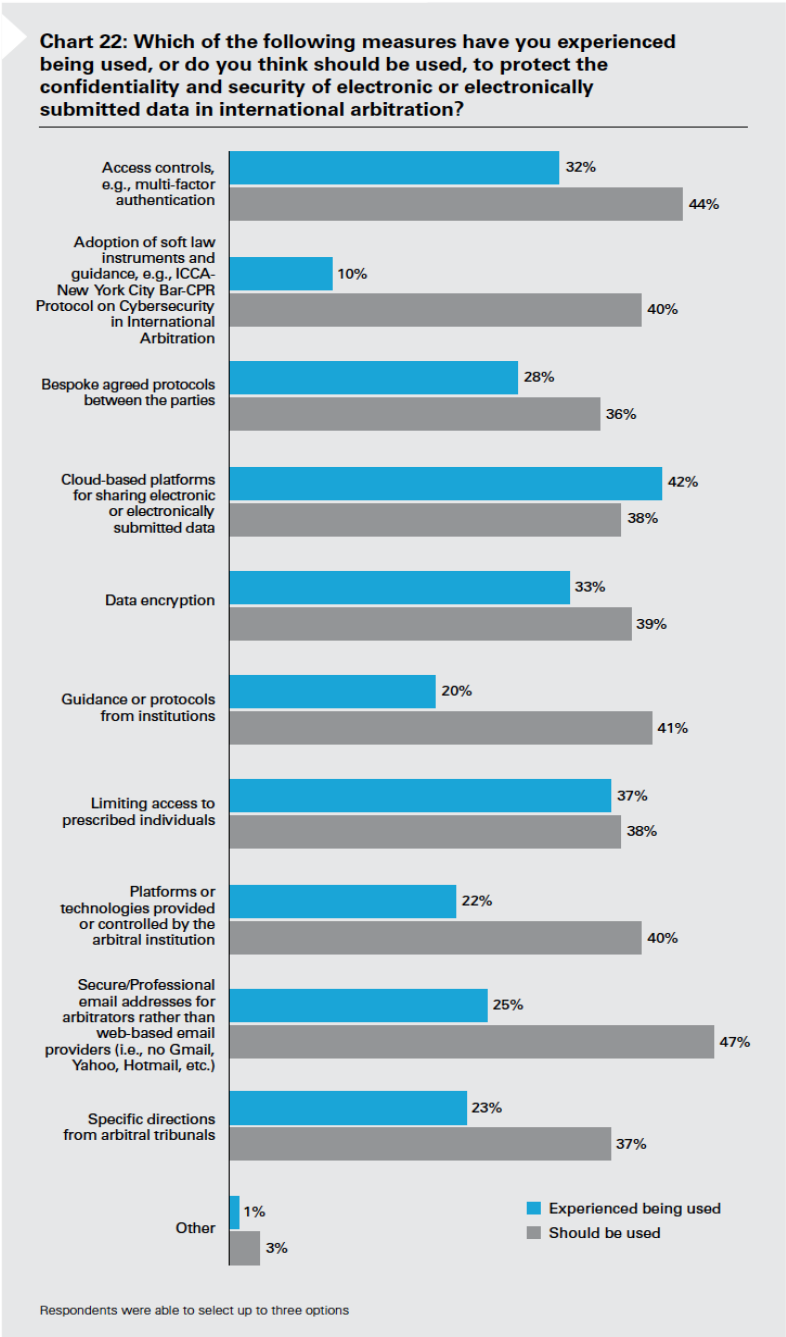
建議仲裁程序參與者於程序前階段、尚未進入聽證程序前之案件管理會議上，即針對網絡安全、資料保護與處理進行討論與分析[88]，使主要程序相關人員（仲裁員、當事人及其律師）對處理行為有重疊的情況下就最低限度的資料保護標準達成一致，例如簽訂資料保護協議[89]，對所涉權責加以界定分配並對所採取之措施達成共識，如果案件複雜所涉資料主體人數龐大，與專業之資料保護團隊先行諮詢或可避免誤踩規範之紅線。

參、各大仲裁機構與國際組織之應對與改革

根據二〇二一年倫敦大學瑪麗皇后學院的調查（2021 International Arbitration Survey: Adapting arbitration to a changing world By Queen Mary, University of London，該調查調查了仲裁使用者之偏好、觀念上的趨勢）[90]，其指出資料保護在國際仲裁上應用上的缺乏，過去三年近半仲裁未採取任何措施來保護電子資料或以電子方式所提交的資料的機密性和安全性，多數人並不理解現有資料保護法規、所涉問題以及解決這些問題所須採取的措施，即便資料保護法規的影響受到廣泛承認也難以定義影響為何以及其對仲裁程序上的意義[91]。在網路安全議題上，受訪者肯認仲裁中對網絡安全的考慮程度在很大程度上取決於爭端的性質以及當事方的利益和身份[92]。參酌其調查受訪者經歷過何

[84] GDPR Art.32; GDPR Recital 78.
[85] GDPR Recital 84.
[86] GDPR Recital 85
[87] GDPR Recital 86
[88] Zahariev, *supra* note 44.
[89] Rosenthal, *Complying with the General Data Protection Regulation (GDPR) in International Arbitration: Practical Guidance*, 37 ASA Bull. 822, 824 (2019).
[90] Queen Mary, University of London, *2021 International Arbitration Survey: Adapting arbitration to a changing world*, 1, 30, http://www.arbitration.qmul.ac.uk/research/2021-international-arbitration-survey/(last visited May 22, 2021).
[91] *Id.* at 31.
[92] *Id.*

種保護措施（如下圖所示），僅雲端平台分享電子資料與電子方式提交的資料佔比近半，其他措施之使用均不到三分之一，可見實務上對資料保護與網路安全意識的低落；然而當涉及到受訪者認為應該使用何種措施時，近半（47%）建議使用「受保護/專門的電子郵件，而非基於一般網路的電子郵件服務供應商（Gmail、Yahoo、Hotmail 等）」，而其他建議選項也都取得超過三分之一的支持度，顯示網絡安全問題以及解決這些問題的必要性也開始受到重視[93]。



[93] *Id.* at 32.

