

ICC COMMISSION REPORT

Leveraging Technology
for Fair, Effective and Efficient
International Arbitration Proceedings

Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings is a Report of the ICC Commission on Arbitration and ADR, which was approved at its virtual meeting of 23 November 2021.

Acknowledgements

This Report is the result of an ICC Working Group's revision of the second edition of the ICC Commission Report 'Issues to be Considered when Using Information Technology in International Arbitration' (2017, and first published in 2004).

Members of the Working Group, led by Stephanie Cohen, include: Sana Belaid, Mikal Brøndmo, Iuliana Iancu, Anna Masser, Claire Morel de Westgaver, Mark Morril, Lars Perhard, Sebastian Salazar, Erik Schäfer, Debora Visconte, David B. Wilson.

The two previous reports on this subject were produced by an ICC Task Force established by the ICC Commission on Arbitration and ADR and chaired by Erik Schäfer, joined by David Wilson for the second edition.

With special thanks to Melanie van Leeuwen as liaison for the Steering Committee, Mirèze Philippe, Hélène van Lith and Jennifer Jones for their valuable contribution to this revision.

ICC Publication DRS898 ENG

ISBN: 978-92-842-0619-3

Publication date: February 2022

Copyright © 2022

International Chamber of Commerce (ICC)

33-43 avenue du Président Wilson

75116 Paris, France

www.iccwbo.org

The views and recommendations contained in this publication originate from a Task Force created within ICC's Commission on Arbitration and ADR. They should not be thought to represent views and recommendations of the ICC International Court of Arbitration or the ICC International Centre for ADR, nor are they in any way binding on either body.

ICC holds all copyright and other intellectual property rights in this work, and encourages its reproduction and dissemination subject to the following:

- ICC must be cited as the source and copyright holder mentioning the title of the document, © International Chamber of Commerce (ICC), and the publication year.
- Express written permission must be obtained for any modification, adaptation or translation, or for any commercial use.
- The work may not be reproduced or made available on websites except through a link to the relevant ICC web page.

Permission can be requested from ICC through copyright.drs@iccwbo.org

Trademarks: ICC, the ICC logo, CCI, International Chamber of Commerce (including Spanish, French, Portuguese and Chinese translations), International Court of Arbitration and ICC International Court of Arbitration (including Spanish, French, German, Arabic and Portuguese translations) are all trademarks of the ICC, registered in several countries.

Contents

1	Introduction	5
1.1	Introductory remarks	5
1.2	Structure of the Report	6
2	The Relevance of Technology to Arbitrator Selection	7
3	The Role of Technology in Effective Case Management	8
3.1	Pre-dispute agreements	8
3.2	Party autonomy	9
3.3	Tribunal authority	10
3.4	Cybersecurity, data privacy, and confidentiality	11
	3.4.1 <i>Obligations concerning cybersecurity breaches</i>	15
	3.4.2 <i>Data protection obligations</i>	15
3.5	Allocation of costs	15
3.6	Technical problems during the arbitration	16
3.7	Technical tutorials or conferences during the arbitration	16
4	Electronic Exchange of Communications, Exhibits, and Other Submissions	17
4.1	Applicable arbitration rules and mandatory law	17
4.2	Methods of electronic exchange	18
	4.2.1 <i>E-mail</i>	19
	4.2.2 <i>File share transfers</i>	19
	4.2.3 <i>Physical data carriers (e.g. flash drives, hard disks)</i>	20
	4.2.4 <i>Online case management platforms</i>	20
4.3	Exceptional circumstances warranting non-electronic exchange	21
4.4	Whether hard copies will also (or sometimes) be provided	22
	4.4.1 <i>Tribunal members</i>	22
	4.4.2 <i>Hearing witnesses</i>	23
4.5	Electronic file organisation and naming conventions	23
4.6	Prescribed rules for file format	23
	4.6.1 <i>For convenience</i>	23
	4.6.2 <i>Data integrity issues</i>	23
4.7	Proof of service	25
4.8	Signature requirements	25
5	Other Uses of Technology to Consider	29
5.1	E-briefs or e-bundles	29
5.2	Machine learning artificial intelligence	29
5.3	Specialised hardware or software	30

