Intersecting and Dissecting Confidentiality and Data Protection in Online Arbitration

Mo Egan* and Hong-Lin Yu**

INTRODUCTION

Confidentiality and data protection are distinct legal obligations but often intersect in online arbitration. For example, where there is an obligation of confidentiality, measures taken to secure data protection may be used as evidence of compliance should there be an assertion that there has been a breach of confidentiality. Yet, the fact that data protection measures have been implemented does not automatically mean that a breach of confidentiality has not taken place. There are data protection obligations that far exceed the requirements of confidentiality or, indeed, conflict with that obligation. This is because confidentiality could be achieved provided information has been kept confidential; whereas data protection has two strands of obligations, those that seek to protect personal data and those that seek to provide access and control over data.

While the consequences of a breach of confidentiality include orders preventing further disclosures or damages,[1] the consequences of data protection breaches vary in different jurisdictions with the possibility of administrative, civil and criminal penalties. Of particular note, the EU General Data Protection Regulation (hereinafter GDPR) introduced a selection of financial penalties that has garnered practitioner attention in the field of arbitration.[2] Not only do individuals have a right to compensation for both material and non-material damage as a result of breaches of the regulation, but also, controllers and processors of data can be fined by Supervisory Authorities for breaches of the regulation where no damage has resulted.[3] These administrative fines are substantial with the regulation dictating that fines can range from 10,000 Euro to 4% of the total worldwide annual turnover of an undertaking of the preceding financial year.[4] Significantly, the higher penalties are applicable where the breach relates to infringements of an individual data subject's rights or an infringement of the measures restricting transfer of data.[5] However, many of those who partake in online arbitration are likely to be subject to both a duty of confidentiality and data protection, presenting tensions.

*Dr Mo Egan, Lecturer in Law, University of Stirling, UK; ** Dr Hong-Lin Yu, Reader in Law, University of Stirling, UK

[1] Ileana M. Smeureanu, *Confidentiality in International Commercial Arbitration*, (Kluwer Law International 2011) 161, 161-184. *Ali Shipping Corporation v Shipyard Trogir* [1998] 2 All E.R. 136; [1998] 1 Lloyd's Rep. 643, *John Foster Emmott v Michael Wilson & Partners Limited* [2008] EWCA Civ 184

[2] Martin Zahariev, 'GDPR Issues in Commercial Arbitration and How to Mitigate Them', September 7 2019, Kluwer Arbitration Blog. Available at: <http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/> accessed 25 September 2020.

[3] arts.82(1) and 83(4)–83(5), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*),* OJ L 119, 4.5.2016, 1–88 (hereinafter GDPR).

[4] arts.83(4)–83(5), GDPR. The UK Supervisory Authority, the ICO fined Marriott International £99 million (July 2019) and Cathay Pacific £500,000 (March 2020) for failing to protect personal data in cyberattacks.

[5] art.83(5)(b)(c) GDPR.

The intersection of confidentiality and data protection can see clashes in (1) the contractual duty of confidentiality and data protection obligations and (2) the statutory duties of confidentiality and data protection. In the former case, though the statutory duty of data protection is likely to prevail, the various scope of the contractual duty of confidentiality demands a robust approach to data protection to avoid any breach. In the latter case, the relationship between the competing statutory duties requires further consideration. Indeed, to reconcile the competing duties in both categories, it is essential to ascertain the interactions between the exceptions to both duties.

The duty of confidentiality provided by arbitration institutions and data protection legislation are by no means harmonised. Therefore, the current research is limited to an examination of international institutional arbitration, how the duty of confidentiality is imposed by the parties' confidentiality agreement, arbitration institutional rules and applicable laws upon the arbitration institutions, arbitrators, parties, experts and witness and considers whether these rules can be overwritten by the legal data protection requirements imposed on these partakers in the transmission of data. The EU data protection framework[6] is commonly recognised for its extraterritorial reach, making the EU provisions of greater international significance and consequently the focus of this paper.[7] Although one can analyse the consequences of that extraterritorial reach in general terms, it is more constructive to consider the interaction with specific arbitration centres from outside the EU. Moreover, since the Court of Justice of the European Union has invalidated the previous adequacy decision in relation to the EU-US Privacy Shield, it is now important to consider the implications of this decision in the arbitration context.[8] To draw out these issues three arbitration institutions, the International Chamber of Commerce (hereinafter "ICC"), the London Court of International Arbitration (hereinafter "LCIA") and the International Centre for Dispute Resolution (hereinafter "ICDR") are chosen for the case study given their significance in international arbitration.

The aim of this research is to highlight how the obligations of confidentiality and data protection can intersect and dissect in online arbitration. The researchers will outline the variations in the scope of the duty of confidentiality imposed on the individuals partaking in the international institutional arbitration. Their anticipated roles in maintaining confidentiality, privacy and data safety in online arbitration will be the focus of this research. This paper will firstly, set out the latest developments in practitioner engagement with digitisation, address measures developed and proposed by the practitioner community before addressing specifically the intersection of the legal obligations of confidentiality and data protection. It will be followed by the examination of the limited awareness of data protection in online arbitration. The research will be furthered by providing a detailed study of the duty of data protection and how the duty can impact on the partakers' involvements in online arbitration. The practice of the ICC, the LCIA and ICDR will form the case study on how both duties

[6] The relevant provisions in the EU are: art.7 (Right to Privacy) and art.8 (Right to Data Protection) The Charter of Fundamental Rights; GDPR (n3) and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89–131(hereinafter Directive 2016/680).

[7] See Symposium on extraterritoriality in EU data protection law, Special Issue (2015) 5(4) *International Data Privacy Law* <https://doi.org/10.1093/idpl/ipv025> accessed 25 September 2020.

[8] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*.

intersects. The research will finally highlight that raising awareness of the competing duties borne by the partakers in online arbitration is the key to full compliance.

THE RISE OF DIGITALISATION OF INTERNATIONAL ARBITRATION WHERE CONFIDENTIALITY AND DATA PROTECTION INTERSECT

COVID-19 brought the world to a standstill. Following the United Kingdom (hereinafter "UK") Parliament's introduction of the Coronavirus Act 2020[9] on 25 March 2020, the UK Courts and Tribunals Service (hereinafter "HMCTS") significantly reduced its capacity and operation. Nevertheless, the arbitration community reacted very differently to the COVID-19 crisis. The arbitration institutions see the standstill as an opportunity to review its current practice and adopt the online dispute resolution platform. They also see necessity as the mother of invention allowing the fast acceleration of digitalisation of international arbitration process.[10] During this process, one saw the use of electronic means of communications, such as website and telephone,[11] email and telephone,[12] facsimiles and email,[13] a secure and encrypted email communication,[14] unencrypted email communication,[15] for the communication between the arbitration institution, the tribunal, parties and non-parties involved in arbitration. For the filing of any written submissions,[16] encrypted email option,[17] portal,[18] email and the secure online file- sharing platforms[19] for data transmission may be used when the traditional physical service of document is suspended by arbitration institutions.[20] For hearings, most arbitration institutions stopped or postponed in-person hearings[21] or advised against the use of institutional facilities for in-person hearings[22] and encouraged the use of alternative hearing arrangements, such

[9] Coronavirus Act 2020.

[10] COVID-19: Institution and Organisation Specific Proposals as at 23 April 2020 <https://hsfnotes.com/arbitration/wp-content/uploads/sites/4/2020/04/COVID-19-Institution-and-Organisation-Proposals-23_04_2020-HSF-Arbitration-Notes.pdf> accessed 25 September 2020.

[11] American Arbitration Association - International Centre for Dispute Resolution (AAA-ICDR), Financial Industry Regulatory Authority, Inc. (FINRA) for communications, Judicial Arbitration and Mediation Services (JAMS).

[12] Australian Centre for International Commercial Arbitration (ACICA), Asian International Arbitration Centre (AIAC).

[13] Singapore International Arbitration Centre (SIAC).

[14] International Institute for Conflict Prevention & Resolution (CPR).

[15] Dubai International Arbitration Centre (DIAC), German Institute of Arbitration (DIS), Hong Kong International Arbitration Centre (HKIAC), International Chamber of Commerce (ICC), International Dispute Resolution and Arbitration and Mediation Centre (IDRC), London Court of International Arbitration (LCIA), London Maritime Arbitrators Association (LMAA).

[16] Cairo Regional Centre for ICA (CRCICA), Dubai International Financial Centre-London Court of International Arbitration (DIFC-LCIA), Hong Kong International Arbitration Centre (HKIAC), Vienna International Arbitral Centre (VIAC).

[17] CPR (n14).

[18] FINRA (n11) for documents.

[19] International Centre for Settlement of Investment Disputes (ICSID), Arbitration Institute of the Stockholm Chamber of Commerce (SCC), ICC (n15).

[20] AIAC (n12), CPR (n14), DIAC (n15) but DIS (n15) required hard copy.

[21] In-person hearings are either cancelled, postponed or replaced by virtual hearings in the cases of CPR (n 14), DIS (n15), FINRA (n11) and AAA-ICDR (n11).