以下將檢視各大仲裁機構針對資料保護是否有所規範、內容為何，以及仲裁社群內部所建議之應對措施。

一、各仲裁機構規則現行規定與補充

（一） International Chamber of Commerce Arbitration (ICC)

ICC 仲裁規則本身對於資料保護並未有相關規範。新冠肺炎疫情爆發後，於二〇二〇年四月九日 ICC 發布「國際商會關於減輕新冠肺炎疫情影響的若干可參考措施的指引 (ICC Guidance Note on Possible Measures Aimed at Mitigating the Effects of the COVID-19 Pandemic[94])」，主要聚焦於非實體進行程序，給予仲裁程序參與者程序進行上之建議，其中提及資料保護者為「任何非實體聽證都需要仲裁庭與當事方進行磋商，目的是實施足以遵守任何適用的隱私法規的措施（通常稱為網絡協議）。此類措施亦應處理仲裁程序中和電子文件交流平台中聽證的隱私性和電子通信機密性的保護」[95]、「客製化或收費的視訊平台可能比免費使用的公共平台提供更高的安全性、機密性和資料保護」[96]，並於本指引之附件中補充關於機密性、隱私權和安全性之考量[97]。

雖然仲裁規則並沒有規範，ICC 機構本身之 ICC 爭端解決程序資料隱私聲明（ICC Data Privacy Notice for ICC Dispute Resolution Proceedings）[98]針對資料保護有較貼近 GDPR 之內容，其肯認機構作為控管者的地位，並概括描述將如何使用所收到之個人資料以及可能分享資料之對象，針對資料之跨境移轉，明

---

[94] ICC Guidance Note on Possible Measures Aimed at Mitigating the Effects of the COVID-19 Pandemic, ICC, https://iccwbo.org/publication/icc-guidance-note-on-possible-measures-aimed-at-mitigating-the-effects-of-the-covid-19-pandemic/(last visited May 1, 2021).

[95] *Id.* Art. 26.

[96] *Id.* Art. 31.

[97] *Id.* ANNEX I CHECKLIST FOR A PROTOCOL ON VIRTUAL HEARINGS part C - Confidentiality, Privacy and Security "(i) Consultation between the tribunal and the parties on whether the virtual hearing will remain private and confidential to participants; (ii) Agreeing an access and confidentiality undertaking that binds all participants; (iii) Consultation between the tribunal and the parties on:

- the recording of the virtual hearing (audio-visual recording, confidentiality of the recording and value of recording compared to any produced written transcript, etc.);
- any overriding privacy requirements or standards that may impact access or connectivity of certain participants; and
- the minimum requirements of encryption to safeguard the integrity and security of the virtual hearing against any hacking, illicit access, etc."

[98] International Chamber of Commerce, *ICC Data Privacy Notice for ICC Dispute Resolution Proceedings*, INTERNATIONAL CHAMBER OF COMMERCE, https://iccwbo.org/dispute-resolution-services/icc-data-privacy-notice-for-icc-dispute-resolution-proceedings/ (last visited May 1, 2021).

確指出如果接收者不在受歐盟適足性認定（Adequacy Decision）的司法管轄區中，則將根據歐盟批准的定型化契約標準合同條款傳輸資料予秘書處，並為了滿足收集資料的目的以及滿足任何法律，會計或報告要求，將儲存個人資料，最後具體點出資料主體權利。

除上述規定之外，配合新修正之規則，ICC 也提供一份「關於各締約方和仲裁庭根據 ICC 仲裁規則進行仲裁的說明 Note To Parties and Arbitral Tribunals on The Conduct of The Arbitration Under The ICC Rules of Arbitration (2021/1/1)」為當事方和仲裁庭提供程序進行面上的參考依據，針對資料保護有較為具體的內容，諸如任何非實體聽證都需要在仲裁庭與當事方之間進行磋商，以實施通常被稱為網絡協議的措施，遵守任何適用的數據隱私法規，此類措施應涉及仲裁程序和任何電子文檔平台中聽證會的私密性和電子通信機密性的保護[99]；仲裁庭應與當事方協商，以確保用於非實體聽證會的任何影音共享平台均已獲得許可並設置為最大安全層級[100]；客製化或經授權許可的收費平台可能比免費使用的公共平台提供更好的安全性、機密性和數據保護[101]；當事人與其代表、仲裁人、秘書、證人、專家以及可能參與仲裁的其他個人都肯認，收集、轉移和儲存個人資料是出於仲裁程序之必要目的，並且在仲裁判斷、程序性命令和不同意見和/或協同意見公開時可以公開資料[102]；雙方應確保（1）其代表以及他們的證人、由當事人任命的專家以及代表他們或為他們的利益參加仲裁的任何其他個人，知悉其個人數據可能為仲裁目的而被收集、移轉、公開和儲存，（2）遵守所適用的資料保護法規[103]；在仲裁的適當時間，仲裁庭應提醒當事各方、代表、證人、專家和其他在場的個人，GDPR 或其他數據保護法律和法規適用於該仲裁，並且其個人資料可能根據仲裁協議或合法利益收集、移轉、發布和儲存，以解決爭端、仲裁程序公正有效地運作。為此，鼓勵仲裁庭制定資料保護協議[104]；當事人和仲裁員應確保僅處理對於仲裁程序而言必要且正確的

[99] Note To Parties and Arbitral Tribunals on The Conduct of The Arbitration Under The ICC Rules of Arbitration Art.101, ICC, https://iccwbo.org/publication/note-parties-arbitral-tribunals-conduct-arbitration/(last visited May 1, 2021).
[100] *Id.* Art.106.
[101] *Id.* Art.107.
[102] *Id.*
[103] *Id.* Art.118.
[104] *Id.* Art.119.

個人資料，並根據適用的資料保護法規，在仲裁範圍內被收集和處理其個人資料者都可以隨時對資料控管者行使其近用權，並且糾正或取締不正確的資料[105]；仲裁庭、當事方及其代表應準備妥當，並確保代表其行事者均採取適當的技術和組織性措施，以確保適合仲裁的資料安全，並考量所處理的範圍和風險、對資料主體的影響、所有涉及仲裁的人員的能力和監管要求、成本以及所處理或傳輸的資料的性質是否包含個人資料或敏感資料等[106]；任何違反個人資料安全性和機密性的行為都必須立即向個人資料可能受影響者報告， ICC 機構本身為資料控管者時，必須通知主管當局以及視情況將有關違規行為通知相關個人[107]。由說明內容可見其規範與提醒對應 GDPR 之權利義務，具有極高參考價值。

（二） London Court of International Arbitration (LCIA)