6	Issues Relevant to Evidentiary Hearings	31
6.1	General considerations	31
6.1.1	<i>Advance planning</i>	31
6.1.2	<i>Displaying electronic exhibits</i>	31
6.1.3	<i>Visual presentation software</i>	31
6.1.4	<i>Real time transcripts</i>	32
6.2	Virtual hearings	32
6.2.1	<i>Factors to be considered before proceeding with a virtual hearing</i>	32
6.2.2	<i>Organisation of virtual hearings</i>	36
6.2.3	<i>Special issues relating to witnesses</i>	36
6.2.4	<i>Recordings</i>	37
6.2.5	<i>Hearings with large numbers of participants</i>	38
6.2.6	<i>Technical testing</i>	38
6.2.7	<i>Intra-tribunal and intra-party communications</i>	39
6.3	Hybrid hearings	39
	Appendix A – Key Findings from the Survey on Use of IT in International Arbitration	41
	Appendix B – Sample Procedural Language Relating to Technology Tools and Solutions	46
I.	Sample Procedural Directions in Preparing for the First Case Management Conference	46
II.	Sample Wording for Terms of Reference Regarding Electronic Notifications and Communications	47
III.	Sample wording for first procedural orders	48
	Appendix C – Organisational Checklists for Virtual Hearings	55
I.	Considerations for parties when choosing a third-party service provider as host	55
II.	Pre-hearing checklist for parties and tribunals coordinating hearing preparations with virtual hearing host	56
III.	Counsel's pre-hearing checklist for preparing individual witnesses	57
IV.	Arbitrator's checklist to prepare for virtual hearing	58
V.	Counsel's checklist to prepare for virtual hearing	60
	Appendix D – Template Procedural Order for Conduct of Evidentiary Hearing via Videoconference	62
	Appendix E – Checklist of Issues to Consider When Choosing an Online Case Management Platform	70

1 Introduction

1.1 Introductory remarks

This Report focuses on technology tools and technology-related practices that may serve the important function of making international arbitration more effective or efficient, while ensuring the fairness of the proceedings and equal treatment of the parties.¹

To help parties and tribunals evaluate how and when to use technology to facilitate an efficient, fair, and cost-effective arbitration process,² the Report (i) identifies prevalent technology being used in support of international arbitration, (ii) describes features and functionality that may enhance the arbitral process, and (iii) discusses useful procedural practices and pitfalls to be avoided.

There is no one-size-fits-all when it comes to technology and recommendations about the 'best' products. Services may change rapidly with technological advancements, the unique circumstances of each case, and with regional variances in available products and services. Thus, the Report does not endorse any specific technological developers, products, or services, but does give examples of tools and services so that parties and tribunals will have some starting points when investigating the marketplace.³

As a practical resource for practitioners, the Report highlights available detailed guidance on specific issues (concerning cybersecurity and data protection, for example), and includes appendices with sample language for procedural orders and organisational checklists that can be consulted quickly and easily on an ongoing basis. Sample procedural language is provided for illustration purposes – to demonstrate the issues discussed in this Report – and any procedural order must necessarily be tailored to the needs of a particular case.

The Report addresses the importance of early consideration of how technology will be used in an individual case – no later than the initial case management conference – and how parties and tribunals can integrate technology in a way that will maximise savings of time and cost with due regard for fundamental principles of fairness and equality. The Report also flags potential recognition and enforcement concerns that may arise from the use of technology in some jurisdictions,⁴ such as electronic notifications and electronic signatures, or hearings convened by videoconference over the objection of a party.

- 1 This Report sometimes refers to technology tools and practices as 'IT' or 'IT solutions'. Examples of technology tools or practices currently used in international arbitration include: (i) online e-filing platforms for exchanging communications between and among the parties, the arbitrator or arbitrators (the 'tribunal'), and the administering body; (ii) storage of information for access by the parties and the tribunal using cloud-based file-share services or portable or fixed storage media (e.g. flash drives or hard drives); (iii) sophisticated cloud-based case management platforms that allow the parties and tribunal to store, share, manage, and annotate case-related documents in a single repository with enterprise-grade security and data privacy compliance controls; (iv) software and media used to facilitate 'paperless' case presentations (e.g. to create searchable electronic document bundles with hyperlinks to exhibits and legal authorities); (v) other electronic case preparation tools, such as software for machine-generated document translations; (vi) hearing room technologies, such as videoconferencing, multimedia presentations, instant messaging, simultaneous language interpretation software, and 'real time' electronic transcripts; and (vii) electronic document scanning or digital signature software to facilitate the electronic signature and notification of awards. Readers who encounter unfamiliar terminology in this Report or wish to delve deeper may wish to consult IT industry glossaries, such as *Gartner's Information Technology Glossary*, or more specialised glossaries such as the *SANS Institute's Glossary of Security Terms*.
- 2 Unless the context requires otherwise, 'parties' is generally used in this Report to refer to parties and their counsel.
- 3 This Report does not address infrastructure, baseline equipment, or commonly used software such as office suite packages of e-mail, word processing, presentation, and spreadsheet applications that arbitral participants likely use in their daily practices, although some of the discussion and resources cited here may be relevant to those considerations.
- 4 Comprehensive legal analysis of recognition and enforcement considerations is, however, beyond the scope of this Report and any statements about the law of a particular jurisdiction should be checked by parties and tribunals against their own independent analysis.