[22] AAA-ICDR (n11).

as remote hearings[23] with the institutional assistance. This includes the use of video teleconferencing[24] or an online dispute resolution software platform[25] that utilises the IP-based[26] or cloud-based[27] remote participation in hearings. And so, the gathering pace of the digitalisation of international arbitration proceedings demands scrutiny of the compliance of confidentiality in arbitration and data protection measures.

Cross-border online arbitration has its own challenges in meeting the duites of confidentiality and data protection. Different geographic locations lead to the transmission of audio / video images recordings during the hearing and transmission of documentation submitted across borders. The issue is exacerbated further as audio clips, video images and documentation generated for the arbitration proceedings may contain confidential information and sensitive personal data which allows the data subjects to be identified. Consequently, the compliance of the duty of confidentiality in arbitration and data protection in the digitalisation of arbitration proceedings intersect.

With the development of online arbitration accelerating as a result of COVID-19 there is a greater potential for ad hoc arrangements that do not satisfy either obligations of confidentiality nor the requirements of data protection. While COVID-19 may have been the stimulus, the direction of travel has been towards greater engagement with technology facilitated dispute resolution for some time. Yet, the participants' awareness of cybersecurity, data protection compliance and understanding of their roles in a digitalised arbitration becomes essential to avoid any breach of obligations. With the increasing use of e-filing, audio/videoconferencing, and email communications in arbitration proceedings, data protection becomes an eminent issue. Still, it appears that the appeal of online arbitration is set to flourish and therefore there is a need to examine more fully the issues presented to data protection and confidentiality compliance.

Confidential Information and Data in Arbitration

Confidentiality is often highlighted as one of the main advantages and reasons why the parties have chosen arbitration as the means of resolving commercial disputes. [28] Confidentiality was also identified as a significant issue corporations would consider in the parties' negotiation stance. Prior to the events of digitalisation and COVID-19, 27% of the surveyed corporations in the White & Case / QMUL Report 2010 indicated that confidentiality is a deal-breaker which they would never be willing to concede. However, 52% of them indicated that it is a key issue and only willing to re-consider if it is necessary.[29]

[23] AAA-ICDR (n11), AIAC (n12), ICC (n15), ICSID (n19), IDRC (n15), SIAC (n13) and VIAC (n16).

[24] Virtual hearings and meetings are allowed in CRCICA (n16), DIAC (n15), DIFC-LCIA (n15), HKIAC (n16). Both Korean Commercial Arbitration Board (KCAB) and LMAA (n15) use Zoom for lower value claims.

[25] ACICA and AIAC (n12) uses ADC Virtual, an online dispute resolution (ODR) software platform. ICSID (n19), telephone is allowed when the internet connection is poor.

[26] LMAA (n15), ACICA, AIAC (n12), ICSID (n19).

[27] HKIAC (n16) uses virtual hearing services; IDRC (n15) uses an integrated platform; JAMS (n 11) and LMAA (n 15) uses Zoom; SCC (n 19) where audio and visual meeting facilities are encouraged.

[28] Filip De Ly, Mark Friedman, Luca Radicati Di Brozolo, International Law Association International Commercial Arbitration Committee's Report and Recommendations on 'Confidentiality in International Commercial Arbitration' (2012) 28(3) Arbitration International 355, 356; Reza Mohtashami and Sami Tannous, Arbitration at the Dubai International Financial Centre (2009) 25(2) *Arbitration International* 173; Leon E. Trakman, Confidentiality in International Commercial Arbitration (2002) 18(1) Arbitration International 1, 1-5 and 11.

[29] Paul Friedland and Loukas Mistelis, *2010 International Arbitration Survey: Choices in International Arbitration*, 7

This widely acknowledged characteristic has led the parties to believe that they can keep their disputes from the gaze of the outside world and potential court proceedings at the enforcement stage. However, "keeping disputes from the gaze of the outside world" is more related to privacy which excludes third parties from accessing the arbitration proceedings. Privacy and confidentiality are two different concepts[30] in arbitration. As Collins, Paulsson and Rawding[31] have pointed out, some literature confusingly used the terms inter-changeably[32] when they make reference to the advantages of arbitration. Strictly speaking, privacy refers to access to arbitration proceedings only. Whereas, confidentiality refers to the information used or stated during the proceeding which should be kept confidential and not be revealed to people who are not involved in the arbitration proceedings.

Empirical research of the 50 jurisdictions that offer the duty of confidentiality has demonstrated that the scope of confidential information varies.[33] The possible information which can fall into the scope of confidentiality includes information pertaining to the arbitral process itself and the documents and other materials which are part of the arbitration, the documents, evidence and information which were used, introduced and disclosed in arbitration proceedings.[34] For instance, rule 26(4) of the Scottish Arbitration Rules contained in the Arbitration (Scotland) Act 2010 prescribes that confidential information includes any information which is not and has never been in the public domain but relating to, (a) the dispute; (b) the arbitral proceedings; (c) the award; or (d) any civil proceedings relating to the arbitration in respect of which an order has been granted under s.15 of the Act (anonymity in legal proceedings). Both section 2 of the New Zealand Arbitration Act 1996 and section 15 (1) of the Australian International Arbitration Act 1974, amended in 2018 define confidential information as (i)the statement of claim, statement of defence, and all other pleadings, submissions, statements, or other information supplied to the arbitral tribunal by a party: (ii) any evidence (whether documentary or otherwise) supplied to the arbitral tribunal: (iii) any notes made by the arbitral tribunal of oral evidence or submissions given before the arbitral tribunal: (iv) any transcript of oral evidence or submissions given before the arbitral tribunal: (v) any rulings of the arbitral tribunal. Although the scope of confidential information appears to be wider than the personal data protected under the EU framework, the personal data can be scattered in various categories of confidential information defined above. Yet, context is everything.

Awareness of Cybersecurity and Data Protection in The Digitalisation of International Arbitration

The arbitration community has steadily adopted new technologies to assist in the resolution of disputes.[74] The COVID-19 pandemic provides the arbitration community the best opportunity to move the practice into a virtual world. For example, it has become fairly commonplace for case management

[30] Michael Collins QC, Privacy and Confidentiality in Arbitration Proceedings (1995) 11(3) Arbitration International 321; Jan Paulsson and Nigel Rawding, The Trouble with Confidentiality (1995) 11(1) Arbitration International 303; Friedland and Mistelis (n29) 3.

[31] *Ibid*. Collins, 321–336; Paulsson and Rawding, 303–320.

[32] Ola O. Olatawura, Nigeria's Appellate Courts, Arbitration and Extra-Legal Jurisdiction: Facts, Problems, and Solutions (2012) 28(1) *Arbitration International* 63, 64.

[33] Hong-Lin Yu, The Chinese Arbitration Association (CAA) Report on The Duty of Confidentiality Within the Global Landscape (2020) 7 (Forthcoming).

[34] De Ly, et al. (n28) 356.

conferences to be run using virtual meetings or video conferencing, and it is not uncommon – where the circumstances justify it – for cross-examination of some witnesses and experts to take place remotely.

Although the international nature of disputes has also made electronic document storage, trial presentation and electronic bundling a practical option for many arbitrations, the Seoul Protocol on Video Conferencing in International Arbitration (hereinafter "Seoul Protocol"),[35] demonstrates that 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. In particular, most key arbitration institutions subscribe to the duty of confidentiality. Against this background, the Cybersecurity Protocol for International Arbitration (hereinafter "Cybersecurity Protocol")[36] and the ICCA/IBA Joint Task Force's Roadmap on Data Protection in International Arbitration (hereinafter "the Roadmap")[37] were introduced in 2019 and 2020 in order to address the issues of cybersecurity, confidentiality and data protection.

(1) The Seoul Protocol

During the COVID-19 Pandemic, the arbitration practice was signposted to the Seoul Protocol[38] for guidance on how to conduct virtual hearings. The Protocol was published as "the best practice" for planning, testing and conducting video conferences in international arbitration on 18 March 2020.[39] According to the Protocol, the use of video-conferencing should be requested by the parties before the commencement of the hearing[40] and approved by the tribunal. The tribunal will subsequently be imposed with a duty to ensure an effective, safe and fair use of video conference for the arbitration proceedings.

Under the Seoul Protocol, parties have the responsibility for cybersecurity. They shall fulfil the logistical and technological requirements of the video conference attended by a witness.[41] Their responsibility is supplemented by the tribunal's duty to verify the identity of the individuals attending the video hearings to deliver a fair, equal and reasonable arbitration proceedings. This duty includes ensuring the quality and compatibility between the hardware and software used at the venues,[42] a good connection between the hearing venue and the remote venue,[43] an on-call individual with adequate technical knowledge to assist in planning, testing and conducting the video conference,[44]

---

[35] Seoul Protocol on Video Conference in International Arbitration (Mar. 18, 2020) <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 25 September 2020.

[36] ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration (2020 Edition) Foreword. <https://www.arbitration-icca.org/media/14/76788479244143/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf > accessed 25 September 2020.