新冠肺炎疫情爆發後，LCIA 於二〇二〇年八月宣布更新其仲裁規則[108]。該新版仲裁規則已於同年十月一日生效，此次修正特點之一為補足舊版規則對非實體聽證規範上之缺漏，並支持機構在疫情下順利運作[109]。原於二〇一四年公佈之舊仲裁規則僅針對保密性有所規定（「作為一般原則，雙方對仲裁中所有裁定、為仲裁目的而創建之所有文件以及他方在程序中產生之一切文件進行保密，除非是法律義務可能要求當事方披露、保護或追求合法權利、在法院或其他法律機構的程序中強制執行或質疑仲裁判斷，否則不得公開披露[110]」、「仲裁庭審議內容將對其成員保密，除非適用法律另有規定並且根據第 10、12、26 和 27 條，仲裁庭其他成員必須披露仲裁員拒絕參加仲裁的情況」、「未經所有當事人和仲裁庭的事先書面同意，機構不會發布任何仲裁判斷或仲裁判斷的任何部分[111]」）。新修正之仲裁規則增加第 30A 條資料保護，規定「對個人資料

---

[105] *Id.* Art.120.
[106] *Id.* Art.121.
[107] *Id.* Art.122.
[108] Evgeniya Rubinina, *The LCIA Publishes its 2020 Rules: A Light-Touch Update to Meet Modern Needs*, KLUWER ARBITRATION BLOG (Aug.13. 2020), http://arbitrationblog.kluwerarbitration.com/2020/08/13/the-lcia-publishes-its-2020-rules-a-light-touch-update-to-meet-modern-needs/.
[109] LCIA, Updates to the LCIA Arbitration Rules and the LCIA Mediation Rules (2020) , LCIA , https://lcia.org/lcia-rules-update-2020.aspx (last visited Jan. 4, 2021).
[110] LCIA Arbitration Rules Art.30.1.
[111] *Id.* Art.30.3.

的任何處理均應遵守適用的資料保護法規，並且可以在 LCIA 網站上找到 LCIA 的資料保護通知[112]」、「根據其在第 14.1 條下的職責，在仲裁的早期階段，仲裁庭應諮詢當事方意見（並於適當之情況諮詢 LCIA 機構）考慮是否適宜：（i）採取任何具體的資訊安全措施，以保護在仲裁中共享的實體和電子資訊；和（ii）對仲裁中產生或交換的個人資料處理根據所適用的資料保護或相同效力之法律採取措施[113]」、「LCIA 機構本身和仲裁庭可以發布有關資料安全或資料保護的指示，這些指示對當事方具有約束力，對於 LCIA 機構發出的指示，也對仲裁庭成員具有約束力，但必須遵守強制性規定任何適用的法律或法律規則[114]」。除此之外也公布 LCIA 機構程序資料隱私聲明[115]與一般隱私聲明[116]，前者表明機構之資料控制者身份、如何取得個人資料、取得之個人資料種類、將如何使用與保存個人資料，並保證不會透露予第三方，除非是根據契約而受信任的第三方；後者則更細緻處理在仲裁程序中對個人資料之搜集處理，諸如針對不同參與者所搜集之不同個人資料、如何使用個人資料與其法律依據、個人資料分享之對象、個人資料移轉與保存以及程序參與者所享有之個人資料相關權利。上述兩項聲明對所有程序參與者提供詳盡之參考。

（三） Stockholm Chamber of Commerce Arbitration (SCC)

SCC 機構早在疫情爆發之前就已經著手推動仲裁程序電子化， 二〇一九年創建平台（SCC Platform）供所有仲裁文件共享交流。考慮到國際仲裁的性質以及許多國家之防疫措施，二〇二〇年 SCC 機構鼓勵仲裁庭使用實體參與以外的其他方式（例如視訊會議）繼續仲裁程序以避免程序延遲[117]，如利用 Microsoft Teams 和 Zoom 等視聽會議設施進行程序。SCC 機構仲裁規則本身並未針對個人資料處理有所規範，其所發佈之 SCC 機構平台指南（SCC Platform Guidelines）

---

[112] *Id.* Art. 30.4.
[113] *Id.* Art. 30.5.
[114] *Id.* Art. 30.6.
[115] LCIA, *Data Privacy Notice for LCIA Proceedings*, https://www.lcia.org/data-privacy-notice.aspx (last visited Jan. 4, 2021).
[116] LCIA, *General Privacy Notice*, LCIA, https://www.lcia.org/privacy-policy.aspx (last visited Jan. 4, 2021).
[117] Arbitration Institute of The Stockholm Chamber of Commerce, *COVID-19: INFORMATION AND GUIDANCE IN SCC ARBITRATIONS* (Mar. 23, 2020), https://sccinstitute.com/about-the-scc/news/2020/covid-19-information-and-guidance-in-scc-arbitrations.

[118]關於資料安全僅提及「所有文件都保存在具有高安全性之雲端，並在不同位置具有單獨的備份措施，主要和備用設施都位於德國，所有資料均使用軍用級加密並且在上傳時會掃描所有文件中的惡意軟體和病毒」，並提及所使用之安全措施。

（四） Singapore International Arbitration Centre (SIAC)

SIAC 機構規則本身並未針對資料保護有所規範（僅著墨於保密性），而該機構於二〇二〇年八月發布相關指引（SIAC Guides-Taking Your Arbitration Remote）[119]，幫助仲裁程序參與者有效地使用視訊會議等非實體程序進行方式，為不熟悉非實體審理者提供指導並提醒須注意之事項、列出主要考慮因素等等[120]，其中即包含考慮非實體聽證得否錄音錄影、錄音錄影是否涉及資料安全性問題（例如影音儲存在非實體聽證所使用之平台）、是否存在機密性和資料安全性問題（所使用之平台以及通過第三方儲存、託管和交換仲裁中之資料所可能面對的網絡安全風險，例如未經授權的第三方通過駭客方式取得機密資料、未經授權而保留、公開或使用機密資料等），當事人和仲裁庭應盡最大努力確保資料的安全性，並採取必要措施以確保遵守適用的資料保護法規[121]，在選擇非實體聽證所使用之平台時也應注意資料保護法規和網絡安全要求[122]。此外，其亦提供仲裁庭與當事方進行討論並準備與聽證有關的程序命令時得加以考量之清單，其中即包含機密性、資料保護與安全，當事人應盡最大努力確保非實體聽證會中交換、共享之資料之安全性[123]。

（五） Chartered Institute of Arbitrators (CIArb)

---

[118] Arbitration Institute of The Stockholm Chamber of Commerce, *SCC Platform Guidelines* (May. 25, 2020), https://sccinstitute.com/scc-platform/guidelines/.
[119] SIAC, Release of the SIAC Guides - Taking Your Arbitration Remote, SIAC (Aug. 31, 2020), https://www.siac.org.sg/69-siac-news/672-release-of-the-siac-guides-taking-your-arbitration-remote.
[120] SIAC, SIAC Guides - Taking Your Arbitration Remote, SIAC, (Aug. 31, 2020), https://www.siac.org.sg/images/stories/documents/siac_guides/SIAC%20Guides%20-%20Taking%20Your%20Arbitration%20Remote%20(August%202020).pdf.
[121] *Id.* at 3.
[122] *Id.* at 6.
[123] *Id.* at 10.

