Accepted for publication in *Contemporary Asia Arbitration Journal* published by National Taiwan University.

"Business as usual" during an unprecedented time – the issues of data protection and cybersecurity in international arbitration

Hong-Lin Yu

"The maxim of the British people is 'business as usual'" – Winston Churchill

The emergency measures operated in the UK by Her Majesty's Courts and Tribunals Service during COVID-19

COVID-19 brought the world to a standstill. Following the UK Parliament's introduction of the Coronavirus Act 2020[1] on 25 March 2020, it is evident that the UK Courts and Tribunals Service (HMCTS) has significantly reduced its operation and is also carrying out remote proceedings during the lockdown. Section 55 and Schedule 25 of the Act stipulate the temporary measures for public participation in court proceedings by video or audio. At the time of writing,[2] in line with public health advice, HMCTS has announced further measures to maintain the safety of all in the courts. The current measures include: observing social distance, avoiding gatherings, consolidating the work of courts and tribunals into fewer buildings, avoiding physical hearings, using telephone and video / remote hearings wherever possible. These measures see the HMCTS covering "urgent work" only and operating remote hearings. As a result, the delivery of civil justice operates in a much-reduced capacity in all courts, in particular in the Magistrates' Courts, the County Courts, the High Court,[3] and the Court of

[1] http://www.legislation.gov.uk/ukpga/2020/7/contents/enacted <accessed on 7 April 2020>
[2] 6 April 2020
[3] https://www.judiciary.uk/you-and-the-judiciary/going-to-court/high-court/ <accessed on 7 April 2020>

Appeal[4] in England and Wales, as well as the Sheriff Courts, the Sheriff Appeal Court and the Court of Session in Scotland.[5]

On 6 April 2020, a sub-division of the English High Court, the Technology and Construction Court (TCC), delivered its first case concerning the impact of the COVID-19 emergency in the context of adjudication of a construction dispute. The message from *MillChris Developments Ltd v Waters*[6] is pretty much "business as usual" as well as delivering the courts' commitment to carrying on during the COVID-19 outbreak and their expectation that parties should continue with their adjudication process.

In this case, Ms. Waters, the home owner, complained about an overcharge of £45,000 for defective work undertaken by MillChris Developments Ltd. Ms. Waters commenced an adjudication on 23 March 2020, the same date as the day the UK government imposed the strict lockdown and social distancing policy to combat COVID-19. The timetable issued by the adjudicator indicated that the submissions should be completed by 3 April 2020 and a site visit on 14 April 2020. MillChris Developments Ltd. requested a postponement of the adjudication until the end of the COVID-19 crisis. The adjudicator refused the postponement but offered an extension to the timetable of 2 weeks. MillChris Developments Ltd. applied to the TCC for an injunction prohibiting the homeowner from proceeding with the adjudication on the ground of breach of natural justice should adjudication be allowed to continue in its current timetable.

[4] https://www.judiciary.uk/you-and-the-judiciary/going-to-court/court-of-appeal-home/ <accessed on 7 April 2020>
[5] http://www.scotland-judiciary.org.uk/16/0/Court-Structure <accessed on 7 April 2020>
[6] *MillChris Developments Ltd v Waters* [2020] 4 WLUK 45

The judge, Mrs Justice Jefford, rejected the application for the injunction. Citing *American Cyanamid v Ethicon,*[7] the court followed the requirement of clear cut situations and found that there was no real issue to be tried in the current case. The court held the view that short timescales are the essence of the adjudication process and COVID-19 was not the real cause that exacerbated the situation. The court also stated that the papers required for the adjudication could be scanned or sent to the adjudicator. The two-week extension would have allowed MillChris Developments Ltd. the extra time required to contact its witnesses. It also decided that the site visit should continue as parties are not allowed to be present at a site visit in adjudication; moreover measures being put in place to avoid undue influence on the adjudicator can be arranged. Based on the principle of adjudication, the court rejected the unmeritorious application in this case and maintained a "business as usual" approach. *MillChris* highlighted that any claim for *force majeure* or the like must demonstrate a link and impact between the global pandemic and failure to comply with a contractual obligation.

Although no case related to arbitration proceedings in the context of COVID-19 has been published, it is reasonable to expect that the English courts will hold the same commitment to arbitration. This perhaps is the reason why the arbitration community reacted differently to the COVID-19 crisis. The purpose of this article is to, first of all, highlight the "business as usual" approach adopted by the international arbitration community, in particular, institutional arbitrations. It will be followed by a discussion on how the temporary measures of using e-platforms, electronical filings and videoconferencing can impact on the duty of confidentiality, data protection and cybersecurity. As regards data protection and cybersecurity, an in-depth discussion will be carried out in the context of the Seoul Protocol on Video Conferencing in

[7] *American Cyanamid v Ethicon* [1975] AC 396

International Arbitration (the Seoul Protocol), [8] the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration 2020 (the Cybersecurity Protocol), [9] and the consultation draft of the ICCA/IBA Joint Task Force's Roadmap on Data Protection in International Arbitration (the ICCA/IBA Consultation),[10] as well as considering whether they can address the concerns of cybersecurity and data protection in light of COVID -19 and beyond. The examination will conclude with an emphasis on the arbitral participants' understandings of their dual roles in both arbitration and data protection / cybersecurity as well as their mutual impact in order to ensure the delivery of cybersecurity across borders in international arbitration.