While technology brings substantial benefits to the international arbitration process, access to technology resources, including hardware, software applications, and broadband internet, may vary widely by region and according to the financial resources of the parties. Such an imbalance in the technology resources available in different regions or between the parties in an arbitration case could contribute to a ‘digital divide’ broadly or an inequality of arms. By increasing awareness of, and access to, information on technology tools and practices that may enhance the arbitration process, and by suggesting mitigation strategies to overcome technological challenges faced in emerging markets, this Report may help level the technological playing field.

The conclusions and recommendations in this Report are informed by a Survey of over 500 members of the arbitration community about their general experience with, and views on, the use of technology tools and solutions. The Survey results (as set out in **Appendix A**) evidence important and widespread support for greater use of technology tools in international arbitration going forward,⁵ including increased willingness to deviate from old norms (e.g. supplemental hard copy filings in favour of paperless proceedings, at least up until the hearing) and to employ underutilised tools (e.g. ‘e-briefs’ with hyperlinked exhibits). These results compel us to ensure an early consideration of how technology can and will be leveraged in individual matters and to re-visit past assumptions about how proceedings will unfold (e.g. most respondents believed there should be no presumption in favour of physical, hybrid, or virtual hearings; rather, the tribunal should decide what is appropriate based on the individual circumstances of the case).

1.2 Structure of the Report

Following this introduction, the Report is structured as follows:

Section 2 addresses the *relevance of technology to arbitrator selection*, including expectations about technological competence and technological literacy.

Section 3 focuses on *effective case management when integrating technology* in the arbitral process. It stresses the importance of early consideration of how technology will be used in an individual matter (no later than the initial case management conference) and provides general considerations regarding choices and implementation to help parties and tribunals integrate technology in a way that will maximise savings of time and cost with due regard for fundamental principles of fairness and equality. Cybersecurity and data protection issues are covered in this discussion.

Section 4 canvasses a wide range of *practical issues related to the electronic exchange of communications and notifications*, including: (i) the relevance of arbitration rules and mandatory law; (ii) methods of electronic exchange; (iii) circumstances warranting non-electronic exchange; (iv) courtesy hard copies; (v) file organisation and naming conventions; (vi) file format and data integrity issues; (vii) electronic proof of service; and (viii) signature requirements.

Section 5 identifies *other uses of technology* parties and tribunals may wish to *consider*, such as e-briefs and machine learning artificial intelligence.

Section 6 flags *practical considerations and potential pitfalls* related to the use of technology to facilitate evidentiary hearings, with special attention paid to the organisation of both virtual and hybrid hearings. This Section includes a discussion of recognition and enforcement issues related to virtual hearings held over the objection of a party and provides insight into the approach taken by ICC parties and tribunals in recent cases.

To facilitate ongoing reference to key considerations and recommendations made in this Report, an overview of the results of a Survey in **Appendix A** is followed by a series of appendices with practical checklists and sample procedural language.

Appendix B contains *Sample Procedural Language Relating to Technology Tools and Solutions*.

⁵ Among the answers received, 83% of respondents agreed that technology has been underutilised in the arbitral process, and over half of respondents reported they would use IT solutions ‘more often’ after the pandemic.

Appendix C contains five organisational *Checklists for Virtual Hearings*:

- I. Considerations for Parties When Choosing a Third-Party Service Provider as Host
- II. Pre-Hearing Checklist for Parties and Tribunals Coordinating Hearing Preparations with Virtual Hearing Host
- III. Counsel's Pre-Hearing Checklist for Preparing Individual Witnesses
- IV. Arbitrator's Checklist to Prepare for Virtual Hearing
- V. Counsel's Checklist to Prepare for Virtual Hearing

Appendix D is a *Template Procedural Order* for the conduct of evidentiary hearings via videoconference.

Appendix E is a *Checklist of Issues to Consider When Choosing an Online Case Management Platform*.