CIArb 機構仲裁規則本身對於資料保護並未多著墨，僅於其附件「附錄二：當事人和仲裁庭在案件管理會議上可能考慮的事項」中提及「任何需要採取特殊措施來保護機密或專有資料的機密性或商業秘密問題。」[124]。二〇二〇年四月，CIArb 發布「遠端爭議解決程序指引 Guidance Note on Remote Dispute Resolution Proceedings」，協助非實體程序之參與者順利進行程序，詳盡列出需要考慮之因素與建議[125]，對於程序前考量事項包含「應在聽證會之前將涉及非實體程序的網絡安全和安全技術層級納入考量並得到當事方的同意」[126]、「必須確保所使用的技術使所有參與者對其於非實體聽證上所揭露的資料的機密性感到安全。應嚴格限制所有非實體聽證群組和分組討論區的登入權限」[127]。

（六）Hong Kong International Arbitration Centre (HKIAC)

HKIAC 機構仲裁規則並未有相關規定，機構於二〇二〇年五月發布非實體聽證指南（HKIAC Guidelines For Virtual Hearings）[128]協助仲裁程序參與者順利有效地完成非實體聽證，然而其並未針對資料保護有實質性之規範，僅為確保聽證之機密性和安全性，尤其是在使用雲端平台時，要求使用密碼[129]。

（七） Korean Commercial Arbitration Board International Arbitration Rules（KCAB）

韓國國際商務仲裁委員會之仲裁規則並未針對資料保護有所著墨，惟為了因應視訊會議於國際仲裁中興起，加之肺炎疫情推波助瀾，於二〇二〇年三月發布首爾議定書（Seoul Protocol on Video Conferencing in International Arbitration, "Seoul Protocol")[130]，旨在通過電子化措施促進仲裁程序，同時使其程序之進行

---

[124] CIArb Arbitration Rules Appendix II "Matters for potential consideration by the parties and the arbitral tribunal at the case management conference", Art.1.2 "Any confidentiality or trade secret concerns that will require particular measures to protect confidential or proprietary information."

[125] CIArb, *Guidance Note on Remote Dispute Resolution Proceedings*, CIArb (2020), https://www.ciarb.org/media/9013/remote-hearings-guidance-note_final_140420.pdf.

[126] Guidance Note on Remote Dispute Resolution Proceedings Art.1.5.

[127] *Id.* Art.6.1.

[128] HKIAC Service Continuity During COVID-19, HKIAC, https://www.hkiac.org/news/hkiacservice-continuity-during-covid-19 (last visited Dec.1, 2020).

[129] HKIAC Guidelines For Virtual Hearings Art. 9.

[130] KCAB, *Seoul Protocol on Video Conference in International Arbitration is Released*, KCAB (Mar. 18, 2020),

更加簡單和安全，針對國際仲裁中視訊會議之規劃、測試與使用提供建議。議定書關於資料保護者有第 2.1 條 c 項「在可能的範圍內，並經雙方同意或法庭下令，視訊會議應在符合以下最低標準的地點舉行：地點應設在適當的位置，以令當事人與相關人員得公平，平等和合理進入會議。跨境連線也應得到適當保護，以防止第三方非法竊聽[131]」，針對安全漏洞的可能性提出建言，並建議充分保護視訊會議連結；第 8 條「未經仲裁庭許可，不得錄製視訊會議。視訊會議的任何錄影應於結束後的 24 小時內分發給仲裁庭和當事方。」限制視訊會議之錄音錄影以使錄音不會使與本案無關者接觸審理之內容[132]。

（八） Vienna International Arbitral Centre (VIAC)

雖然 VIAC 機構仲裁規則本身並未對資料保護有所規範，VIAC 機構為因應疫情下之非實體聽證需求，於二〇二〇年六月發布「The Vienna Protocol – A Practical Checklist for Remote Hearings」[133]，以清單形式提供仲裁人與當事人為適當地執行非實體聽證所需考量與執行之事項，鼓勵其為合理檢視並促進程序進行。此清單介紹選擇平台時建議考慮之因素、聽證前措施以及聽證過程中建議之注意事項等等，其中關於選擇非實體聽證平台須考量之因素，包含文件共享（考慮在聽證會期間如何取得文件，諸如通過雲端、螢幕共享、單獨的鏡頭顯示文件等）、影音記錄（平台的錄製功能，包括將影音儲存於在何處以及由誰儲存）以及資料安全性、機密性（確保平台提供足夠的保護措施以防止未經授權人員取得聽證內容，例如設定密碼、充分的加密等）等等。除此之外，於聽證會前籌組會議事先與各方詳細討論之事項包含機密性（討論所有必要步驟以確保程序機密性）、資料安全性、錄製（禁止未經參與者和仲裁庭事先許可的情況下記錄程序的任何部分）。

（九） China International Economic and Trade Arbitration Commission Arbitration (CIETAC)

---

http://www.kcabinternational.or.kr/user/Board/comm_notice_view.do?BBS_NO=548&BD_NO=169&CURRENT_MENU_CODE=MENU0025&TOP_MENU_CODE=MENU0024.

131 Seoul Protocol on Video Conference in International Arbitration Art.2.1.

132 *Id.* Art.8.1.

133 VIAC, *Checklist on Holding Hearings in Times of COVID-19*, VIAC, https://www.viac.eu/en/news/checklist-on-holding-hearings-in-times-of-covid-19 (last visited May 19, 2020).