The swift reaction to COVID -19 from the arbitration community

Since the introduction of travel restrictions, quarantine, self-isolation, social distancing and lockdowns, remote hearings and electronic data transmission at the substantive stages of arbitration have become a norm. Instead of reducing its capacity as HMCTS has done, the arbitration community's operation is pretty much "business as usual". The arbitration community swiftly adopted remote access technologies to carry out case management conferences, electronic document storage, procedure preparation, and examination of witnesses and expert witnesses when the circumstances justify it. Some arbitration institutions have decided to remain fully operational with split institutional administration teams with the main offices closed.[11] Others have transitioned to working remotely and are operating under a

---

8 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 <accessed on 7 April 2020>

9 http://documents.nycbar.org/files/ICCA-NYC-Bar-CPR-Cybersecurity-Protocol-for-International-Arbitration-Electronic-Version.pdf <accessed on 7 April 2020>

10 https://www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf <accessed on 7 April 2020>

11 Following the additional measures announced by the Singapore Government on 3 April 2020, the SIAC offices were closed on 7 April 2020, even though SIAC remains fully operational with all staff telecommuting. See the announcement on https://www.siac.org.sg/ <accessed on 7 April 2020>

new e-filing system.[12] Most institutions require requests/notices of arbitration to be filed via email for the duration of the pandemic and have shifted to electronic or telephonic methods of communication.[13] In-person hearings are replaced with virtual hearings where one sees virtual online dispute resolution being brought back to international arbitration with the use of Cisco WebEx, FaceTime, Skype, Microsoft Teams, Zoom, virtual ADR service, ISDN or IP communication lines, ICSID's video conferencing platform, … and so on.[14] Within a very short period of notice, arbitration institutions have been forced to adapt different ways of working in order to keep the dispute resolution process agreed between the parties going. Placing business continuity as the top priority and being equipped with contingency plans, arbitration continues during the lockdown.

As one adjusts themselves to navigate through the unfamiliar social distancing and remote working during this unsettling period, arbitration appears to be able to proceed without significant interruption. Arbitrators seem to be well placed to handle the procedures creatively and flexibly. However, words of warning have been spoken in terms of cybersecurity, data protection compliance and arbitral participants' training and understanding of their roles with the increasing use of e-filing, video-conferencing, and email communications in arbitration proceedings and data protection; particularly the interaction between data protection / cybersecurity and the arbitration institutions' undertaking of the duty of confidentiality.

---

[12] ACICA requests that all new filings, from 19 March 2020 until staff return to the office, be made through the ACICA E-Filing system (which allows payment directly by credit card) or by email to the ACICA Secretariat (secretariat@acica.org.au). Please note that hard copies will be required to be provided to ACICA once the office re-opens. Similar arrangements were made by the Vienna International Arbitral Centre (VIAC), https://www.viac.eu/en/news/availability-and-general-measures-undertaken-by-viac-in-times-of-covid-19; The Cairo Regional Centre for International Commercial Arbitration (the "CRCICA") https://crcica.org/NewsDetails.aspx?ID=120; London Court of International Arbitration (LCIA) https://www.lcia.org/lcia-services-update-covid-19.aspx <accessed on 7 April 2020>

[13] International Chamber of Commerce, https://iccwbo.org/media-wall/news-speeches/covid-19-urgent-communication-to-drs-users-arbitrators-and-other-neutrals/ <accessed on 7 April 2020>

[14] Adrianne Goins and Elena Guillet, The Advantages of Arbitration During the Coronavirus Pandemic, https://www.velaw.com/insights/the-advantages-of-arbitration-during-the-coronavirus-pandemic/ <accessed on 7 April 2020>

The confidentiality requirement in the institutional arbitration rules

The use of e-platforms, electronic filings and videoconferencing in arbitration proceedings has raised concerns over whether arbitration institutions and arbitrators are equipped to deal with the issues of cybersecurity and compliance with data protection during the COVID-19 pandemic; in particular most key arbitration institutions subscribe to the duty of confidentiality. In the case of the International Centre for Dispute Resolution (AAA/ICDR), Article 37 of the AAA/ICDR International Arbitration Rules imposes on arbitrators and the administrator the duty of confidentiality to keep all matters relating to the arbitration or the award confidential[15] unless otherwise agreed by the parties or required by applicable law.[16] This includes information revealed by the parties or the witnesses during the arbitration proceedings. Similar provisions can be seen in Article 4.18.2 of the ADRIC Arbitration Rules 2016, which requires the parties, the tribunal, the institution and any third parties attending any portion of the arbitral hearings or meetings to maintain their duty of confidentiality.[17] The requirement is subject to the parties' agreement,[18] a requirement made by a court,[19] by law,[20] or its necessary nature in connection with a judicial challenge to, or enforcement of, an award.[21] Similarly, Article 30(1) of the LCIA Arbitration Rules 2014 requires the parties and the institution[22] to undertake as a general principle to keep all awards confidential. The parties are also required to keep materials created for the purpose of the arbitration and all other documents which are not in the public