[37] ICCA-IBA (2020) Roadmap to Data Protection in International Arbitration. <https://www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf> accessed 25 September 2020.

[38] Seoul Protocol (n35).

[39] *Ibid*.

[40] *Ibid*.

[41] *Ibid*. art.1. under art.4.1.

[42] *Ibid.* art.5.1 and art.5.6 (requirement of a quality audio output).

[43] *Ibid.* art.2.1.a.

[44] *Ibid.* art.2.1.b.

fair, equal and reasonable right of access to the parties and their related persons in the choice of the venue,[45] liaison with the appropriate individuals[46] to carry out testing[47] and backup arrangements in the event that the video conference fails[48] as well as informing the appropriate individuals involved in the hearing of the backup plan.[49] Parties are also responsible for ensuring the safeguards against unlawful interceptions by third parties[50] and the security of the participants in the video conferencing. A shared virtual document repository must be agreed by the parties. It shall be made available via computers at all venues. The parties use their best efforts to ensure the security of the documents.[51]

Nevertheless, this document failed to consider the online arbitration partakers' roles in the data protection requirements. It also fails to provide justification of imposing heavy burdens on the parties involved in an institutional arbitration. It does not seem to be fair on the parties to bear the responsibility and pay for the services of an institutional arbitration. In other words, whether the arbitral institution's responsibility to deliver a platform using ISDN or IP communication lines in order to ensure cybersecurity and data protection should be considered.[52] Furthermore, the Protocol did not address the concerns over data protection and the allocation of responsibility among the parties, the legal counsels, the tribunal and the arbitration institution in the context of collecting, holding, managing and transmitting personal and sensitive data arising from the use of video conferencing.

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

The 2020 Cybersecurity Protocol was introduced on 21 November 2019.[53] The principles contained in the Cybersecurity Protocol intend to provide a framework highlighting the reasonable information security measures, to increase awareness about information security for individual arbitration matters and to promote the users' confidence in the arbitration proceedings conducted virtually.[54] It is also designed to raise the awareness of risks involved in using and transmitting information generated for arbitration proceedings.

In contrast to the Seoul Protocol, the Cybersecurity Protocol establishes a framework which distributes responsibilities of cybersecurity and data protection among "each" party, including the tribunal and the administering arbitration institution. All of them are (1) defined as the custodians of arbitration-related information, (2) required to implement effective information security and adopt reasonable information security practices,[55] (3) required to follow the standard of reasonableness in their consideration.[56] They are all required to consider what information security measures are

[45] *Ibid.* art.2.1.c.
[46] *Ibid.* art.9.1.
[47] *Ibid.* art.6.1.
[48] *Ibid.* art.6.2.
[49] *Ibid.* art.9.4.
[50] Such as by IP-to-IP encryption.
[51] The Seoul Protocol (n 35) art.4.3.
[52] Kari Paul, *Worried About Zoom's Privacy Problems? A Guide to Your Video-Conferencing Options*, THE GUARDIAN (Apr. 9, 2020), <https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives> accessed 25 September 2020.
[53] The Cybersecurity Protocol (n36)
[54] *Ibid.*
[55] *Ibid*. princ.2.
[56] *Ibid*. princ.5.

reasonable to apply to a particular arbitration matter,[57] the baseline information security practices and the impact of their own information security practices on the arbitration,[58] in order to ensure 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.[59]

Both the parties and the tribunal are required to consider the various security factors[60] in their decision on the information security measures applied to an arbitration.[61] Both the parties and the tribunal have to consider the risk profile of the arbitration,[62] the existing information security practices, infrastructure, capabilities of the parties,[63] the burden, costs, and the relative resources available to any party, any arbitrator and any administering institution,[64] proportionality relative to the size, value, and risk profile of the dispute[65] and the efficiency of the arbitral process.[66] 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.[67]

According to Principle 9, both parties are responsible for reaching an agreement on reasonable information security measures.[68] On their own initiative or at the request of any party,[69] arbitrators are empowered to modify the agreed measures in the case of unexpectedly evolved circumstances.[70] Without parties' agreement, the tribunal has authority to determine the information security measures applicable to the arbitration providing Principles 4-9 on the applicable laws/rules/codes, reasonable standards/measures are taken into consideration.[71] According to Principle 13, in the case of a breach, the tribunal has the discretion to allocate the relevant costs among the parties and, in the event of breach, impose sanctions on the parties.

As the personal data protection regimes vary from jurisdiction to jurisdiction, the Working Group emphasised the importance of collaboration among the parties, the tribunal and the arbitration institution to address the 'concepts of 'reasonableness', 'adequacy', 'appropriateness', and 'proportionality' . . . applied, since the interpretation of these terms may differ under various legal regimes.'[72] For instance, the tribunal is also expected to consult both the parties and any administering

[57] *Ibid*. princ.1.
[58] *Ibid*. princ.2.
[59] *Ibid*. princ.3.
[60] e.g. asset management, access controls, encryption, security for communications, information, operations, incident management and environment.
[61] The Cybersecurity Protocol (n36) princ.7.
[62] *Ibid*. princ.6(a).
[63] *Ibid*. princ.6(b).
[64] *Ibid*. princ.6(c).
[65] *Ibid*. princ.6(d).
[66] *Ibid*. princ.6(e).
[67] *Ibid*. princ.8.
[68] *Ibid.* princ.9.
[69] *Ibid.*
[70] *Ibid*. princ.12.
[71] *Ibid*. princ.11.
[72] *Ibid.*

arbitration institution to work out the way to implement data protection obligations by observing the principles of proportionality and due process.[73]

In the document, the role played by the arbitration institutions is seen as the key to full compliance with the local data protection requirements. The Working Group held the view that the institutions have a shared responsibility in the compliance. Therefore, '[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.'[74] To achieve a full compliance,

> [I]t 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.[75]

Considering the international background of arbitrators and the parties, the consultation and coordination between them and the institutional arbitrations may lessen their burdens in their compliance with data protection and cybersecurity. Nevertheless, the complexity associated with the GDPR and virtual arbitration should not be under-estimated by any international arbitrator, any party, or any arbitration institution and their legal counsels in the context of cross-border transmission of data, conflicting regulations on data protection and cybersecurity and "each party's" capacity to implement cybersecurity and ensure the integrity of data.

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

The Working Group of the Cybersecurity Protocol left the full compliance to the forthcoming Roadmap to Data Protection in International Arbitration Proceedings[76] by the ICCA/IBA Joint Task Force on Data Protection in International Arbitration Proceedings.[77] According to the Roadmap, the duty of confidentiality can be imposed on the arbitrators / the tribunal, parties, lawyers and / or the non-parties working for or with them. For instance, in the case of arbitrators, the parties can impose direct (by agreement) or indirect (by arbitration institutional rules or applicable laws) a duty of confidentiality on arbitrators or subject the arbitrators to the duty. While arbitrators are subject to the duty of confidentiality, the duty may also extend to the non-parties, such as the tribunal secretary, employees of arbitrator's law firm/ chamber/ university, secretary, paralegal, arbitration institution, arbitration institution staff, counsels, registrar, accountants, Court members. Where video-conferencing is used, the issue of privacy may have to be considered in the case of people working for or with the tribunal, the arbitration institution administrative and IT staff in the case of institutional

[73] The Cybersecurity Protocol (n36) 15 (Commentary to Principle 4).
[74] *Ibid.*
[75] *Ibid.*
[76] Roadmap (n37).
[77] *Ibid*. foreword.

assisted virtual hearings and the institutional registrar or court members dealing with any matters related to the institutional arbitration.

The Roadmap is still in its draft consultation form and recently finished the public consultation on 30 June 2020. 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.'[78] Due to the potential civil[79] administrative 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.'[80] 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 Roadmap 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 personal data. Arbitral participants identified include the parties, their legal counsel, the arbitrators and the arbitration institution, and the people working for or with arbitral participants during an arbitration, such as tribunal secretaries, experts and service providers.[81] The Task Force further raises the awareness of 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 in both confidentiality and data protection.

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). It is essential to understand that all actors' 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 data protection law. Both transmission and processing data in international arbitration will trigger the extraterritorial application of the GDPR to an arbitration (discussed further below). All parties should have reasonable security measures in place and be prepared to deal with the conflicting of regulations involving cross-border data transfer in international arbitration.

[78] Roadmap (n37) 1.
[79] The potential fines of 4% of overall global incomes or EU 20-millions (whichever is higher) under the GDPR.
[80] Roadmap (n37) 1.
[81] *Ibid*. 2.

As COVID-19 has spread across the globe the business case for, and viability of, increased use of online arbitration specifically, has gained momentum.[82] Indeed, during their period of closure, the ICC has invested significantly in its infrastructure to enable virtual and hybrid arbitration hearings.[83] While *ad hoc* arrangements can be put in place to facilitate temporary remote arbitration hearings on a case by case basis, this investment indicates the prospect of online arbitration becoming a more sustainable practice. As a consequence, the practitioner community must reconsider data protection issues in a fresh light. Now is an opportune time to reflect on how data protection rights and responsibilities intersect with arbitration in the online environment.