中國國際經濟貿易仲裁委員會仲裁規則（China International Economic and Trade Arbitration Commission Arbitration Rules）本身對於資料保護原本未有規定，僅於審理方式上給予仲裁庭裁量權限[134]。疫情爆發後於二〇二〇年四月二十八日發佈「關於新冠肺炎疫情期間積極穩妥推進仲裁程序指引（China International Economic and Trade Arbitration Commission Guidelines on Proceeding with Arbitration Actively and Properly during the COVID-19 Pandemic）」，此指引於二〇二〇年五月一日起施行，計畫疫情結束後廢止，然而觀其內容其仍未有針對個人資料與網路安全有所著墨。

（十）The Japan Commercial Arbitration Association Commercial Arbitration (JCAA)

日本商務仲裁協會商務仲裁規則（The Japan Commercial Arbitration Association Commercial Arbitration Rules）對於資料保護並未有所規定，僅約略提及仲裁庭應選擇適當的舉行聽證的方式[135]，給予仲裁庭程序上裁量權限。

二、近期國際仲裁社群所提出之建議

除卻上述各大仲裁機構規範以及所補充之相關內容，國際仲裁社群也陸續提供程序執行面上的建議，其中資料保護與網路安全具有一定關聯性，當事方、仲裁庭和仲裁機構間資料共享與傳遞也增加資料遺失或外流的可能性，有害於資料保護。以下將檢視近期國際仲裁社群針對資料保護與網路安全所提出之相關建議。

（一） ICCA-IBA Roadmap to Data Protection in International Arbitration

國際商務仲裁理事會（International Council for Commercial Arbitration, ICCA）與國際律師協會（International Bar Association, IBA）共同成立國際仲裁資料保護工作小組，針對國際仲裁中的資料保護研議一份大眾諮詢草案，即ICCA-IBA國際仲裁資料保護藍圖（ICCA-IBA Roadmap to Data Protection in International

[134] 中國國際經濟貿易仲裁委員會仲裁規則第 35 條。

[135] The Japan Commercial Arbitration Association Commercial Arbitration Rules (2019) Art.50.3.

Arbitration，以下簡稱為「藍圖」），針對 GDPR 對國際仲裁程序的潛在影響提供建議[136]，使仲裁參加者能夠在程序中識別並有效解決資料保護問題[137]。

藍圖主要分為兩大部分。第一章對 GDPR 之規範內容進行簡述，著重於可能適用於國際仲裁的重要部分，從 GDPR 的適用範圍、管轄內容、法適用下的角色、資料移轉規定到在仲裁中適用的原則。對於程序中的角色，路線圖明確認定大多數仲裁參與者被視為資料控制者，因為其本質上可以控制自己處理資料時的目的和方式，例如歐盟和英國的相關資料保護機構都認為律師是控制者[138]。秘書與口譯員等則可能會被視為處理者[139]。資料跨境傳輸是國際仲裁程序本質上所固有，藍圖明確指出允許進行資料跨境傳輸的情況有四種：接受資料地為已取得歐盟充足資料保護認定之國家、具有適當保障措施（仲裁而言最有可能是以定型化契約條款方式為事前約定）、特定例外（仲裁中通常為行使或防禦法律上請求而有必要之資料處理）以及合法利益（因高門檻而難以適用）[140]，強調每一位仲裁程序參與者應在程序開始時考慮所適用之規定與限制，提早進行規劃。藍圖亦詳細針對資料保護九項法律原則（公正合法、比例性、資料最少蒐集原則、目的限制、資料主體權利、正確性、資料安全性、透明性、責任）為適用討論。

第二章更近一步討論國際仲裁程序中如何遵守資料保護，區分仲裁的事前準備與程序開始後的注意內容，值得注意者為此藍圖強調儘早分配資料保護義務責任的重要性，以遵守相關法律並符合仲裁效率[141]，附件三更提供仲裁過程中所需考慮的檢查清單。同時，藍圖也鼓勵針對如何適用資料保護訂定資料保護協議（Data Protection Protocol），在仲裁中有效管理所有仲裁參與者遵守相關法規[142]，附件四則為資料保護協議之範本。除此之外，藍圖之附件五合法利

[136] International Council for Commercial Arbitration, *ICCA-IBA Roadmap to Data Protection in International Arbitration*, https://www.arbitration-icca.org/icca-iba-joint-task-force-data-protection-international-arbitration (last visited Jan.20, 2021).
[137] *Id.* at 3.
[138] *Id.* at 9.
[139] *Id.* at 10.
[140] *Id.* at 12.
[141] *Id.* at 40.
[142] *Id.* at 41.

益評估、附件七歐盟定型化契約等內容也提供仲裁參與者對於資料保護之處理上的建議。

藍圖並未針對非實體聽證有特殊規定，惟按照上述內容，仲裁庭在非實體聽證舉行之前即應考慮所有資料保護的問題，並於第一次案件管理會議上與所有仲裁參與者進行討論。於平台選擇上，應考慮平台對於資料之收集處理是否符合資料保護要求、是否符合 GDPR 第 32 條所規範之內容（個人資料之假名化及加密、理系統及服務持續之機密性等等），如果涉及條特殊類型之個人資料處理，於非實體聽證中是否得傳輸、共享、紀錄，仲裁庭作為資料控制者也應事先為評估。

（二） Africa Arbitration Academy Protocol on Virtual Hearings in Africa

二〇二〇年四月，非洲仲裁學院（Africa Arbitration Academy）發布非洲仲裁學院關於非洲非實體聽證議定書 （Africa Arbitration Academy Protocol on Virtual Hearings in Africa，以下簡稱為「議定書」）[143]，此議定書是為因應疫情延燒，針對非洲之具體現況而制定，供仲裁庭、當事人和律師於非實體聽證之籌備與進行時加以參酌。其涵蓋了後勤準備、安全和隱私注意事項以及技術規範等內容，確保在仲裁程序中交換的資料的安全性、機密性以及保護措施[144]，並提供四項附件（「附件一–最低網絡安全標準 Annex I Minimum Cybersecurity Standards」、「附件二–非洲仲裁學院示範仲裁條款（包括非實體聽證的選項）Annex II Model Africa Arbitration Academy Arbitration Clause (including Virtual Hearing Option)」、「附件三-非洲仲裁學院示範非實體證協議。Annex III Model Africa Arbitration Academy Virtual Hearing Agreement」、「附件四–仲裁庭發布之網絡協議 Annex IV Tribunal-Issued Cyber Protocol」）供仲裁庭與當事方參考使用。

與非實體聽證相關者為，其要求當事人和仲裁庭應事先就所有非實體聽證參與者所使用的所有技術、軟體、設備和平台達成事先協議，所使用的技術、

[143] Africa Arbitration Academy, Africa Arbitration Academy Protocol on Virtual Hearings in Africa 2020, https://www.africaarbitrationacademy.org/protocol-virtual-hearings/.
[144] *Id.* Art.1.5.