[15] Art 37(1), the AAA/ICDR International Arbitration Rules 2014, https://www.icdr.org/sites/default/files/document_repository/ICDR_Rules.pdf <accessed on 7 April 2020>
[16] Article 30, the AAA/ICDR International Arbitration Rules
[17] Article 4.18.2, the ADRIC Arbitration Rules 2016, The ADR Institute of Canada
[18] Article 4.18, the ADRIC Arbitration Rules 2016
[19] Article 4.18.2(a), the ADRIC Arbitration Rules 2016
[20] Article 4.18.2(c), the ADRIC Arbitration Rules 2016
[21] Article 4.18.2(b), the ADRIC Arbitration Rules 2016
[22] Article 30(3) of the LCIA Arbitration Rules 2014, London Court of International Arbitration. The provision provides: "The LCIA does not publish any award or any part of an award without the prior written consent of all parties and the Arbitral Tribunal."

domain and produced by another party in the proceedings confidential. Disclosure of such confidential information may be required of a party by legal duty, to protect or pursue a legal right, or to enforce or challenge an award in legal proceedings before a state court or other legal authority.[23] In Asia, an overarching duty of confidentiality over any recordings, transcripts, or documents used in relation to the arbitral proceedings shall remain confidential[24] and be imposed on all parties (the parties, a party and any arbitrator, including any emergency arbitrator, and any person appointed by the tribunal, including any administrative secretary and any expert) involved in arbitration administered by the Singapore International Arbitration Centre. In the region of Oceania, Article 22 of the Australian Centre for International Commercial Arbitration (ACICA) Rules 2016 requires the parties to secure the same level of the duty of confidentiality for the witnesses[25] attending the arbitration proceedings as those being imposed on the parties, the institution, and the tribunal.[26]

Cybersecurity and data protection during arbitration proceedings in the context of COVID-19

Given the duty of confidentiality and the sensitivity of most arbitrations, cybersecurity and data protection should be maintained throughout the proceedings. In early 2020, international efforts addressing this issue can be seen in four documents; namely the Seoul Protocol on Video Conferencing in International Arbitration (the Seoul Protocol), [27] the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration 2020 (the Cybersecurity Protocol),[28] the

[23] Article 30(1) of the LCIA Arbitration Rules 2014
[24] Article 24.4 of the SIAC Arbitration Rules 2016. The exceptions are listed in Article 39.2.
[25] Article 22.4, the ACICA Arbitration Rules 2016
[26] Article 22.2, the ACICA Arbitration Rules 2016
[27] 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 <accessed on 7 April 2020>
[28] http://documents.nycbar.org/files/ICCA-NYC-Bar-CPR-Cybersecurity-Protocol-for-International-Arbitration-Electronic-Version.pdf <accessed on 7 April 2020>

consultation draft of the ICCA/IBA Joint Task Force's Roadmap on Data Protection in International Arbitration (the Roadmap)[29] and the Delos checklist[30] on holding arbitration and mediation hearings in times of COVID-19. Among them, the Delos checklist mainly focuses on the logistical considerations involving in-person hearings, such as lockdown, proximity, travel restrictions, and the management of arbitration and mediation meetings during the COVID-19: hence, this article will focus on the remaining three documents, namely, the Seoul Protocol, the ICCA-NYC Bar-CPR Protocol and the ICCA/IBA Consultation.

The Seoul Protocol

Considering the global nature of dispute resolution and the practicalities surrounding the attendance of third parties and the advent of new powerful technologies, the Korean Commercial Arbitration Board International introduced this Protocol at the 7th Asia Pacific ADR Conference on 5-6 November 2018 and later published it as a guide to the best practice for planning, testing and conducting video conferences in international arbitration on 18 March 2020.[31] According to the Seoul Protocol, parties are allowed to make a request to the tribunal to use video conferencing at the hearing. The request has to be made at least 72 hours before the commencement of the hearing.[32] Once this has been agreed, a duty is imposed on the tribunal to ensure an effective, safe and fair use of video conferences for the arbitration proceedings.