COMPETING AND DISSECTING THE DUTY OF CONFIDENTIALITY AND DATA PROTECTION

In the absence of the statutory or implied duty of confidentiality, parties can exercise an "opt-in" choice with a confidentiality agreement, a procedural law or by agreeing or submitting their dispute to an institutional arbitration demanding the non-disclosure of information. Similarly, such a duty can also be waived by an "opt-out" in the form of the parties' agreement or the prescribed statutory exemptions.

Data gathered to structure the global landscape of arbitration institutional rules on the duty of confidentiality indicates that 144 institutions offer various degrees of express duty of confidentiality to the people who have access to information.[84] The emphasis is placed on arbitrators with 112 institutions requiring arbitrators not to disclose information obtained during arbitration proceedings. This is followed by parties' duty of confidentiality where 90 institutions surveyed impose the duty on the parties. In 84 arbitration institutions, their employees and administrative staff are required to abide by the duty of confidentiality. For third parties, the analysis of the words used in the arbitration institutional rules shows that witnesses require fewer restrictions on the duty of confidentiality than experts. Less emphasis is placed on both witness and experts, with 39 institutions requiring it for witnesses and 53 institutions imposing an express duty of confidentiality on the experts. Some require parties or arbitrators to ensure a confidentiality agreement is in place before experts can access the information. The parties who are unwilling to be subject to the duty of confidentiality prescribed by the arbitration institutional rules can exclude the application of the implicit duty of confidentiality with an "opt-out" imposed when they sign up for an institutional arbitration.[85]

Regardless of an "opt-in" or "opt-out" of confidentiality, data protection may prevail in the clash between the duty of confidentiality and data protection unless that duty falls within one of the recognised exceptions in data protection law. In data protection once the jurisdictions involved have been established, data protection rights and responsibilities will be determined by the type of data and the designation of the legal subject. This designation depends on the relationship to the data. In

[82] For analysis of the implications of COVID-19, see Hong-Lin Yu, '"Business as usual" during an unprecedented time – the issues of data protection and cybersecurity in international arbitration' (2020) 13(1) Contemporary Asia Arbitration Journal 45.

[83] Alexander G. Fessas, 1 July 2020. <https://iccwbo.org/media-wall/news-speeches/icc-hearing-centre-reopens-doors-for-physical-presence-dispute-resolution-hearings/> accessed 25 September 2020.

[84] Yu (n 33).

[85] For instance, "unless the parties agree otherwise" is used in art.1 of the CAAI Arbitration Rules 2017 and r.20 of the CPR Rules 2019.

the EU protection is offered to two tiers of data, 'personal data'[86] and 'special categories of data'[87] with the processing of the latter generally prohibited unless there are appropriate safeguards in place. At the core of 'personal data', is that the information relates to a natural person and allows them to be identified. Personal data can be seen in the confidential information safeguarded under the duty of confidentiality. For instance, the evidence, the memorandum, the notes taken by the tribunal,[88] the audio or video, the evidence and the award since they contain details of individuals. The bar for identification is low, meaning that it encompasses any data capable of causing identification even where it does so indirectly. In the case of the EU framework, it specifically highlights examples of identification such as 'an identification number, location data, [and] an online identifier'.[89] Such data is regulated by the European systems whether it relates to digital data or hardcopy data.[90] In the EU system the person to whom the data relate is known as the 'data subject'. It is important to emphasise that the 'data subject' can only be a natural person.[91] This can range from parties, arbitrators, institutional administrative teams, experts, to witnesses. Significantly, this 'data subject' is furnished with a number of rights which, at least in theory, allow them to control their data.[92] In contrast, the key roles to which responsibilities attach, are if you are considered to be a 'controller'[93], 'joint controller'[94] or 'processor'[95] of data.

In simple terms, a 'controller' or 'joint controller' is someone who has the ability to determine what data is collected and what is done with it. Where there are joint controllers involved they are obliged to agree who is responsible for which aspect of compliance.[96] However, even in circumstances where such an agreement is in place, the data subject is free to approach either controller to exercise their rights.[97] In the context of arbitration 'controllers' is likely to be include arbitrators if they have discretion to request specific information/evidence that includes personal data, arbitration institutions where they set specific rules as to what information has to be provided, and the parties in the preparation and communication of their evidence.

[86] art.4(1) GDPR 'means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'; also see art.3(1) Directive 2016/680.

[87] art.9(1) GDPR and Art 10 Directive 2016/680 uses the same definition on special category of data.s1(3) SHIELD Act 2019 (New York provisions) provides the categories of 'Personal Information' (which is broadly similar to 'personal data') and 'Private Information' (which is quite different to 'sensitive data' since it includes only social security numbers, driver's license, account information, biometric data, user names and passwords that in combination would allow access to accounts.)

[88] Kathleen Paisley, It's all about the data: The Impact of the EU Data Protection Regulation on International Arbitration (2018) 41(4) Fordham Int'l L.J. 841, 864.

[89] art.4(1), GDPR, Art 3(1) Directive 2016/680.

[90] The protection offered within s1(3)(C) the SHIELD Act is limited. It regulates computerised data held by businesses or state entity but only that which relates to New York residents.

[91] art.1(1), GDPR, s.1(3) SHIELD Act 2019, s.3 Data Protection Act 2018.

[92] Chapter III, GDPR, Chapter III Directive 2016/680.

[93] art.4(7) GDPR and art.3(8) Directive 2016/680.

[94] art.26 (1) GDPR and art.21 (1) Directive 2016/680 share the same definition of joint controllers.

[95] art.4(8) GDPR and art.3(9) Directive 2016/680 share the same definition of processor.

[96] art.26(1), GDPR.

[97] art.26(3), GDPR.

A 'processor' on the other hand, is someone who performs a task in relation to data on the instruction of a controller and has no decision-making power in relation to it. In the context of online arbitration, the number of participants who may fall into this category increases. For example, it may include not only the Tribunal Secretary but also case management providers, webfiling service providers, cloud storage providers, videoconferencing providers and secure network hosts.

There is a hierarchy within the designation of 'controller' or 'processor' with those who have decision-making power carrying a greater number of responsibilities. However, both the controller and processor are expected to abide by the data protection principles. In accordance with these principles, personal data should be processed lawfully, fairly and transparently, for a specific purpose, limited to what is necessary, be accurate, stored for the minimum amount of time needed, and processed in circumstances that guarantee the data's integrity and confidentiality.[98] However, the legal obligation for safeguarding that these principles are complied with by the controller and processor falls to the controller.[99] While there is no doubt about the applicability of these principles to arbitration Paisley has highlighted that there remains confusion in relation to the specific steps that must be taken to ensure compliance in this field.[100]

Yet, beyond these broad principles, there are further specific provisions that do provide concrete obligations. From the outset there must be a lawful foundation for the processing.[101] Processing is lawful where the data subject has consented. This may, on first perusal appear appealing in that one could simply request the consent of the data subject from the outset of the arbitral proceedings. However, as the EU framework has taken root it has become apparent that the 'consent' basis for the processing of data is strictly construed.[102] Consent can only be meaningful where the party is informed and genuinely has the ability to choose. If, for example, there is a power dynamic in the relationship, consent would not be the appropriate ground on which to base such processing.[103] Despite its initial appeal, this would tend to suggest that in the arbitration context, consent is not a suitable lawful basis between the arbitrator, tribunal and the parties, the parties and any employees, or the parties and their witnesses. If consent is used it will be the responsibility of the controller to be able to demonstrate that such consent has been given.[104] Still, even once consent has been given the data subject has the right to withdraw their consent.[105] While such withdrawal is not retroactive, it will present a challenge where arbitration proceedings have been initiated and the processing of personal data is the foundation of evidential claims. This reason alone is a deterrent from the use of consent as a lawful basis for processing.

---

[98] art.5(1), GDPR.
[99] art.5(2), GDPR.
[100] Paisley (n 88) 841.
[101] art.6, GDPR.
[102] ICO Guide to the GDPR for organisations: Lawful basis for processing - consent <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/> accessed 25 September 2020.
[103] Section 2.4, *European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law* (2018) 111. <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 25 September 2020.
[104] art.7(1), GDPR.
[105] art.7(3), GDPR.

There are, of course, alternative grounds on which data may be processed. Those most likely to be engaged within the online arbitration context include that it is necessary for the performance of a contract to which the data subject is party;[106] it is necessary for compliance with a legal obligation to which the controller is subject;[107] in the exercise of official authority vested in the controller;[108] or it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.[109] While the Roadmap expresses the view that 'legitimate interests' is likely to be the bases 'best suited' to data processing in the context of international arbitration, it must be acknowledged that online arbitration will include more third parties who's role in the processing of data is more tenuously linked to a legitimate interest.[110] For example, if you provide videoconferencing services with a functionality that enables the storage of recordings (video or audio) there may be questions as to whether such a facility can be justified within the 'legitimate interests' basis.