軟體、設備和平台應符合本議定書附件一中詳述的最低標準[145]。非實體聽證與證據呈現上，「雙方可能同意利用雲端儲存服務來保存在非實體聽證所用的所有文件，並應採取適當的措施以確保儲存本身以及敏感性電子資料受到密碼保護（免於非法擷取或遭第三方取得）[146]，雙方得同意在非實體聽證期間使用文件共享平台，該平台允許所有使用者同時查看正在討論的文件[147]，而非實體聽證的任何記錄均應用於產生聽證筆錄，並應在虛擬聽證會結束後商定的時間表內分發給各當事方[148]。安全性與隱私考量方面，「非實體聽證期間進行的任何資料交換均應安全且機密[149]，非實體聽證的每一方均應在聽證會舉行前的一周內，向仲裁庭提供所有參加者的名單，根據仲裁庭的任何其他指示，非實體聽證參加者應限於當事方的代表、律師、證人、仲裁庭成員、仲裁庭庭秘書、報告者以及在呈現證據或出現任何技術問題時提供所需協助的後勤人員、技術人員或其他輔助人員[150]，當事雙方應確保用於連接非實體聽證的房間，配備有進行非實體聽證所必需的設備，並且在非實體聽證期間非參與者或未經授權的人員不得進入[151]。議定書並針對聽證協議、基礎設施和技術標準有所要求，當事雙方應確保其同意使用之平台均已獲得許可，並具有足夠的安全性和隱私標準，技術設備應安全且用使用者友善[152] 。

（三） IBA Rules on the Taking of Evidence in International Arbitration

二〇二〇年十二月十七日，國際律師協會（International Bar Association）通過新修訂的國際仲裁取證規則（IBA Rules on the Taking of Evidence in International Arbitration）[153]。其中新修訂第 2.2（e）條新增關於網絡安全和資料保護之內容，「關於證據的磋商得解決取證的範圍、時間和方式，包括在適

[145] *Id.* Art.2.1.2.
[146] *Id.* Art.3.3.2.
[147] *Id.* Art.3.3.3.
[148] *Id.* Art.3.5.2.
[149] *Id.* Art.4.1.
[150] *Id.* Art.4.2.
[151] *Id.* Art. 4.5.
[152] *Id.* Art. 5.2
[153] IBA Rules on the Taking of Evidence in International Arbitration (2020), INTERNATIONAL BAR ASSOCIATION, https://www.ibanet.org/Publications/publications_IBA_guides_and_free_materials.aspx(last visited May 22, 2021).

用的範圍內處理任何（e）網絡安全和數據保護問題」[154]，將網絡安全和資料保護添加到仲裁庭可以諮詢當事方意見的問題範圍，強調在早期階段即考慮資料保護（包含隱私和網絡安全）相關問題。同規則第 8.2 條也規定「……仲裁庭應與當事方協商，以達成遠程聽證協議……。該協議得解決：（a）所使用的技術；（b）對該技術進行預先測試或針對該技術進行培訓……」[155]，鼓勵仲裁庭積極主動，並且如果以非實體形式進行證據聽證，則應與當事雙方共同制定相關的協議[156]。此次規則的修訂體現網絡安全和資料保護應當受到仲裁庭與程序參與者的重視，但是並沒有為近一步具體建議，僅要求為事前程序協議。

（四） ICCA-New York City Bar-CPR Protocol on Cybersecurity in International Arbitration

國際商務仲裁理事會（ICCA） 與紐約律師協會（New York City Bar Association, NYC Bar）、國際爭端預防與解決中心（Conflict Prevention and Resolution, CPR）組成仲裁網絡安全工作小組，其為仲裁員、律師、機構提供指引，並提供雙方當事人在仲裁中可以採用的選擇性協議，仲裁網絡安全工作小組並於二〇一九年十一月二十一日發布「二〇二〇年國際仲裁網絡安全議定書（ICCA-New York City Bar-CPR Protocol on Cybersecurity in International Arbitration）」[157]。該議定書反映了來自世界各地的仲裁機構、律師事務所、仲裁程序中的專家證人等等的意見，處理涉及維護資料的機密性、完整性與可用性的措施[158]，肯認任何仲裁參與者在資料安全性上的影響都可能不利於所有參與者並損害整個仲裁的安全性[159]。其多次強調參與人員對相關規範之認知與相互協商之必要，諸如「各方當事人、仲裁員和機構應確保所有直接或間接參

[154] *Id.* Art.2.2.
[155] *Id.* Art. 8.2.
[156] 1999 IBA Working Party & 2010 IBA Rules of Evidence Review Subcommittee & 2020 IBA Rules of Evidence Review Task Force, *Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration*,1, 25 (Jan. 2021), https://www.acerislaw.com/wp-content/uploads/2021/03/Commentary-on-2020-IBA-Rules-on-Taking-Evidence-in-Int-Arbitration-1.pdf.
[157] International Council For Commercial Arbitration, *ICCA-New York City Bar-CPR Protocol on Cybersecurity in International Arbitration*, https://www.arbitration-icca.org/cybersecurity-international-arbitration-icca-nyc-bar-cpr-working-group (last visited Mar. 8, 2021).
[158] *Id.* at 7.
[159] *Id.* at 10.

與仲裁者均知悉並遵循訴訟所採取的任何資料措施,以及資料安全事故的潛在影響[160]」、「決定哪些特定資料安全措施適用於特定仲裁時,訴訟各方和審裁處應考慮:（a） 仲裁的風險狀況，同時考慮附表 B 所列因素（b）各方、仲裁者以及機構的現有資料安全的做法、基礎設施和能力……（d）與爭端規模、價值和風險狀況成比例……」等等，而其也列出在決定合理資訊安全措施時須考慮的因素[161]，並提供資料安全措施數項供參考選擇[162]。仲裁人、當事人和管理機構應參考附表 C，以瞭解如何制定每一類別的安全措施以應對不同的風險[163]。第一次案件管理會議上仲裁庭應邀請法律代表討論合理的資訊安全措施、討論仲裁庭成員採取措施的能力和意願以及處理關於合理資訊安全措施的程序爭議[164]，仲裁庭在適當的情況下,有權決定適用於仲裁的資料保安措施[165]，如違反所採用的資料安全措施或發生資料安全事故,仲裁庭可酌情決定相關成本分配及對各方施加懲罰[166]。最後提供三張附表：「Schedule A Baseline Security Measures」（補充原則 2 並提供一般可以採用之措施清單）、「Schedule B Arbitral Information Security Risk Factors 」（協助訴訟各方及仲裁庭評估仲裁中的資料安全的風險，約有以下考慮因素：所處理資料之本質、與仲裁主體以及程序參與者相關之風險、其他影響仲裁風險狀況之因素、違反資料保護之可預期結果，按風險狀況進行分析可將需要不同保護措施的風險進行分類並進一步採取合理應對）[167]、「Schedule C Sample Information Security Measures」（建立在附表 A 的基礎上補充原則 7、8，列出針對特定事項所採取的措施參考清單）[168]。

此議定書提供仲裁程序整體上所需要考量之內容以及可以採取的措施，為仲裁參與者指出具體而明確的方向，雖然並沒有對聽證程序本身提出具體建言，然則所有程序參與者均得依照自身情況參酌議定書內容決定如何進行資料保護與網路安全並採取相應措施，給予仲裁庭以及當事人相當大的靈活度。

---

[160] *Id.* at 12-3.
[161] *Id.* at 18.
[162] *Id.* at 24.
[163] *Id.* at 20.
[164] *Id.* at 26.
[165] *Id.* Principle 11.
[166] *Id.* Principle 13.
[167] *Id.* at 50.
[168] *Id.* at 55.