Parties' responsibility to ensure the logistical and technological requirements and tribunal's duty to verify the identification of witnesses

[29] https://www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf <accessed on 7 April 2020>
[30] https://delosdr.org/wp-content/uploads/2020/03/Delos-checklist-on-holding-hearings-in-times-of-COVID-19-v2-as-of-20-March-2020.pdf <accessed on 7 April 2020>
[31] 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 <accessed on 7 April 2020>
[32] Article 9.1, the Seoul Protocol

According to Article 1, it is the parties who have the responsibility to ensure the logistical and technological requirements of the video conference attended by a witness. For instance, the parties are responsible for the quality and compatibility between the hardware and software used at the venues,[33] the connection between the hearing venue and the remote venue,[34] an on-call individual with adequate technical knowledge to assist in planning, testing and conducting the video conference,[35] fair, equal and reasonable right of access to the parties and their related persons in the choice of the venue,[36] liaison with the appropriate individuals[37] to carry out testing[38] and backup arrangements in the event that the video conference fails[39] as well as informing the appropriate individuals involved in the hearing of the backup plan.[40]

It also prescribes the set-up of the rooms where the witnesses are located. For instance, the witnesses shall give their evidence sitting at an empty desk or standing at a lectern with their faces being clearly visible.[41] Only video conferencing is allowed. People who are allowed to be in the same room as the witness are limited to their counsel, interpreters, paralegals to assist with the documents, and representatives from each party's legal team on a watching brief.[42] It is worth noting that each party shall provide information on the identities of every participant to the other party/parties to the tribunal prior to the video conference; however it is the

[33] Article 5.1, the Seoul Protocol suggests the minimum transmission speeds should not be less than 256 kbs/second, 30 frames/second, and the minimum resolution should be HD standard. The Hearing Venue should also be equipped with both ISDN and IP communication line capabilities and all Venues should be equipped with appropriate portable equipment in the event of unforeseen technical complications. Also see the requirement of a quality audio output device provided in Article 5.6.
[34] Article 2.1.a, the Seoul Protocol
[35] Article 2.1.b, the Seoul Protocol
[36] Article 2.1.c, the Seoul Protocol
[37] Article 9.1, the Seoul Protocol
[38] Article 6.1, the Seoul Protocol
[39] Article 6.2, the Seoul Protocol
[40] Article 9.4, the Seoul Protocol
[41] Article 1.3. Article 5.2, the Seoul Protocol: "There shall also be adequate placement and control of the cameras to ensure that all participants can be seen."
[42] Article 3.1

tribunal's responsibility to take steps to verify the identity of each individual present at the start of the video conference.[43] Arrangements must be made for a sufficient number of microphones[44] and a computer with email facilities and a printer at the venue.[45] An agreed translation of the oath administered should be in place.[46] The tribunal can terminate the session if it deems the video conference so unsatisfactory that it has concerns over fairness to either party.[47]

Cybersecurity

Safeguards against unlawful interceptions by third parties[48] and the security of the participants in the video conferencing, including the witnesses, observers,[49] interpreters,[50] experts, document repository … and so on, are to be provided by the parties. The use of ISDN or IP communication lines is strongly recommended. Where the parties agree to use a web-based video conferencing platform, the venue should provide a sufficiently large screen that can project the video transmission displayed through the video conferencing solution and ensure that the Ethernet or wireless internet connection is secure and stable throughout the proceedings.[51]

Transmission of data

[43] Article 3.1
[44] Articles 5.2 and 5.4
[45] Article 1.5
[46] Article 1.6
[47] Article 1.7
[48] Such as by IP-to- IP encryption
[49] An observer means any individual who is present in the Venue other than the Parties, Tribunal, Witness, interpreter, as described in Article 3
[50] Article 9.3, the Seoul Protocol requires the appointing party of the witness to brief the interpreters about the Protocol and the arrangements for video conferencing to allow adjustment of their interpretation service.
[51] Article 5.5, the Seoul Protocol

Over and above the requirements of clearly identified and paginated document(s) the witness will refer to during their evidence session,[52] the party has a duty to supply an unmarked copy of the Agreed Bundle of Documents to the tribunal.[53] Both parties have to agree to a shared virtual document repository (i.e. document server) to be made available via computers at all venues, provided that the parties use their best efforts to ensure the security of the documents.[54]

Due to the private nature of arbitration, no recording shall be allowed with the exception of the tribunal's leave.[55] In the event that the recording is allowed, the recording must be forwarded to both the tribunal and the parties.[56]

Under the Seoul Protocol, the requesting parties bear most responsibility for the arrangements of video conferencing. Their responsibility is supplemented by the tribunal's duty to verify the identifies of the individuals attending the video hearings to deliver a fair, equal and reasonable arbitration proceedings. A few points worth exploring include: the practicality of the Seoul Protocol in the event of lockdown during COVID-19, the venue's duty to deliver a secure and stable internet connection throughout the proceedings, the issues of recording and data transmission, and allocation of responsibility. As the Korean Commercial Arbitration Board pointed out, it is clear that the Seoul Protocol was not released in response to the COVID-19 pandemic but was a collective effort among the arbitral community to address the issues arising from the use of video conference and data transmissions in international arbitration in general. Consequently, the guidance provided in the Seoul Protocol is not practical in the event of lockdown where public gathering and social distancing are used as the main means to slow down the spread of COVID-19 in most jurisdictions.