Even if 'legitimate interest' appears to provide a suitable basis for processing, it must be noted that it is possible for member states to supplement these grounds with specific requirements that must be satisfied.[111] This potential for disparate approaches means that one has to be cautious in assuming compliance has been achieved by following the GDPR alone. It always has to be contextualised with the jurisdictional specifics. Indeed, the Roadmap highlights that there are jurisdictions that 'have created a specific legal basis to allow processing of data in arbitral proceedings'.[112] Accordingly, the Roadmap recommends that participants in arbitration proceedings should, at the outset, give careful consideration to the lawful basis for processing.[113]

A particular challenge when selecting the lawful basis for processing in the arbitration context will be that the personal data may have been collected in the first instance for one thing, and now is potentially being considered for processing in a different context. For example, communications sent by employees of the parties. Whether this further processing is compatible should be considered in light of

> (a)any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed […] or whether personal data related to criminal convictions and offences are processed, […]; (d) the possible consequences of the intended further processing for data subjects; [and] (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.[114]

In selecting the legal basis for processing the ICCA-IBA Joint Taskforce suggest that information exchanged in the course of the arbitration process is 'essential for the proper administration of

[106] art.6(1)(b), GDPR.
[107] art.6(1)(c), GDPR
[108] art.6(1)(e), GDPR.
[109] art.6(1)(f), GDPR.
[110] Roadmap (n 37) 17.
[111] art.6(2), GDPR.
[112] Roadmap (n 37) 19.
[113] Roadmap (n 37) 16.
[114] art.6(4), GDPR, exceptions include consent or the compliance to Union or member state law.

justice.'[115] They highlight specifically that if data is processed in breach of confidentiality obligations then it will not have a lawful basis for processing.[116] However, such an assertion does not address the tension between obligations of confidentiality and the data subjects rights to control their data.

Data Subject's Rights

The data subject has specific rights that seek to secure their ability to control information about them. For example, the data subject has a right to transparent information and communication.[117] What this means is that a controller is bound to provide details of how information is processed and who to contact in order to exercise their other rights.[118] Where personal data has not been collected directly from the data subject, the data subject also has a right to information from the controller about how they intend to process their data and who to contact to exercise their rights in that case.[119] Data subjects also have an explicit right to access the information being processed about them.[120] Indeed, they are entitled to a copy of the personal data being processed about them.[121] In the context of international arbitration in the online environment, it is important to note that the scope of this right includes the right to information concerning 'the recipients or categories of recipient to whom the personal data have been or will be disclosed, [including] recipients in third countries or international organisations'[122] as well as 'the right to be informed of the appropriate safeguards […] relating to the transfer'. [123]

However, the data subject rights are not only designed to ensure they know what is being done with their data but also so that they are able to take steps to control that information. These steps include the right to request rectification, the right to erasure, the right to restrict processing and the right to object.[124] The right to rectification does not contain any caveats that would allow scope for parties to restrict this right.[125] Therefore, the right to rectification will have to be addressed by participants should the situation present itself. The right to erasure, restriction and objection all provided an exception "for the establishment, exercise or defence of legal claims."[126] Consequently, it can be argued these specific data subject's rights can be restricted in arbitration proceedings. Nevertheless, it is notable that to access the exception to the right of erasure states that in order to exercise this exception the controller would have to demonstrate that the processing is "necessary".[127]

Despite the possibility of exercising exceptions to data subjects' rights, participants in international arbitration should consider how and if these rights can be facilitated without breaching their other obligations concerning privacy and confidentiality concerning the arbitration proceedings themselves.

[115] Roadmap (n 37) 16.
[116] Roadmap (n 37) 17.
[117] art.12, GDPR.
[118] art.13, GDPR.
[119] art.14(1), GDPR.
[120] art.15, GDPR.
[121] art.15(3) and (4), GDPR.
[122] art.15(1)(c), GDPR.
[123] art.15(2), GDPR.
[124] arts.16, 17, 18 and 20, GDPR, respectively.
[125] Paisley (n 88) 904.
[126] arts.17(2)(e), 18(2) and 21(1), GDPR, respectively.
[127] art.17(3), GDPR.

One mechanism that contributes to meeting the obligations of privacy, confidentiality and data protection, is cybersecurity.

Cybersecurity and Data Protection

In EU data protection law, cybersecurity is a central feature. 'Data protection by design and default' requires that controllers 'integrate the necessary safeguards into the processing'.[128] Controllers and processors must ensure technical and organisational measures are in place that will provide sufficient security.[129] Significantly, such measures are to be assessed for compliance in light of state of the art.[130] This means that controllers and processors have to review on an ongoing basis the level of security provided by their current technical and organisational measures. In addition, since data subjects have a right to data portability, they should ensure that technical measures are not prohibitive to a data subject being able to consent to a transmission of data to another controller.[131]

One of the key challenges in adopting appropriate cybersecurity measures is ensuring that external providers are assessed for their data protection compliance and that, where appropriate, contractual arrangements are put in place to ensure that such providers are aware of their data protection obligations if data is being transferred out of the EU. This requirement is overlooked by the Seoul Protocol which placed most burdens on the parties.

Extraterritoriality and Data Transfers

In the context of online international commercial arbitration, it is highly likely that proceedings will involve parties inside and outside of the EU. For example, if the ICC Rules are being adopted, a request for arbitration must be submitted to the Offices of the Secretariat (being Paris, Hong Kong, New York, Sãn Paulo, Singapore, Abu Dhabi).[132] If parties to the arbitration are not members of the EU this presents the opportunity to initiate arbitration proceedings that avoid being captured by the EU provisions. However, the parties must consider the channel through which the data flows and who's hand is on the tiller. For example, they must consider the location of the servers used by the parties, arbitrators, institutions or third parties. Indeed, they also have to consider the participation of non-parties such as expert witnesses. In the case of arbitrations adopting the LCIA rules, they are now (as of the 1st October 2020) required to submit all requests to commence proceedings via electronic means, a material change from the 2014 rules.[133]

The extraterritorial reach of the EU provisions extend to 'the processing of data [by] a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.[134] Even in circumstances where a controller or processor are established outside of the EU, they will still have to comply with the EU provisions if they offer goods or services to data subjects within the EU.[135] Indeed, the EU provisions are so far reaching that they will also attach where a controller or processor is not established in the EU, and does not offer goods and services, but will receive data for processing from another party who does meet that criteria. This is because the EU provisions also regulate

[128] art.25(1), GDPR
[129] art.32, GDPR.
[130] art.32(1), GDPR.
[131] art.20, GDPR.
[132] art.4(1), ICC Rules of Arbitration as of 1st March 2017.
[133] art.1.3 and 1.4, LCIA Rules 2020.
[134] art.3(1), GDPR.
[135] art.3(2), GDPR.

transfers of data to 3rd countries.[136] The consequences are that if data is transferred from a controller or processor to another entity for further processing outside the EU the original controller or processor must ensure that the recipient will provide the same 'level of protection' to the data subject.[137] With the potential consequences of such provision evident to international companies based in the US, the EU-US Privacy Shield was developed. This system established a set of principles that aimed to ensure personal data sent from the EU to the US was treated in a manner compatible with EU law. Through this system companies were able to self-certify their compliance with those principles and would be held to account for their compliance by a relevant independent recourse mechanism.[138]

Recently, the Federal Trade Commission (hereinafter FTC) has taken steps to pursue those who falsely claim to be compliant with the EU-US Privacy Shield. For example, on the 13 January 2020, the FTC issued a complaint against Thru, Inc. (a company who provide cloud-based file transfer software).[139] On the 23 January 2020 it issued complaints against TDARX Inc. (an IT management and security services company) and Global Data Vault, LLC (a data storage and recovery services provider).[140] These complaints demonstrate one has to exercise caution and take appropriate due diligence measures when engaging with service providers in a cross-border context. This will be all the more important in online arbitration where much of the supporting infrastructure will involve aspects of outsourcing elements of data processing.

The EU-US Privacy Shield had been subject of a decision by the Court of Justice of the European Union in 2016 that declared that the provisions "did" provide adequate protection to data subjects in the EU.[141] However, the situation has recently become more complicated because on the 16 July 2020 that same court declared that adequacy decision invalid.[142] Critically, the Court emphasised that in order for there to be an adequate level of protection there must be appropriate safeguards, enforceable rights and effective legal remedies available to the data subject.[143] In assessing these criteria, consideration should be given to any contractual clauses applicable to the controller, processor and recipient of data in a third county but "also" that further consideration should be given to the ability of public authorities to access that data.[144] This means that those who had been placing reliance on the self-certification of compliance with the EU-US Privacy Shield, whether or not it was supported by standard data protection clauses within contracts, will now have to do more to ensure that data is not transferred to a 3rd country where the legal system offers a lower level protection than the EU. Consequently, measures to ensure appropriate safeguards should be in place in international arbitration where data can be transferred from the EU to non-EU jurisdiction(s). Specifically, the scope of such safeguards will have to look beyond the inclusion of a standard clause which had arguably become the expected measure.