2 The Relevance of Technology to Arbitrator Selection

Basic technological competence, including awareness of and attention to cybersecurity and data privacy issues, is not case-dependent and is now reasonably expected of arbitrators (as well as other arbitral participants, including counsel). This expectation stems from continuing digitalisation of the legal industry and international arbitration, with corresponding evolution of existing professional and ethical obligations, including well-established obligations to maintain the confidentiality of proceedings and the arbitrator's duty of 'competence'.⁶ Although such duty of competence is generally undefined in ethical codes,⁷ it is given context and meaning from the evolution of lawyer ethics codes in some jurisdictions, which explicitly state that the duty of competence requires an understanding of the key role of technology, including staying abreast of technology's benefits and risks.⁸ Taking reasonable steps to avoid the unauthorised sharing of data is also a foundational requirement of most data protection statutes enacted in recent years. Many of these statutes have a broad jurisdictional sweep, and it is likely one or more will be applicable in most international arbitrations.⁹

With this background in mind, major arbitral institutions and professional bodies have revised their arbitration rules or other guidance for the conduct of proceedings to expressly require or encourage consideration of cybersecurity and data privacy issues at the initial case management conference or other early stage of the proceedings.¹⁰ Because a basic understanding of cybersecurity and data privacy

- 6 S. Cohen and M. Morril, *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion*, 40 *Fordham Int'l Law J.* 981 (2017).
- 7 See e.g. *IBA Rules of Ethics for International Arbitrators* (1987), Introductory Note and Rule 2.2 ('International arbitrators should be ... competent'; 'A prospective arbitrator shall accept an appointment only if he is fully satisfied that he is competent to determine the issues in dispute'); Chartered Institute of Arbitrators, *Code of Professional and Ethical Conduct for Members* (2009) at Part 2, Rule 4; *AAA/ABA Code of Ethics for Arbitrators in Commercial Disputes*, Canon 1 (2004) (an arbitrator should accept appointment in a particular matter only if fully satisfied that he or she is 'competent to serve').
- 8 See S. Cohen and M. Morril, *supra* note 6, at 997-1002.
- 9 These include, for example, the General Data Protection Regulation (EU) 2016/679 ('GDPR') in Europe, the General Data Protection Law in Brazil, the California Consumer Privacy Act in the United States, and the Personal Information Protection and Electronic Documents Act ('PIPEDA') in Canada.
- 10 See e.g. *ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration Under the ICC Rules of Arbitration* (1 Jan. 2021) ('ICC Note to Parties and Tribunals') at para. 119: 'At an appropriate time in the arbitration, the arbitral tribunal shall remind the parties, representatives, witnesses, experts and any other individuals appearing before it that the GDPR or other data protection laws and regulations apply to the arbitration and that their personal data may be collected, transferred, published and archived pursuant to the arbitration agreement or the legitimate interests to resolve the dispute and that arbitration proceedings operate fairly and efficiently. Arbitral tribunals are encouraged to draw up a data protection protocol to that effect'; and para. 121: The arbitral tribunal, the parties and their representatives shall put in place and ensure that all those acting on their behalf put in place appropriate technical and organisational measures to ensure a reasonable level of security appropriate to the arbitration, taking into account the scope and risk of the processing, the state of the art, the impact on data subjects, the capabilities and regulatory requirements of all those involved in the arbitration, the costs of implementation, and the nature of

risks arising from the use of information technology ('IT') is required for tribunals to be able to consider and give appropriate procedural directions on these matters, the institutional rules and guidance documents may also be viewed as reflecting an expectation, and in some respects a requirement, that arbitrators and counsel will possess basic technological competence.¹¹

When nominating an arbitrator or when seeking to agree with the other party on a joint nominee, a party may consider asking the candidate about their familiarity with and ability to use specific technology tools that might be used in the case. Although technological competency is unlikely in most cases to be an overriding factor in arbitrator selection, it is becoming one of many factors that parties may consider when choosing arbitrators. Arbitrator candidates who lack a basic competence to use and manage the technology currently in use and the tools and processes that will emerge over time may find they are selected by the marketplace less over time. Conversely, arbitrators may find they are at an advantage in the selection process by demonstrating their competence with technology and comfort with its place in the international arbitration process. When asked whether technological competence will be an important consideration going forward in the selection of arbitrators, 51% of respondents to the Survey responded 'yes', 40% responded 'it depends', and only 9% responded 'no'.¹²

If the parties are unable to agree on the sole arbitrator or tribunal president (where the arbitration agreement provides for a joint nomination), each party should provide sufficient information to the appointing authority (e.g. ICC) or the co-arbitrators about the need for the tribunal to be able to accommodate the parties' expected technology needs.