[52] Article 4.1, the Seoul Protocol
[53] Article 4.2, the Seoul Protocol
[54] Article 4.3, the Seoul Protocol
[55] Article 8.1, the Seoul Protocol
[56] Article 8.2, the Seoul Protocol

In relation to the venue's duty to provide a stable internet connection, issues may arise in the practice of using multiple venues under the Seoul Protocol. During normal times, it would be difficult to establish any venue's liability in the case of a failure / slowdown of internet connection where multiple carriers and venues can be involved; let alone the high demand for an internet connection during the COVID-19 period. Moreover, the prohibition of recording of hearings without the tribunal's leave would make it difficult for the parties or the tribunal to police activities in the modern time when covert filming or recording can be carried out with a click of a button on a smart phone. Under the Seoul Protocol, the concerns over data protection and the allocation of responsibility among the parties, the legal counsels, the tribunal and the arbitration institution (if applicable) are not addressed in the context of collecting, holding, managing and transmitting personal and sensitive data arising from the use of video conferencing. Finally, requiring the parties to bear most of the responsibility may be justified in an *ad hoc* arbitration; nevertheless, what could be the rationale behind such a high level of responsibility imposed on the parties in an institutional arbitration? Would it be fair for the parties to bear the responsibility and pay for the services of an institutional arbitration? On the point of institutional arbitrations, instead of using web-based platforms which have recently come to the scrutiny of their data protection policy,[57] should it be the arbitral institution's responsibility to deliver a platform using ISDN or IP communication lines in order to ensure cybersecurity and data protection?

The ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration

[57] For instance, Zoom's security problems (e.g. zoombombing) have been highlighted in https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives, https://www.cnet.com/news/zoom-every-security-issue-uncovered-in-the-video-chat-app/, https://www.bbc.co.uk/news/technology-52133349 <accessed on 7 April 2020>

The 2020 Cybersecurity Protocol for International Arbitration was announced on 21 November 2019.[58] It is intended to provide a framework determining the reasonable information security measures and to increase awareness about information security for individual arbitration matters. The Protocol suggests that adherence to the Protocol may comply with a global trend in providing data protection to individuals; nevertheless, its compliance is not meant to supersede applicable legal or other binding obligations.[59] Consequently, it left the full compliance to the forthcoming Roadmap to Data Protection in International Arbitration Proceedings by the ICCA/IBA Joint Task Force on Data Protection in International Arbitration Proceedings.[60]

Framework

Instead of placing the major burden on the parties as the Seoul Protocol does, the Cybersecurity Protocol establishes a framework which distributes responsibilities among "each" party, the tribunal and the administering institution in their considerations of cybersecurity and data protection. The parties, the tribunal and the administering institution are defined as the custodians of arbitration-related information and are required to implement effective information security and adopt reasonable information security practices.[61] All of them are required to follow the standard of reasonableness in their consideration,[62] considering what information security measures are reasonable to apply to a particular arbitration matter,[63] the

[58] Forward, The Cybersecurity Protocol
[59] Principle 4, The Cybersecurity Protocol, page 1
[60] Forward, The Cybersecurity Protocol
[61] Principle 2, The Cybersecurity Protocol
[62] Principle 5, The Cybersecurity Protocol
[63] Principle 1, The Cybersecurity Protocol

baseline information security practices and the impact of their own information security practices on the arbitration,[64] ensuring that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.[65] Both the parties and the tribunal are required to consider the factors of asset management, access controls, encryption, communications security, physical and environmental security, operations security and information security incident management in their decision on the information security measures applied to an arbitration.[66] Matters to be considered by the parties and the tribunal include the risk profile of the arbitration,[67] the existing information security practices, infrastructure, capabilities of the parties,[68] the burden, costs, and the relative resources available to any party, any arbitrator and any administering institution,[69] proportionality relative to the size, value, and risk profile of the dispute[70] and the efficiency of the arbitral process.[71] Risk assessment of information exchanges and transmission of arbitration-related information, storage of arbitration-related information, travel, hearings and conferences and post-arbitration retention and destruction policies should allow for flexibility in tailoring the information security measures.[72]

Information security

The Cybersecurity Protocol is designed to raise the awareness of risks involved in using and transmitting information used in arbitration proceedings. It is important to raise awareness of

[64] Principle 2, The Cybersecurity Protocol
[65] Principle 3, The Cybersecurity Protocol
[66] Principle 7, The Cybersecurity Protocol
[67] Principle 6(a), The Cybersecurity Protocol
[68] Principle 6(b), The Cybersecurity Protocol
[69] Principle 6(c), The Cybersecurity Protocol
[70] Principle 6(d), The Cybersecurity Protocol
[71] Principle 6(e), The Cybersecurity Protocol
[72] Principle 8, The Cybersecurity Protocol

the risks among those involved in arbitration proceedings. They should also be made aware of some of the readily accessible information security measures available to improve everyday security practices.[73] The scope of "information security risks in the arbitral process"' covers both cybersecurity and physical security risks. The importance of information security is highlighted as the key to the users' confidence in the overall arbitral regime conducted over the internet connection.[74]

It is suggested that the parties should attempt in the first instance to agree on reasonable information security measures after taking the factors listed in Principles 6-8 into consideration.[75] The agreement should be reached as early as possible; no later than the first case management conference.[76] The potentially unexpected evolving circumstances of the case allow the tribunal to exercise its power to modify the agreed measures.[77] Such modification can be carried out by the tribunal on its own initiative, or at the request of any party.[78] In the absence of parties' agreement, the tribunal will consider Principles 4-9 on the applicable laws/rules/codes, reasonable standards / measures and determine the information security measures applicable to the arbitration within its authority.[79] Differently from the Seoul Protocol, the Cybersecurity Protocol addresses the issues of costs involved in setting up the reasonable information security required for the arbitration process and the consequences of breaching of such measures. According to Principle 13, the tribunal has the discretion to allocate the relevant costs among the parties and, in the event of breach, impose sanctions on the parties.