[136] arts.44-50, GDPR.
[137] art.44, GDPR.
[138] Princ.7, EU-US Privacy Shield Framework Principles.
[139] *Complaint Against Thru Inc Docket* No C-4702.
[140] *Ibid.* and *Complaint Against Global Data Vault, LLC Docket* No C4706.
[141] Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield.
[142] *Schrems* (n8) para 199
[143] art.46(1) GDPR, Ibid. *Schrems* para 103-4.
[144] *Schrems* (n8) para 105

Data Protection Solutions

In her comprehensive analysis Paisley forms the view that 'when applying the GDPR to international commercial arbitration the regulators respect its decision making function, and recognize the cross border, consensual and potentially confidential nature of the arbitral process.'[145] However, the difficulty remains that there may be conflict between the demands of each aspect. In order to ensure clarity on the precise demands of GDPR in the arbitration context, she proffers the development of an approved code of conduct. She suggests that such a code could be developed in consultation with the European Data Protection Supervisor and the supervisory authorities within individual Member States.[146] In some respects, Paisley has brought this to fruition in co-chairing the ICCA-IBA Joint Taskforce Roadmap to Data Protection in International Arbitration discussed above.

Given the aim of the consultation was 'to help arbitration professionals better understand the data protection and privacy obligations to which they may be subject in relation to international arbitration proceedings'[147] its production and dissemination will certainly have achieved this end. However, there have been intervening factors that will require revision of the Roadmap to ensure it can provide a comprehensive route map to compliance. Considering that COVID-19 has introduced a new impetus for engagement with online arbitration as opposed to traditional in person arbitration, that online arbitration brings with it an increase in the actors taking part, an increase in technical infrastructure utilised, and is likely to further complicate the jurisdictions involved, there is a need to map a new how these issues intersect with data protection and the requirements of confidentiality.

CASE STUDY: RECONCILING CONFIDENTIALITY AND DATA PROTECTION IN THE ICC, ICDR AND LCIA

Establishing which jurisdictions are involved and therefore, which legal rules apply to the dispute is essential in arbitration. Still, even where a particular jurisdiction has been established, there may be competing jurisdictional rules applicable to the protection of data that add an additional tier of legal obligations over and above those contained within the arbitration agreement and/or jurisdiction specific arbitration law.[148] In particular, the different scope and effects of an Opt-in or Opt-out of the duty of confidentiality in the context of legislation and institutional rules, can be further complicated in the legal obligations imposed by data protection regulations. Therefore, it is necessary to identify specific institutional rules and data protection frameworks that can provide concrete examples. By identifying specific institutional rules and frameworks, this case study will be able to provide an indicative view of the key issues in marrying international arbitration and data protection rules within the online environment. For that reason, this case study focuses on institutional arbitration within the rules of the ICC, ICDR and LCIA.[149] It will examine those rules within the context of the EU data protection framework.[150]

Approaches to Privacy

[145] Paisley (n88) 920
[146] *Ibid.*
[147] Roadmap (n37) 1.
[148] Ananya Bajpai and Shambhavi Kala, Data Protection, Cybersecurity and International Arbitration: Can they Reconcile? (2019) 3(2) *Indian Journal of Arbitration Law*, 1-18.
[149] ICC Rules 2017 (n 132); LCIA Arbitration Rules 2020 (n 133); ICDR International Dispute Resolution Procedures, Rules 2014.
[150] GDPR (n3) and Directive 2016/680

ARTICLE 26 (3) of the ICC Rules provides that parties not involved in proceedings can be present at hearing only with the approval of the tribunal and the parties. Similarly, the default position of an LICA arbitration requires arbitration proceedings to be private. Although in the LCIA case, such a requirement can be waived by parties' written agreement and does not require the consent of the tribunal.[151] As with the LCIA, privacy is recognised in the ICDR Arbitration Rules which requires all hearings to be private unless the parties agree otherwise or the law provides to the contrary.[152]

In the ICC arbitration proceedings, the use of video-conference, telephone or similar means of communication is also allowed in the proceedings involving the emergency arbitrators and case management. In the case of the LCIA Rules, an emergency arbitrator can choose to hold the hearings either in-person or virtually, by conference call, videoconference or using other communications technology, in order to decide the claim for emergency relief on available documentation.[153] Similarly, the use of telephone, video, written submissions, or other suitable means, as alternatives to an in-person hearing is allowed after the appointment of an emergency arbitrator in an ICDR Arbitration. Based on the urgency of the matters and the appointment, Article 23(3)[154] of the Rules states that an emergence arbitrator is required to establish a schedule for consideration of the application for emergency relief with two business days of appointment.

The ICC requires the IT used for remote meetings and hearings must enable online communication among the parties, the arbitral tribunal and the Secretariat of the Court.[155] Under the ICC[156] and LCIA[157] Rules, an emergency arbitrator can exercise their discretion to instruct the use of videoconference, telephone or similar means of communication during the proceedings. The ICC uses the criteria of "essentiality"[158] to decide whether telephone or video conferencing should be used for procedural matters or hearings where attendance in person is not essential. No criteria is mentioned in the LCIA Rules. However, remoting hearings can also be used to the tribunal's organisation of the proceedings[159] and the proceedings requiring arbitrators to make contact with the parties no later than 21 days from receipt of the Registrar's written notification of the formation of the Arbitral Tribunal, regardless of in-person or virtual. [160] Similar use of the video conference is also allowed in the ICDR International Expedited Procedures. Its use is allowed under the arbitrator's discretion.[161] Article E-9 of the ICDR International Expedited Procedures Rules do not allow the practice of transcript or stenographic recording. Interestingly, such a prohibition is not mentioned in Article 23(3) of the ICDR Arbitration Rules.

Approaches to Confidentiality

[151] art.19.4, LCIA Rules 2020.
[152] art.23(6), ICDR Arbitration Rules 2014.
[153] art.9.7, LCIA Rules 2020.
[154] art.23(3), ICDR Rules 2014.
[155] art.24(4), ICC Arbitration Rules 2017.
[156] *Ibid*. art.4(2).
[157] art.9.7, LCIA Rules 2020.
[158] ICC Case Management Techniques(F).
[159] art.19.2, LCIA Rules 2020.
[160] Ibid. art.14.3.
[161] art.E-9, ICDR International Expedited Procedures International Expedited Procedures

In contrast to ICC arbitration, Article 30 of the LCIA Rules 2020 imposes the duty of confidentiality on the parties,[162] the arbitral tribunal, any tribunal secretary and any expert to the arbitral tribunal.[163] In the case of ICDR, subject to parties' agreement or the restrictions imposed by applicable laws, all information exchanged and disclosed by the parties or by witnesses shall not be divulged by arbitrators or the ICDR administrator.[164] This includes all matters relating to the arbitration or the award. While parties do not seem to be covered by the duty of confidentiality, Article 37(3) of the ICDR Arbitration Rules provides the tribunal powers to make orders in terms of confidentiality of the documents or information disclosed during the arbitration. Nevertheless, this power can be overruled by the parties' agreement.[165]

Regarding ICC arbitration, confidentiality is an "opt-in" with a party's request and having arbitrators as the gatekeepers to decide the issue of duty of confidentiality. In accordance with Article 22(3) of the ICC Arbitration Rules 2017, an arbitral tribunal's discretionary power can only be instigated by a request of any party. Once the discretionary power is activated, arbitrators may make orders concerning the confidentiality of the arbitration proceedings or of any other matters in connection with the arbitration and may take measures for protecting trade secrets and confidential information. Following the orders made by the arbitrators, the parties would be imposed with the contractual duty to observe confidentiality of the proceedings or matters related to arbitration on the basis of Article 22 (5) of the same rules and their submission to the ICC.

The duty of confidentiality in the ICC arbitration can be extended beyond the people mentioned above. On the institutional level, the International Court of Arbitration of the International Chamber of Commerce (the "Court") is mandated with the powers to ensure the application of the Rules of Arbitration of the International Chamber of Commerce to that effect.[166] In exercising its power, the Court would have access to the documents related to arbitrations. Article 6 of the Statutes[167] highlights the confidential nature of the Court's work and require the Court to observe the duty of confidentiality.

The duty of confidentiality imposed on the Court extends to anyone who participates in that work in whatever capacity in their attendance of the meetings of the Court and its Committees as well as their entitlement of the access to materials related to the work of the Court and its Secretariat.[168] This duty is prescribed in the Article 1(3) of the Internal Rules of the International Court of Arbitration where any persons invited by the President of the Court to attend a Plenary or Committee meetings is also subject to the duty of confidentiality. Any researchers undertaking work of an academic nature acquainting themselves with awards and other documents of general interest[169] within the framework of arbitration proceedings are also imposed with the duty of non-disclosure.[170] Furthermore, no authorization can be given by the Court unless the beneficiary has undertaken to respect the

[162] art.30.1, LCIA Rules 2020.
[163] *Ibid*. art.30.2.
[164] art.37(1), ICDR Arbitration Rules 2014.
[165] *Ibid*. art.37(3).
[166] art.1, The Statutes of The International Court of Arbitration.
[167] *Ibid*. art.6.
[168] *Ibid*. art.6.
[169] With the exceptions of memoranda, notes, statements and documents.
[170] art.1(5), The Internal Rules of The International Court of Arbitration.

confidential character of the documents made available to them. The researchers are also restrained from publishing anything based upon information contained without having previously submitted the text for approval to the Secretary General of the Court.[171]

Other people who may have access to the information related to individual cases are the Court members and the ICC National Committees members and groups members. They have to observe the duty of confidentiality of any information concerning individual cases with which they have become acquainted in their capacity as members. The specific information to their respective National Committees or Groups can only be disclosed with a request made by the President of the Court, by a Vice-President of the Court and authorized by the President of the Court, or by the Court's Secretary General.