The level of technological literacy that any arbitrator should possess will depend on the parties and the specific case. Not every arbitrator is comfortable with and able to use every technology tool. This can be due to inadequate training, a lack of access to the necessary software or hardware, or inadequate internet bandwidth. For example, some arbitrators may be unfamiliar with, or lack the software necessary to view, certain file types (e.g. Microsoft Project or Computer Assisted Design ('CAD') files). If such competence is required for the case at hand, it may be necessary to train the arbitrators as discussed further below (see Section 3.7 'Technical tutorials or conferences during the arbitration').

3 The Role of Technology in Effective Case Management

3.1 Pre-dispute agreements

In most cases, it is unusual and impractical to address the use of technology in an arbitration at the contract drafting stage as (i) actual requirements may not then be known in sufficient detail and (ii) technology is likely to continue to evolve between the date of the parties' agreement and the commencement of an arbitration. For example, when the dispute arises, will a better IT solution be available than the solution referenced in the arbitration agreement?

Thus, in most instances, it will make more sense for parties to agree to specific IT solutions after a dispute arises (working with counsel and the tribunal), rather than to mandate specific IT solutions in their arbitration agreement. In ICC arbitrations, this could be done, for example, in the context of the

the information being processed or transferred, including whether it includes personal data or sensitive business, proprietary or confidential information. See also IBA Rules on the Taking of Evidence (2020), Art. 2; LCIA Rules (2020), Art. 30A; ICDR Rules (2021), Art. 22(3); CPR Administered and Non-Administered Rules (2018), Art. 9.3(f). More generally on cybersecurity standards, please visit <https://iccwbo.org/global-issues-trends/cybersecurity/>.

11 A distinction should be drawn between IT equipment, training or technical support that an arbitrator needs as a matter of basic technological competence and that which may be required for a specific case. The former is the arbitrator's responsibility. As to the latter, the parties should consider these issues before agreeing to use a particular form of IT.

12 An overview of the Survey results are set forth in Appendix A.

case management conference held pursuant to Article 24 of the ICC Rules.¹³ This approach is more flexible and is also preferred because in most instances, the parties' agreement will also need to be acceptable to the tribunal.

3.2 Party autonomy

Parties and tribunals should always consider how IT solutions may be used to help move the arbitration forward efficiently and to help the parties save time and costs.¹⁴ As noted above, in ICC arbitrations, the parties should try to reach consensus in anticipation of the initial case management conference so it may be discussed with the tribunal. Although the parties may agree to use IT at any stage of the proceedings, they should bear in mind that once substantial written submissions have been exchanged, agreeing on large-scale use of IT may be less efficient and less cost-effective as it could require the parties to redo work previously performed. Thus, the parties are likely to see greater benefit from agreeing to use an online case management platform from start-to-finish of a case (for example) than if they only agree to use it once the evidentiary hearing approaches. The parties should thus make every effort to anticipate the need for IT throughout the case and to plan for its use at the outset of the case.

While the use of technology will frequently lead to efficiencies, that is not always the case and consideration should be given to the specific IT tools proposed, the timing and manner of their implementation, the associated costs, and the IT sophistication and experience of the tribunal, the parties, and other relevant IT users involved in the arbitration.

Technology tools may also be considered for reasons other than savings of time and costs. For example, even though it might increase costs, a party may decide to prepare an e-brief or multi-media presentation to enhance its case presentation and seek to improve the tribunal's understanding of the issues. Other possible drivers of technology tools could include the ability to provide greater security for sensitive data or to facilitate compliance with data protection rules. When a party contemplates using a particular IT solution, any increased convenience should be balanced against increased costs needed to implement the IT in the specific arbitration.

IT use for a party's internal purposes is permissible as a matter of party autonomy, subject to any security or other concerns that may impact the opposing party or the tribunal. For example, the use of a software program to catalogue documents, or otherwise help counsel analyse the issues and prepare for the hearing, should not be the opposing party's or the tribunal's concern. Indeed, the parties are often more likely to have chosen different software or other IT solutions for their internal purposes.

Party autonomy, however, may be subject to limitations where data is to be exchanged or used by other participants in the process, as in the document disclosure phase. To be effective, some IT solutions (e.g. using an internet-based file repository or e-mail as the primary method of communication; electronic service of submissions by a certain time) necessarily require that all parties use these methods, or at least that different systems be compatible. Further, a tribunal may consider it appropriate to require that data be produced in the arbitration in a format that (i) is reasonably accessible to other participants, (ii) takes into account time and cost factors, and (iii) facilitates and does not impede the review process.