[73] Forward, The Cybersecurity Protocol
[74] Forward, The Cybersecurity Protocol
[75] Principle 9, The Cybersecurity Protocol
[76] Principle 10, The Cybersecurity Protocol
[77] Principle 12, The Cybersecurity Protocol
[78] Principle 12, The Cybersecurity Protocol
[79] Principle 11, The Cybersecurity Protocol

Compared to the Seoul Protocol, the Working Group of the Cybersecurity Protocol made an attempt to provide more detailed recommendations on data protection in the context of Europe, Canada and the USA.[80] As the Working Group pointed out, data security has dominated every aspect of the European business and individuals since the introduction of the General Data Protection Regulation (GDPR)[81] on 24 May 2016, later fully implemented among the Member States on 25 May 2018. Similar regulations with the equivalent legal requirements have been implemented in the USA, Brazil and Canada. They are: the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the California Consumer Privacy Act in the United States, the General Data Protection Law in Brazil, and the Personal Information Protection and Electronic Documents Act ("PIPEDA") in Canada.[82]

While the Working Group pointed out that personal data protection regimes vary from jurisdiction to jurisdiction, it expects the parties, the tribunal and the arbitration institution to work in collaboration to address the "concepts of 'reasonableness', 'adequacy', 'appropriateness', and 'proportionality' … applied, as the interpretation of these terms may differ under various legal regimes."[83] The tribunal is also expected to consult both the parties and any administering arbitration institution to work out the best way to harmonise and

[80] The members of the Working Group are mainly from North America, UK and Europe; such as the UK, Belgium, Canada, USA and France
[81] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 <accessed on 7 April 2020>
[82] Commentary to Principle 4, The Cybersecurity Protocol Page 14
[83] Commentary to Principle 4, The Cybersecurity Protocol Page 14

implement data protection obligations by observing the principles of proportionality and due process.[84]

Consequently, the Working Group highlights the important role played by the arbitration institutions which are burdened with a shared duty to comply with the local data protection requirements. The Working Group succinctly puts it that, "[d]epending on the sensitivity of the information involved in a particular arbitration or the nature of applicable legal obligations, coordination with the institution may be necessary at the time the arbitration is commenced or in some cases even before."[85] Therefore, in the case of an institutional arbitration, "it may be necessary for the parties, their representatives, and the arbitral tribunal to consult and coordinate with that institution prior to adopting information security measures in order to ensure that proposed measures are consistent with, and can be implemented pursuant to, the institution's rules, practices, technical capabilities, and legal obligations. In some cases, the legal obligations of an administering institution (for example, under data protection law) may impact what information security measures are adopted by the parties and tribunal."[86] Considering the international background of arbitrators and the parties, the consultation and coordination between them and the institutional arbitrations will lessen their burdens in their compliance with data protection and cybersecurity.

However, the parties involved in an *ad hoc* arbitration will not be shielded by the co-ordination suggested in the Cybersecurity Protocol as it does not seem to cater for *ad hoc* arbitration.

[84] Commentary to Principle 4, The Cybersecurity Protocol Page 15
[85] Commentary to Principle 4, The Cybersecurity Protocol Page 15
[86] Commentary to Principle 4, The Cybersecurity Protocol Page 15

Consequently, the parties involved in an *ad hoc* arbitration will fall into the same situation under the Seoul Protocol where the parties bear most of the burden and costs in implementing the measures as well as the risk in breaching the relevant data protection regulations and the duty of confidentiality, if applicable. The personal data used in arbitration with a European element is subject to the restrictions imposed by the GDPR. The complexity associated with the GDPR should not be under-estimated by any international arbitrator, any party, or any arbitration institution and their legal counsels. Its complexity can be seen in the detailed provisions on, and not limited to, personal data,[87] processing of data,[88] data controller,[89] filing system,[90] processor,[91] data protection officer,[92] recipient,[93] consent,[94] right to withdraw,[95] right of access by the data subject,[96] right to erase (right to be forgotten),[97] cross-border processing,[98] data protection impact assessment,[99] right to data portability,[100] transfer of personal data to third countries or international organisations,[101] and remedies available to the data subject in their right to lodge a complaint with a supervisory authority,[102] right to an effective judicial remedy against a supervisory authority,[103] and right to an effective judicial remedy against a controller or processor.[104]