While Article 22(3) of the ICC Rules defines confidential information as the information of the arbitration proceedings, any other matters in connection with the arbitration and trade secrets and confidential information, the scope of confidential information in an LCIA Arbitration covers all awards, all materials created for the purpose of the arbitration, and all other documents produced by another party which are not otherwise in the public domain. The tribunal's deliberations are included in the scope of confidential information and remain confidential to its member and the secretary to the tribunal.[172] The parties are mandated with an undertaking to keep all information related to arbitration confidential as well as secure confidentiality agreements with all people involved in the arbitration. Article 37(1) of the ICDR Arbitration Rules only mentions that confidential information is related to all matters relating to the arbitration or the award leaving a wide and ambiguous scope.

In an ICC arbitration, parties' opt-out of privacy or opt-in to duty of confidentiality is subject to the tribunal's discretion under Article 26(3) or Article 22(3) of the ICC Arbitration Rules respectively. The language used in Article 30.1 in the LCIA Rules does not seem to allow a contractual opt-out of the duty. According to the provision, disclosure can only be made on the grounds of a party's legal duty, protection or pursuance of a legal right, or enforcement or challenge an award in legal proceedings before a state court or other legal authority, including but not limited to any authorised representative, witness of fact, expert or service provider during the arbitration proceedings. However, it is possible to have an opt-out if the parties' choice of applicable law prescribes parties' consent as a ground for the waiver. Parties' agreement is the only ground allowing an opt-out of the duty under Article 37(1) of the ICDR Arbitration Rules.

Approaches to Data Protection

Neither the ICC or the ICDR make express provisions regarding data protection within their most recent rules.[173] Within the ICC data protection considerations have been addressed through the work of the ICC Commission on Arbitration and ADR Task Force on the Use of Information Technology in International Arbitration together with practice notes. Their most recent report lamented the limited use of information technology and indicated that the ICC were attempting to develop an updated case

[171] *Ibid*. art.1(6).
[172] art.30.2, LCIA Rules 2020.
[173] ICC Rules of Arbitration 2017; ICDR Rules 2014; and LCIA Arbitration Rules 2020.

management system.[174] Despite expressing concern that some IT products tended to include terms and conditions that prioritised the rights of the service providers over the 'concerns about confidentiality, security and data integrity' they still advocated greater use of technologies to support international arbitration.[175] While acknowledging that it is for the parties to agree the terms of IT use within proceedings they also suggested that 'the tribunal is ultimately responsible for the efficiency and integrity of the proceedings, and may wish proactively to encourage the parties to think more fully about the costs and benefits of the proposed IT'.[176] In providing direction on the use of IT, they advise the tribunal should consider the implications of such use in terms of substantive laws and in particular data privacy law.[177]

Writing in 2017, the Task Force's view was that despite increasing use of email there may be circumstances were this mode of communication is not considered to offer sufficient protection to confidential information. Perhaps with *Schrem* on their mind, they provided the specific example of a party being concerned about communications being intercepted by governmental authorities or third parties. In such circumstances they acknowledged that delivery by courier or hand delivery may be preferred.[178] In doing so, they acknowledged that data collected and shared in arbitration proceedings may be physical and digital.

In relation to the use of shared databases, such as data repositories in arbitration, they acknowledged that there may be limitations in terms of data protection laws as to what can be transferred or stored.[179] Furthermore, they raised particular concern where a commercial internet service provider is the host since they may 'impose terms and conditions that are incompatible with confidentiality and data protection requirements.'[180] Still, they emphasised that parties should agree on matters such as a 'minimum level of security' to ensure there is no 'unauthorised access by third parties'.[181] This highlights that it is the responsibility of each party 'to [protect] access to and the confidentiality and security of information under his, her, or its control'.[182] The main thrust of the Report is ultimately to encourage the use of IT where possible, and to encourage the parties to have appropriately drafted provisions included in either their terms of reference or through orders/directions given by the Tribunal.

In 2019 the ICC Court updated its Note to the Parties and Arbitral Tribunals on the Conduct of Arbitration to specifically address data protection.[183] The ICC acknowledged that itself, the Court, and its Secretariat collect and process personal data in an effort to fulfil their obligations under its Rules of Arbitration.[184] Similarly, the ICDR have highlighted that Arbitral Tribunals will also process such

[174] ICC Commission on Arbitration and ADR Task Force, Report on the Use of Information Technology in International Arbitration, 2017, 2.
[175] *Ibid.* 2.
[176] *Ibid.* 6.
[177] *Ibid.* 8.
[178] *Ibid.* 9
[179] *Ibid.* 10
[180] *Ibid.* 11.
[181] *Ibid.* 15.
[182] *Ibid.* 15.
[183] Note to Parties and Arbitral Tribunals on the Conduct of Arbitration under the ICC Rules of Arbitration January 2019.
[184] *Ibid.* para 81.

personal data to fulfil their obligations under their Rules.[185] The ICDR have indicated that the Arbitration Tribunal will be responsible for 'managing the exchange of information between the parties' and that **'**the parties may provide the tribunal with their views on the appropriate level of information exchange for each case, [although] the tribunal retains final authority'.[186] In making such declarations the ICC and ICDR would seem to indicate that the Tribunal, in both cases, will be a controller of personal data, or at the very least, a joint controller, since there may be a dialogue with the parties to agree when and what information should be exchanged. This will include personal data about 'the parties, their representatives, the arbitrators, the administrative secretary, the witnesses, the experts, and any other individuals that may be involved in any capacity in the arbitration'.[187] The ICDR acknowledge that as a result, data may be transferred into and out of the EU.[188] Indeed, within their privacy policy, they highlight that in using 3rd parties to deliver services 'transfers of data to countries outside of the United States or the EU may occur based upon the EU's adequacy decisions, or based upon confirmation of adequate safeguards among other lawful bases.'[189]

Perhaps most significantly, the ICC state that all of those involved in proceedings by agreeing to 'participate' 'acknowledge' and 'accept' this use of their data.[190] This is a little problematic since it seems to suggest that the lawful basis for processing would be consent. However, such consent would not be considered validly given since they are required to consent in order for the proceedings to take place within the ICC Rules. In addition, there will be individuals who are arguably not participating in proceedings, but their data is being processed. For example, employees of the parties.

In order for this to be implemented, they advise that the parties are responsible for ensuring that any person appearing on their behalf is 'aware and accepts' such processing, but also that 'applicable regulations', specifically citing the GDPR, are complied with.[191] Still, the ICC specifically highlight that it will be the responsibility of the "Arbitral Tribunal" to periodically remind participants that the 'GDPR applies to the arbitration and that by accepting to participate in the proceedings, their personal data may be collected, transferred, published and archived.'[192] To this end they reiterate the advice of the Task Force that the Tribunal should include a data protection protocol within the Terms of Reference.[193]

In the ICC's view it is the responsibility of 'the parties, their representatives and all other participants in the proceedings [to] ensure the security of personal data [that they process]'.[194] Importantly, acknowledging the rights of the data subject they affirm that 'any individual', 'can at anytime', contact the Secretariat or the arbitral tribunal to exercise their right of access and correction.[195] They recommend that any breaches of 'security or confidentiality' should be reported immediately to the

[185] *Ibid*.
[186] art.21, ICDR Arbitration Rules 2014.
[187] Note (n183) para 81.
[188] *Ibid.*
[189] ICDR Privacy Policy <https://www.icdr.org/index.php/PrivacyPolicy> accessed 25 September 2020.
[190] Note (n183) para 82.
[191] *Ibid.* para 83.
[192] *Ibid.* para 84.
[193] *Ibid.*
[194] *Ibid.* para 86.
[195] *Ibid.* para 85.

data subject and the ICC. In cases where the ICC is the controller of the data at the point of breach, they will report to the relevant supervisory authority and notify the data subject.[196] The ICC acknowledge that arbitrators may retain, for a specific period of time, personal data after the conclusion of the arbitration provided that they notify the data subject and the Secretariat.[197] The Secretariat may archive 'awards, Terms of Reference and decisions of the Court [and] pertinent correspondence of the Secretariat.'[198] This update provides some guidance to those involved in arbitration in terms of their data protection obligations. However, the guidance itself is somewhat opaque.