（五） Hogan Lovells Protocol for the use of technology in virtual international arbitration hearings April 2020[169]

除上述仲裁組織，也有其他法律相關從業人員提出建議。Hogan Lovells 法律事務所提出於國際仲裁非實體聽證會技術使用協議（Hogan Lovells Protocol for the use of technology in virtual international arbitration hearings April 2020）協助確保程序順利進行，減少技術問題。其協議內容精簡，對於非實體聽證資料保護與網路安全上，其建議當事人應努力選擇一個安全穩定的平臺，各方應考慮平臺所提供的加密程度、保安措施的種類（例如平臺是否提供受密碼保護的會議）以及調查平臺可能帶來的網絡風險，在沒有有線網路的情況下不應使用公共無線網路而是應該使用受密碼保護的、安全的無線網路[170]。各方當事人（包括代表其作證的代表、證人和專家）應確保其行為均符合所適用之資料保護法規[171]。各方當事人可同意使用雲端儲存服務以接收仲裁過程中所有文件。任何敏感性電子文件應受密碼保護，如使用第三方雲端儲存、傳送文件，應採取足夠措施確保該等儲存系統受密碼保護[172]。

三、小結

機構仲裁規則本身針對非實體聽證程序多數未有相關規範，惟並不意味機構並未認知到非實體聽證之重要性與特殊性，而多以不更動機構規則的補充指引形式給予建議。而藍圖之出現也體現對資料保護面向的重視，非洲仲裁學院關於非洲非實體聽證議定書更特別針對非實體聽證下程序議題有所討論。資料保護尚涉及各資料保護法規規範範圍不同，以不具有拘束力之指引形式或可以保持適用上的彈性而交予仲裁庭、律師與仲裁庭個案判定最適切的做法，僅發揮提醒的功能。由上述指引、議定書等等的內容可知當事人、律師以及仲裁庭應在仲裁過程前階段即相互協商，評估將在仲裁過程中共享的資料的性質、採

169 Hogan Lovells, *Hogan Lovells Protocol for the use of technology in virtual international arbitration hearings April 2020* (Apr. 2020), https://www.hoganlovells.com/en/publications/hogan-lovells-protocol-for-the-use-of-technology-in-virtual-international-arbitration-hearings.
170 *Id.* Art. 2.5.3 (b).
171 *Id.* Art. 2.9 (a) (iv).
172 *Id.* Art. 3.2. (a).

取適當的保護措施、所涉及之資料保護法規、是否為資料保護評估等等。仲裁規則中或可以要求仲裁庭即應於案件管理會議階段強制要求程序參與者為討論協商甚至參考 GDPR 要求進行資料保護評估，預防程序開始後各項限制與風險。

肆、我國內國相關規範修正與仲裁庭程序執行上建議

GDPR 施行生效至今，已有許多國家取得適足性認定，個人資料得從歐盟移轉至該該取得認定之國家而無需任何進一步的保護措施，韓國於與歐盟之協商也已經取得重大進展，有望近期取得適足性認定[173]。我國則已經對歐盟提交申請，積極尋求適足性認定[174]，我國國家發展委員會已根據 GDPR 要求提交了自我評估報告使歐盟能夠確定台灣是否具有足夠的資料保護水準[175]，為取得 GDPR 適足性認定與因應國內需求，國家發展委員會已於 108 年啟動個人資料保護法之修法[176]，立法委員並已提出修法草案，參照 GDPR 內容對現行個資法進行全文修正[177]，可見我國對於接軌 GDPR 之強烈企圖，若日後相關修法通過生效，可期待我國之個人資料保護將提升至歐盟層級，並享有與歐盟間順暢之資料流通。

回歸我國之仲裁法與中華民國仲裁協會仲裁規則，關於資料保護與網路安全均未有所提及。中華仲裁國際中心仲裁規則（CAAI Arbitration Rules）[178]其僅規定「仲裁庭得允許或要求當事人提示仲裁庭認為與案件相關並對案件結果有重要影響之文件、附件或其他證據……除當事人另有約定外，仲裁庭應決定是否召開詢問會以提示證據或行言詞辯論，或是否僅以文件及書狀為基礎進行審

---

173 European Commission, *Joint Statement by Commissioner Reynders and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea*, EUROPEAN COMMISSION (lasted visited May 1, 2021), https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506.

174 Liao Wei-min, Digital protection necessary for Taiwan, TAIPEI TIMES (Sep.9, 2019) , https://www.taipeitimes.com/News/editorials/archives/2019/09/09/2003721955.

175 Central News Agency, *EU lauds Taiwan's efforts to push for talks on data transfer deal*, TAIWAN NEWS (Mar. 11, 2019), https://www.taiwannews.com.tw/en/news/3655633.

176 國家發展委員會，「國發會推動個資法修法，力拼 GDPR 適足性認定」 https://www.ndc.gov.tw/nc_27_33660。

177 立法院議案關係文書，院總第 1570 號 委員提案第 25284 號， https://lis.ly.gov.tw/lygazettec/mtcdoc?PD100204:LCEWA01_100204_00037。

178 參照中華仲裁國際中心仲裁規則第一條規定，此規則適用於仲裁地係臺灣地區以外之仲裁，至於以臺灣地區為仲裁地之仲裁，則繼續適用中華仲裁協會規則。

理。仲裁庭得於仲裁程序之適當階段依當事人之聲請或依職權召開詢問會」[179]，以及關於當事人發表、揭露或傳遞資訊之機密問題以及仲裁判斷得公開之情況[180]，至於程序中涉及之相關問題則回歸仲裁庭之程序指揮權限以及各參與者在依其所適用之法規下各負其責。除卻歐盟本身，也有國家紛紛推動參照歐盟規範內容進行資料保護之要求之相關立法（如美國維吉尼亞州已通過之 Consumer Data Protection Act，CDPA），中華仲裁國際中心所處理之案件所使用之資料如若被涵蓋於歐盟或相近立法之國家之資料保護法規之範圍內，於仲裁過程中極可能面對相似風險，且我國亟欲取得適足性認定並推相關修法，於此之狀態下也須考量將來施加於仲裁程序參與者之責任與程序上限制，我國國內尚未有所規定或建議稍顯遺憾。