[87] Articles 4(1), 4(12), 13 and 14, the GDPR
[88] Articles 4(2), 29, 30 and 32, the GDPR
[89] Articles 4(7), 24, 26 and 27, the GDPR
[90] Article 4(6), the GDPR
[91] Article 4(8) and 28, the GDPR
[92] Articles 37, 38, 39, the GDPR
[93] Article 4(9), the GDPR
[94] Article 4(11), the GDPR
[95] Article 13(2) (c) and Article 14(2)(d), the GDPR
[96] Article 15, the GDPR
[97] Articles 5(1)(d) 17(1)(d), 17(1)(e), 17(2), the GDPR
[98] Articles 4(23), 9(2)(i), 56(1) and 56(4), the GDPR
[99] Articles 35, 36 (1), 36(3)(e), 39(1)(c), 57(1)(k) and 64(1)(a), the GDPR
[100] Article 13(2)(b), 14(2)(c) and 20, the GDPR
[101] Articles 44, 45 and 46, the GDPR
[102] Article 77, the GDPR
[103] Article 78, the GDPR
[104] Article 79, the GDPR

Reflecting the requirements of the GDPR on an *ad hoc* arbitration which requires the parties to make arrangements related to cybersecurity and data protection, the immediate questions would be who the data subject, data controller, data processor are, what their rights and obligations are, what remedies are available to them, whose responsibility it is to carry out a data impact assessment and how cross-border data transferring should be dealt with. Perhaps, one has to enquire whether the parties, or indeed international arbitrators are equipped with the knowledge and capacity to ensure the level of cybersecurity and data protection required for hearings or meetings carried out remotely. What if the arbitrator or the parties are from a jurisdiction with a lower standard of data protection and cybersecurity regulation? In the case of conflicting regulations on data protection and cybersecurity, is the tribunal expected to exercise its authority and choose the higher standard of information security measures to be applied to the arbitration? Under the "business as usual" approach, arbitration carries on and parties have to engage with the process to implement the reasonable cybersecurity measures which they did not expect when arbitration was chosen as the method of dispute resolution. COVID-19 increases the parties' legal liability and the risk in the event of breach of the regulations. If there is a failure to carry out or continue with arbitration, the parties risk the lapse of the time limit prescribed and lose their rights to pursue their claims or counter-claims. Carrying on with arbitration proceedings remotely, failing to fulfil the requirement of reasonable cybersecurity measures for remote hearings or meetings, parties endure the risk of civil and criminal sanctions under the GDPR. Among the arbitration institutions, the tribunal and the parties, perhaps, the parties who receive little exposure to data protection training and / or have little capacity to implement cybersecurity will find themselves in a no-win situation.

The ICCA/IBA Joint Task Force's Roadmap on Data Protection in International Arbitration

The Roadmap is still in its draft consultation form.[105] It focuses on data protection and contains more details than the Seoul Protocol and the Cybersecurity Protocol to "help arbitration professionals better understand the data protection and privacy obligations to which they may be subject in relation to international arbitration proceedings."[106] Due to the potential civil[107] and / or criminal liability triggered by non-compliance with the mandatory application of the GDPR, the ICCA-IBA Task Force highlighted the need for the arbitration professionals to "consider what data they process, where, by what means, with which information security measures and for how long."[108] The Roadmap focuses on the impact of the mandatory application of the GDPR on international arbitration and addresses how data protection laws may apply to the steps of the arbitration process and documents and measures adopted at the different stages of an arbitration.

The Task Force correctly highlights the cross-border nature of international commercial arbitration, the sensitivity of the data used to deliver dispute resolution and the involvement of multiple people and organisations as the key difficulties faced by the arbitration professionals and the parties in their attempt to comply with the data protection regulations. Among them, the cross-border issue adds to the complexity arising from the material and jurisdictional scope of the relevant law. Despite the acknowledgement of different requirements imposed by the different regulations, the Task Force places its emphasis on the steps taken by the arbitration professionals and the parties before, during and after the arbitration proceedings in order to comply with the data protection regulation(s). Such an approach delivers a more detailed

[105] As *The ICCA/IBA Joint Task Force's Roadmap on Data Protection in International Arbitration* expressed "not for citation", this part of the article will not refer to the individual pages for citation but only highlight the key considerations the arbitration professionals should have in their compliance of data protection regulation(s)
[106] Page 1, The Road Map
[107] The potential fines of 4% of overall global incomes or EU20 millions (whichever is higher) under the GDPR.
[108] Page 1, The Road Map

document in information processing and transmission, and a better understanding of the dual capacities of all parties involved in arbitration, data transfer rules and data protection principles, making it a complement for the Cybersecurity Protocol.

Information processing and transmission

The Task Force points out that all arbitral participants must have a good awareness that a substantial portion of the information exchanged during a typical international arbitration is likely to contain data. This data is very likely to fall into the scope of personal data, relating to an individual who is identified or identifiable, and to be regulated by the relevant legislation. Because of personal data used in international arbitration, it is important to understand that all parties' active steps such as collecting, using, disseminating and deleting data and passive operations such as receiving, holding, organising and storing data are categorised as processing in the data protection law. Both transmission and processing data in international arbitration will trigger the extraterritorial application of the GDPR to an arbitration. All parties should have reasonable security measures in place and be prepared to deal with the conflicting of regulations involving cross-border data transferring in international arbitration.