Unlike the ICC, the ICDR assert that they provide secure case administration.[199] This system includes four strands: Storing information securely, encrypting sensitive data, data back-up and recovery procedures and taking steps to ensure employee awareness and compliance. As their network and websites are housed at external off-site data centres they ensure the integrity and security of these data centres through the implementation of the American Institute of Certified Public Accountants (AICPA) for Service Organization Control (SOC) type II reports.[200]

As within the ICDR system there is an obligation of confidentiality placed on arbitrators and administrators,[201] within the LCIA, upon the parties, arbitral tribunal, tribunal secretary and experts to the tribunal, and in the case of the ICC, at the request of the parties with the consent of the tribunal, that would tend to suggest they are obliged to adopt appropriate cybersecurity measures to be compliant. However, boundaries of 'confidential information' and protected 'personal data' are different. What this means is that all parties subject to a duty of confidentiality must understand the distinction between 'confidential information' and 'personal information' to ensure that both categories of information are provided an appropriate level of technical security and in the case of 'personal information' that it can be accessed, rectified and erased if necessary.

In contrast to the ICC and ICDR, the LCIA do include within their more recent rules provisions on data protection.[202] LCIA were clear that although 'the pandemic did not necessitate any change of direction or focus, it allowed the LCIA to address explicitly some changes in recent good practice, notably the increased use of virtual hearings and the primacy of electronic communication across the board.'[203] These rules acknowledge that the LCIA are bound by data protection law.[204] Perhaps most significantly, the LCIA assume responsibility to ensure that data protection issues have been considered by the parties and that LCIA will consider whether it is necessary to issue binding orders in

[196] *Ibid.* para 88.
[197] *Ibid.* para 89.
[198] *Ibid.* paras 90-91.
[199] ICDR Secure case administration <https://www.icdr.org/Secure_Case_Administration> accessed 14 September 2020.
[200] *Ibid.*
[201] art.37, ICDR Arbitration Rules 2014; Steven A. Certilman and Eric W. Wiechmann, 'ADR in the Age of Cybersecurity' (2019) 12(1) New York Dispute Resolution Lawyer 14, 14.
[202] art.30A, LCIA Arbitration Rules 2020.
[203] Updates to the LCIA Arbitration Rules and the LCIA Mediation Rules (2020) <https://www.lcia.org/lcia-rules-update-2020.aspx> accessed 25 Sept 2020.
[204] art.30.4, LCIA Arbitration Rules 2020.

relation to data protection or information security.[205] Coming into force on the 1 October 2020 there has yet to be sufficient proceedings to enable the impact of such orders to be considered.

As with the ICDR, the LCIA provide case management through its provision of online filing.[206] The LCIA unambiguously acknowledges its role as a data controller where personal information has been provided to them.[207] In terms of the security offered to such information, they provide that the information may be shared with 3rd parties including suppliers of document storage and IT service providers and may be transferred and stored outside the European Economic Area.[208] They even go so far as to highlight associated dangers as they state 'unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site including via our online filing system; any transmission is at your own risk.'[209] Nevertheless, as the GDPR will be applicable should a security breach occur they will still have to follow the notification process set out within the regulation and potentially face sanction by the supervisory authority within their state.

CONCLUSION: CONFIDENTIALITY V DATA PROTECTION

This article has highlighted the complexity of the issues. The goal of full compliance can be achieved by identifying the roles played by the participants involved in both data protection and online arbitration and raising their awareness of the intersecting obligations in order to deliver robust data protection. This will avoid any breach of the duties and ensure cybersecurity and privacy which are the cornerstones of data protection and arbitration.

The key to meeting data protection obligations in online international arbitration is to understand what data you need, what you plan to do with it and where data is to be transmitted. The prospect of developing online arbitration as a matter of course does not necessarily change this.[210] However, online arbitration does increase the number of actors engaged in the process and therefore the number of actors who will have access to data and potentially present a risk to its protection. While there may have been an initial reluctance to engage with exclusively online arbitration[211], there is no doubt that within the practitioner community there is an appetite for a solution driven approach to identifying and addressing data protection problems generally, allowing online arbitration to become more feasible. This can be seen in the Seoul Protocol, the Cybersecurity Protocol and the Roadmap.

Nevertheless, partakers in online international arbitration can be subject to both a duty of confidentiality and data protection responsibilities. Since the scope of confidential information is different from personal information it cannot be presumed that measures taken to protect one category of information automatically protects the other. Moreover, since the foundation of their

[205] *Ibid*. art.30.5-30.6.
[206] LCIA Online Filing <https://onlinefiling.lcia.org/> accessed 25 September 2020.
[207] LCIA Privacy Policy: 1.3 <https://www.lcia.org/privacy-policy.aspx> accessed 25 September 2020.
[208] *Ibid*. 7.1 and 8 respectively.
[209] Ibid. 8.3.
[210] Here 'online arbitration' is being used to capture all aspects of conducting arbitration remotely.
[211] Gabrielle Kaufmann-Kohler, 'Online Dispute Resolution and its Significance for International Commercial Arbitration' in *Global Reflections on International Law, Commerce and Dispute Resolution Liber Amicorum in honour of Robert Briner* (ICC Publishing, 2005) 441.

obligations differ, one must consider the interaction between these two. In the case of the LCIA, the duty of confidentiality placed on the parties, arbitral tribunal, tribunal secretary and expert to the tribunal are set out within the LCIA rules and are contractually binding. Although narrower in scope, the ICDR also includes within its rules a duty of confidentiality for the arbitrator and ICDR administrators contractually binding them to the duty. There is additional scope for the ICDR Tribunal to make orders that expressly address issues of confidentiality and place such obligations on additional participants. In the case of the ICC the duty of confidentiality can be requested by the parties and is subject to the discretion of the tribunal. Similar to the position of the ICDR, the ICC tribunal can issue orders placing the duty of confidentiality on named participants. In all three cases the foundation of the duty rests on contract.

On the other hand, the obligations of data protection are predominantly present as a result of the application of the GDPR, due to extra-territorial effect or, complimented by domestic implementation measures. While the ICC have issued a practice note that provides guidance, this does not alter the obligations contained within the GDPR. Rather, it provides possible routes by which parties can agree measures that seek to satisfy their data protection obligations such as producing a protocol within terms of reference. While this may have the effect of binding the parties to that agreement it will not enable them to contract out of their obligations contained within the GDPR. Indeed, the GDPR does allow such arrangements to be made to agree division of responsibilities amongst joint controllers,[212] and to agree the terms of outsourcing processing. However, there is limited scope to shield them from liability to the data subject.[213]

The duty of confidentiality is likely to demand that the obliged actor does not provide access to information or copies of that information. Such a refusal would be in violation of a data subject rights. Since the right of access is only applicable to the controller, it is only those who are designated as controllers and subject to the duty of confidentiality who may be in a position of conflict. However, while the controller is the actor directly captured by the rights as detailed in the GDPR, a processor may be captured indirectly since they are required to assist the controller' in responding to request by a data subject to exercise their rights.[214] Still, there is light at the end of the tunnel. A data subjects access rights can be restricted if the Union or member state has implemented a law allowing such restrictions. While the GDPR provides a number of grounds on which such restrictions can be justified, the most relevant in this context is the possibility to restrict in the interests of 'the enforcement of civil law claims'.[215] Still, even if such a basis does exist on examination of the individual jurisdiction, there is still scope for ambiguity as to whether arbitration proceedings would be captured in such a ground.

In circumstances where the duty of confidentiality is founded on a legislative provision it would be expected that such a provision would detail how that provision is intended to interact with other legal obligations such as those set out by data protection law. For example, the Scottish Arbitration Rules expressly allow disclosure to be made 'in order to comply with any enactment or rule of law'.[216] In

[212] art.26(1), GDPR.
[213] arts.26(3), 28(3) and 82, GDPR.
[214] art.28(3)(e), GDPR.
[215] art.23(1)(J), GDPR.
[216] rule 26(1)(c)(i) Scottish Arbitration Rules.

New Zealand, a disclosure can be made provided it is 'authorised or required by law' and 'the party who, or the arbitral tribunal that, makes the disclosure provides to the other party and the arbitral tribunal or, as the case may be, the parties, written details of the disclosure (including an explanation of the reasons for the disclosure)'.[217] And, in Australia, a disclosure can be made on almost identical terms.[218] These provisions collectively indicate that where confidentiality is based on statutory provisions it is likely that a disclosure can be made to satisfy a data subjects rights although there may be conditions that must be satisfied such as notifying the parties of disclosure.

Still, in making a decision on whether and in what circumstances to disclose information, ultimately the actor has to weigh up the consequences of breach in each case. This paper has highlighted that at the core of such an assessment is consideration of what information is captured within the duty of confidentiality versus the information regulated by data protection law. Accordingly, to make such an assessment effective, the actor must fully understand the scope of their obligations in terms of data protection law.

[217] s14C(d), New Zealand Arbitration Act 1996 and Arbitration Amendment Act 2007.
[218] s23D(9)-(10), Australian Arbitration Act 1974 (amended in 2018).