If the parties cannot find common ground, they should present their respective approaches to the tribunal, which can then decide and give appropriate directions, considering the views of the parties and the issues described in this Report (and any other case-specific issues).¹⁵

13 All references to the ICC Rules herein are to the **ICC Rules of Arbitration** entered into force on 1 January 2021.

14 Many arbitration rules, including the ICC Rules, expressly recognise that tribunals and parties have a duty to conduct the arbitration in an expeditious and cost-effective manner (see ICC Rules, Art. 22(1)), and some also expressly refer to consideration of technology as a means of enhancing the efficiency and expeditious conduct of the arbitration; see e.g. LCIA Rules (2020), Art. 14.6(iii); ICDR Rules (2021), Art. 22(2). See also Appendix A below reporting that 95% of the Survey respondents believe tribunals should routinely discuss with the parties, during the initial case management conference, how IT may be used to increase the efficiency of, or otherwise enhance, the arbitral proceedings.

15 This Report generally assumes that IT use is a 'procedural matter' that the arbitral tribunal typically will address as part of case management and as to which the tribunal's discretion is limited only by (i) the requirement that the

3.3 Tribunal authority

Because the tribunal is ultimately responsible for the efficiency and integrity of the proceedings, it may wish to be proactive in encouraging the parties to think about the costs and benefits of IT solutions and whether those costs and benefits would be proportionate to the value in dispute. (See sample procedural language in **Appendix B.I**.) As with other administrative aspects of the arbitration, the tribunal has broad powers to manage the use of IT, subject to basic procedural principles of fairness and equal treatment of the parties.

In ICC arbitrations, Article 22(1) requires the tribunal and the parties to 'make every effort to conduct the arbitration in an expeditious and cost-effective manner, having regard to the complexity and value of the dispute'. At the same time, under Article 22(4) of the ICC Rules, and consistent with most arbitral laws and institutional and *ad hoc* rules (e.g. UNCITRAL Model Law), the parties have the right to equal treatment and a reasonable opportunity to present their respective cases. Any directions concerning IT should be consistent with each of these principles, but will necessarily depend upon (i) the nature of the parties' dispute, (ii) the IT that the parties propose to use, (iii) the tribunal's preferences and abilities, and (iv) other case-specific circumstances, such as (a) issues of applicable law pertaining to the conduct of the arbitration, cybersecurity and data protection, (b) questions of proportionality relative to the size and value of the dispute, and (c) disparate resources of the parties (e.g. whether both parties have access to IT infrastructure of comparable quality).

Of course, the principle of fairness and the tribunal's power to manage the proceedings in its discretion continues to apply throughout the proceedings. Thus, the arbitral tribunal maintains the power to adapt or review any agreed technological solution as it considers the circumstances may require. Subject to these considerations, tribunals can be expected to allow a party to use whatever IT the party believes is appropriate to present its case.

Although technology use should generally be party-driven, in certain circumstances, tribunals may require specific IT solutions to be used to make it possible or easier for the tribunal to understand and manage the case (e.g. requiring exhibits to be produced in a searchable electronic format, see Section 4.6 and **Appendix B**). Tribunals might also forbid the use of certain IT if it considers that a solution one or more parties propose would be overly cumbersome or unreasonably increase time and/or costs (e.g. software subject to a disproportionately expensive licence fee). The level of specific guidance that the tribunal will need to provide will depend on the case's factual and legal complexity. For example, a large construction case with multiple claims and a large volume of evidence will likely be managed differently from a commercial dispute where the main issue concerns the proper interpretation of the contract.

Where the parties propose different solutions, the tribunal (and the parties) should consider whether a single approach really is necessary. Thus, for example, if one party proposes to present electronic evidence in a particular format (e.g. TIFF, JPEG, BMP files) and the other party proposes to use another format (e.g. PDF files), the tribunal may conclude that the parties' respective approaches are not materially different, that the evidence will be reasonably accessible to all participants, and that the tribunal need not require a uniform approach. The tribunal also might determine that TIFF and other similar file types should not be the primary format in which documents are disclosed because those file types are not searchable without using an OCR (optical character recognition) process to create a separate text file. On the other hand, if one party proposes to present evidence that can only be viewed

tribunal act fairly and impartially and (ii) each party has a reasonable opportunity to present its case. To the extent that it is implicated in the taking of evidence, IT use may also be viewed as an 'evidentiary matter.' In ICC arbitrations, the tribunal's (broad) power to provide directions on IT flows from Arts. 19, 22, and 24 of the ICC Rules, and, with respect to the specific decision of whether any hearing shall be conducted remotely by videoconference, telephone or other appropriate means of communication, from Art. 26(1).

by using software that is unavailable to a party or a tribunal member, the proposing party should either propose a different approach or make the software available at its expense¹⁶ to everyone who will need to use it.