Dual capacities under arbitration and data protection regulations

In a typical international arbitration, parties, tribunal members, arbitration institutions and third parties working for or on behalf of the parties, tribunal and legal counsels all have their roles, rights and duties laid down in the laws applicable to the arbitration. However, in the context of data protection, all parties will also be defined differently and have different roles and

capacities imposed in accordance with the activities and tasks being carried out during the process. The Task Force stressed that the process of an international arbitration can deliver multiple data controllers. According to Article 4(7) of the GDPR, the parties, the arbitration institutions and the tribunal members, legal counsels and law firm employees can be defined as a data controller or joint data controllers.[109] Depends on the activities, each individual may have a joint or different responsibility to ensure the protection of personal data.

Reviewing the arbitration process, the Task Force also pointed out that tribunal secretaries, e-discovery professionals, transcribers, interpreters and other vendors may be considered as data processors when they deal with the tasks delegated by the tribunal members, the parties and the arbitration institution. The data processor's responsibility will depend on the sources of direction given in relation to the purposes and the means of the processing and the revocation of the right to process.

Data transfer rules and principles

Once each individual recognises their role under the data protection regulation, all arbitral participants would be better placed to increase awareness of lawfulness and minimisation of data in data transferring rules required under the GDPR; in particular transmission of personal data across borders. The data controllers must be aware of the restrictions on data transfers between jurisdictions under the GDPR and ensure that no transfer can take place without a lawful basis. Before the transmission, they also have to (1) ascertain the standard of data

[109] Article 4(7) of the GDPR: "A '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 (Art. 4(7) GDPR).

protection of third countries so their legal obligations are not circumvented by the transfer of data to jurisdictions where the standard of protection of personal data is lower, (2) minimise the data to be transferred by culling for relevance, redaction or pseudonymisation of personal data, (3), if applicable, enter into confidentially provisions to safeguard the data and (4) notify the data subjects *and* the supervisory authority about the transfer. Over and above this, the Roadmap contains the common nine principles of data protection regulation. They are: fair and lawful processing, proportionality, data minimization, purpose limitation, observing the data subject's rights, data accuracy, data security, transparency and accountability.

In the context of international arbitration, the Roadmap highlights that it is essential to ensure that the data subjects understand how their data is collected, processed and used. The data subjects should also be advised of their rights, such as rights to be erased, the specific and legal purpose of the data collection and processing, and the notice of transferring data. The arbitral participants falling into the categories of data controllers, joint controllers and data processors must process witness data, data contained in the documentary evidence, sensitive data or criminal data in a legal manner. Factors such as the rights and interests of the data subject, the rights and interests of parties to the arbitration, those of third parties and the need for a fair and efficient administration of justice should be taken into consideration in terms of data protection and cybersecurity measures. The arbitral participants have to ensure that minimised but adequate information in case preparation, claims, counter-claims, defence, administrative matters, witness statements is processed and transferred lawfully and fairly.

The arbitral participants should also ensure the accuracy of the data and implement appropriate / reasonable security measures to protect it. To ensure transparency and accuracy of the data, the data subject's right to information must be observed by the arbitral participants. In the case

where overlapping notices are required to be sent to the data subject, arbitral participants need to find out whether such a requirement can be exempted under the GDPR if they did not originally collect the data from the data subject. The data subjects may seek to exercise their rights under data protection regulations to prevent data from being used in the arbitration or obtain access to processed data during the arbitration proceedings. Consequently, the arbitral participants should also contemplate the possibility of receiving such requests and consider the impact this may have on confidentiality, privilege and arbitration in general.

Concluding remarks

Although the timing is a pure coincidence, the Seoul Protocol, the Cybersecurity Protocol and the Draft of the Roadmap are not intended to address the current arbitration practice affected by COVID-19. However, all three documents demonstrate that cybersecurity and data protection in international arbitration are a live issue which must be dealt with by the arbitration professionals during COVID-19 and beyond. Since it is business as usual for arbitration during COVID-19 remote hearings, the show has to go on with remote hearings and meetings that are actually taking place. The Seoul Protocol falls short on the imbalanced responsibility and costs imposed on the parties. Due to the complexity of surrounding data protection and data transferring across borders, the general guidance issued in the Seoul Protocol and the Cybersecurity Protocol must be supplemented by the Roadmap to enable the international arbitral participants to appreciate the necessity of engaging with the relevant local data protection standards and the requirements imposed on the different players in the international context.

However, data protection varies from jurisdiction to jurisdiction. The Roadmap suggested the practice of a GDPR compliant data processing agreement to ensure full compliance with data

protection and cybersecurity among the arbitral participants. However, the difficulty in securing such an agreement is inherent in the nature of international arbitration. To sum up, reflecting the different operations of international arbitration upon the local data protection laws will enable the arbitral participants, institutional or *ad hoc* arbitration, to follow the legal requirements in data collection and management as well as ensure legitimate data transferring which complies with cybersecurity and data protection in the modern world.