建議仲裁機構可修改仲裁規則明確化資料保護與網路安全之重要性，課予所有程序參與者相關義務，而細部具體內容則因應不同案件之狀況而給予彈性空間，令程序參與者得個案判斷最妥適做法。觀察現行主要仲裁機構中僅 LCIA 明文要求對資料保護有所要求，或可參考其作法直接賦予仲裁庭相關權力與義務，在仲裁前階段仲裁庭應與當事方商討：（1）是否針對仲裁程序中所處理之資料採取何種資料保護措施（2）確定所適用之一切資料保護相關規範為何，並針對所處理之個人資料採取符合上述規範所要求之措施，本仲裁機構和仲裁庭得發布有關於資料保護之指示，對當事方與仲裁庭均具有約束力。

於尚未進入聽證程序前之案件管理會議上，所有程序參與者（尤其是仲裁庭與當事方）即針對網絡安全、資料保護與處理進行討論與分析並進一步達成共識，必須確認:

- 涉及之資料保護法規與違反之潛在法律後果[181]
- 辨別程序參與者各自於資料處理上所擔任之角色[182]
- 所使用之資料之性質、合法處理資料之要件為何（如適用規範即為 GDPR，正當利益之評估可直接參照 ICCA-IBA 國際仲裁資料保護藍圖附件五正當利益評估表 Checklist for Legitimate Interest Assessment）

[179] 中華仲裁國際中心仲裁規則第二十四條。
[180] 中華仲裁國際中心仲裁規則第三十九條。
[181] 詳參前述第貳章第一、二、五節。
[182] 詳參前述第貳章第三節。

- 法規上強制要求之措施

同時，建議訂定資料保護程序協議，清楚界定分配各自所涉責任之範圍與內容，並對須採取之資料保護與網路安全措施以及風險管理達成共識，諸如技術上確保使用安全網絡連線、對資料進行加密、嚴格管理資料之近用、資料傳輸過程之要求（例如使用受保護/專門的電子郵件系統）、資料之儲存刪除、若案件複雜是否尋求專業資料保護團隊的意見協助評估整體風險、是否尋求外部第三方提供對網絡安全措施的支持服務等等。須注意者為訂定資料保護程序協議並非即免除所有疑慮與風險，蓋程序進行中仍可能有突發變數（例如新提出之資料即需要重新審視所涉規範），惟可以盡最大可能避免可知風險與不確定性。

除卻前階段之事前準備，非實體聽證過程中之資料具有流動性，所有程序參與者須隨時注意新「加入處理」之資料並重新確認上述事項。仲裁庭與當事方或可於前述程序協議中建立一個資料處理流程，特別是針對資料主體可能主張之權利，要求使用資料者進行先行查核與通知，確認合法之使用以加速排除使用上的不確定性。擬定上或可參照非洲仲裁學院所提供之「仲裁庭發布之網絡協議」為基礎範本，並增加雙方均有共識將採取之資料保護措施、建立上述應對新提出之資料使用之流程，同時，也參考 ICC 所提出之「ICC 非實體聽證協議核對清單暨非實體聽證會組織程序命令與網絡協議之建議條款 ICC Checklist for a Protocol on Virtual Hearings and Suggested Clauses for Cyber-Protocols and Procedural Orders Dealing with the Organisation of Virtual Hearings」[183]內容，「雙方應在聽證會前（兩週內）共同考慮適用於任何參與者所在地的法律（此法律可能會對資料保護提出要求），並且仲裁庭應與各方協商後決定採取何種措施，以解決在所適用之規範下可能影響任何參與者的資料近用或連線上的問題。如果任何一方認為需要採取進一步的安全措施來保護聽證會的完整性、降低網絡攻擊或未經授權近用聽證會內如的風險，則該方必須在獲悉原

[183] ICC, ICC Checklist for a Protocol on Virtual Hearings and Suggested Clauses for Cyber-Protocols and Procedural Orders Dealing with the Organisation of Virtual Hearings, https://iccwbo.org/publication/icc-checklist-for-a-protocol-on-virtual-hearings-and-suggested-clauses-for-cyber-protocols-and-procedural-orders-dealing-with-the-organisation-of-virtual-hearings/ (last visited July 20, 2021).

因後立即提出。在與雙方協商後，仲裁庭應決定在這方面應採取哪些進一步措施」，明確化程序之進行要求。

我國目前尚待補足相關規定，仲裁機構方面除上述針對資料保護增訂規則之外，也期待參照國際上諸機構所提出之指引，發布適合我國之程序清單或指南，從規則面、實務操作面上盡可能與仲裁庭、所有程序參與者攜手共同維護資料安全，建構無疑慮的紛爭解決程序。

伍、結論

仲裁程序中，資料控管者與處理者本身會面對違反資料保護法之相關責任，依照 GDPR 規定內容，任何人應有權利自控管者或處理者就其損害獲得賠償[184]，除非控管者或處理者能證明其從任何方面皆非造成損害之原因而免除責任，而當控管者或處理者亦參與同一資料處理時，應追究各控管者或處理者就整個損害之法律責任[185]，同時還有受裁處行政罰鍰[186]甚至刑責[187]之風險，是以所有仲裁程序參與者都必須對於相關規定有所警覺並嚴格遵守。

我國相關仲裁規範仍未對資料保護需求有所回應，仲裁機構方面建議進行增補以完善相關規範，惟考慮個案情況不同，仲裁機構規則明確化資料保護之義務已足，或可參考國際上各大仲裁機構已提出之指引內容，提出不具拘束力之指導性指南，提醒仲裁庭與當事雙方程序進行上需注意之事項。另建議仲裁程序參與者於前階段、尚未進入聽證程序前之案件管理會議上，即針對網絡安全、資料保護與處理為前置準備，保有最大的彈性，盡可能涵括各種可預見之風險。非實體聽證作為疫情期間維持程序進行之手段，考慮到國際仲裁中的當事人往往位於世界不同地區，非實體聽證可免去長途跋涉之累，線上平台越加發達，加之日後仲裁庭對非實體程序之熟悉度提升，非實體聽證具備節省時間和成本、具有效率之優點，疫情結束後仍可期待非實體仲裁之發展，是以更應完善化相關規定以因應未來之需求。

[184] GDPR Art. 82.
[185] GDPR Recital (146).
[186] GDPR Art. 83.
[187] GDPR Recital (148), (149).