Further, if a party objects to a specific use of technology, it is necessary to understand why the party objects. Is it because the proposed IT will materially increase costs beyond those that the objecting party reasonably wishes to bear? Are there relevant cybersecurity or data protection concerns? Is there a legitimate concern about fairness or unequal treatment of the parties because of the proposed IT?¹⁷ Or is the objection asserted for another reason?

Particularly where the tribunal considers whether to impose an IT solution over a party's objection, the tribunal should consider the practical implications, in addition to substantive legal and procedural concerns. For example, is the cost of the proposed solution and its complexity proportionate to the amount at stake in the matter? Would the use of a particular IT solution (e.g. an internet-based document repository hosted in a certain country) force a party to violate data privacy laws to which it is subject? If the parties have disparate resources, would a requirement to use a particular solution create an unfair hardship for one party? If an objection is based on alleged unfairness or unequal treatment of the parties, can the tribunal take steps to address and mitigate those concerns? For example, the tribunal might direct that one party bear the cost of the IT solution as a cost of the arbitration subject to later allocation, or adjust the schedule for a virtual hearing to avoid one side participating at unreasonable hours in its time zone.

3.4 Cybersecurity, data privacy, and confidentiality

In recent years, cybersecurity and data privacy have become paramount concerns in international arbitration as they are in society more broadly. International arbitration is not uniquely susceptible to cyber intrusion, nor is it immune. Much of what makes international arbitration attractive to its participants makes it enticing to cybercriminals.¹⁸ International commercial arbitrations routinely involve sensitive commercial and personal information that is not publicly available. The multiple participants in different jurisdictions, including parties, counsel, arbitral institutions, arbitrators, experts and supporting vendors, may have different IT resources and levels of sophistication. Participants are digitally interdependent as the process typically involves the aggregation and transmission of large data sets and collaborative elements.

Proactive attention to cybersecurity and data privacy is required to ensure that international arbitration will maintain its advantage over cross-border litigation as a sophisticated and more private and confidential forum to resolve complex commercial disputes. Unauthorised intrusion threatens more than confidentiality and expectations of privacy; it is a direct threat to the fair, neutral, and orderly process that underlies all arbitrations and public trust in the arbitral process. Reflecting these concerns, parties and institutions now commonly expect that arbitral participants will take reasonable measures to prevent digital intrusion into the arbitral process,¹⁹ and may suggest or require that matters of cybersecurity and

16 Subject to the tribunal's ultimate power to allocate costs in the arbitration.

17 See E. Vidak-Gojkovic and M. McIlwrath, 'Chapter 11: The COVID-19 Revolution: The Future of International Arbitration Is Not Over Yet,' in M. Scherer, N. Bassiri, et al. (eds), *International Arbitration and the COVID-19 Revolution* (Kluwer Law International 2020), pp. 191-202 at 200.

18 See the *Cybersecurity Guidelines (2018)* by the IBA's Presidential Task Force on Cybersecurity.

19 Although individual arbitral participants indisputably have legal and ethical responsibilities to safeguard the data that they import into and use in the arbitration, any view that purports to isolate any one participant as having sole responsibility for cybersecurity and data privacy ignores the inherently interdependent digital landscape and is short-sighted. Any break in the custody of sensitive data may affect all participants, as well as external parties. Accordingly, these obligations, including the necessary minimum level of digital literacy, are both individual and inherently shared responsibilities. Ignorance in this respect and the failure to acquaint oneself with at least the minimum of basic knowledge and abilities which are then applied, may be negligent considering the expectations and professional standards mentioned above. Basic requirements regarding system security may, for example, be gathered from the 'Baseline Security Measures Checklist' at p. 34 of the *ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration* (2020 Edition).

personal data protection be considered at an early stage of the proceedings (at the latest at the first case management conference).²⁰ **Appendix B** contains sample language that tribunals may use to draw issues of cybersecurity and data protection to the attention of the parties in advance of the first case management conference.

‘Cybersecurity concerns’ refer to the protection of data used or generated in the international arbitration process from unauthorised access or disclosure. Arbitrators, parties, counsel, and institutions share responsibility and accountability for cybersecurity, in substantial part because cybersecurity protection is only as strong as its weakest link. Most cybersecurity breaches involve human error, and any arbitral participant may cause a breach, irrespective of the size or sophistication of the practice setting in which he or she works.

The legal industry has become a prime target for cybersecurity attacks because lawyers hold valuable client and other information that hackers are motivated to monetise or use for other unauthorised purposes, often causing significant damage to those whose data is illicitly obtained.²¹ Although international arbitration is not uniquely vulnerable to cybersecurity risks, equally it is not immune from such cyber risks. *First*, as a neutral forum for the resolution of commercial and investment disputes, arbitration often involves parties that sometimes are prominent targets of cybersecurity attacks, e.g. multinational groups, governments or state entities and public figures. The large and complex disputes that these parties submit to international arbitration frequently involve valuable confidential data and require evidence of non-public facts that may have the potential to influence politics and financial markets. *Second*, a key advantage of international arbitration in comparison to litigation in national courts is arbitration’s potential to be a confidential forum. Although the level and scope of confidentiality is variable, some aspects of arbitration, such as arbitrator deliberations, always are confidential. Cybersecurity protection is critical to maintaining international arbitration’s advantages over litigation. *Third*, international arbitration involves actors from different jurisdictions that operate from various settings, as well as extensive communications and data transmission. Parties are typically represented by large and often cross-firm/cross-border teams whose cybersecurity and safety practices and technologies may not be fully harmonised.

To effectively manage cybersecurity risks, counsel, arbitrators, and case participants should be aware of the need to protect against external malicious attacks, and how to avoid and mitigate human error that may result in inadvertent disclosure through everyday actions (e.g. leaving an iPad on an airplane) or falling victim to phishing or social engineering attacks (in which human interaction is used to trick users into making security mistakes and breaking security protocol by sharing their passwords or other sensitive data). According to annual data breach investigation reports by Verizon Enterprise, most confirmed data breaches involve the compromise of weak or stolen passwords.²²

20 See e.g. the ICC **Note to Parties and Tribunals**, paras. 119 and 121 quoted supra note 10. See also IBA Rules on the Taking of Evidence (2020), Art. 2; LCIA Rules (2020), Art. 30A.

21 Although publicly reported instances of cyberattacks involving international arbitrations are rare, in 2021, Brazilian court proceedings staying a partial award in a multibillion-dollar ICC dispute over the sale of a pulp maker exposed sensational allegations that one party orchestrated the hacking of the other party’s servers and thus had access to its confidential and privileged communications, expert reports, and other documents during the arbitration. Brazilian police uncovered evidence of malware used for the cyberattack, but its investigation did not establish who was responsible. In addition to challenging the partial award, the hacked party unsuccessfully challenged the entire arbitral tribunal before ICC on the basis that the counterparty’s allegedly unfettered access to privileged communications during the arbitration had violated principles of fairness and equality of arms and tainted the tribunal. See **‘Brazilian pulp award leads to cyber hack challenge’** (GAR, 12 April 2021); **‘Fancy Buzz Words or a Real Threat? Hacked Evidence in International Arbitration’** (www.iclg.com, 7 July 2021); **‘Arbitrator resigns from Brazilian pulp case’** (GAR, 23 Aug. 2021).

22 The 2017 Verizon report attributed 63% of confirmed data breaches to weak or stolen passwords and the 2021 Verizon report attributed 61% of confirmed data breaches to compromised passwords)., see **‘63% of Data Breaches Result From Weak or Stolen Passwords’** (www.idagent.com, 16 June 2017), **‘Hacking-Related Data Breaches Leverage Compromised Passwords’** (www.securelink.com, 13 May 2021).

In addition to the need for appropriate cybersecurity measures, counsel, arbitrators, and other participants often have legal, ethical, and rules-based obligations to protect the confidentiality of arbitral proceedings, preserve the integrity of the process, and may be required to be competent in technology as part of their larger professional obligations. For example, ICC now advises parties and counsel at the inception of all arbitrations that:

The arbitral tribunal, the parties and their representatives shall put in place and ensure that all those acting on their behalf put in place appropriate technical and organisational measures to ensure a reasonable level of security appropriate to the arbitration, taking into account the scope and risk of the processing, the state of the art, the impact on data subjects, the capabilities and regulatory requirements of all those involved in the arbitration, the costs of implementation, and the nature of the information being processed or transferred, including whether it includes personal data or sensitive business, proprietary or confidential information.²³

Parties and tribunals should ensure that there is a written record of the 'technical and organisational measures' that will apply. Ordinarily, this will be in the form of a procedural order or protocol that the tribunal may amend as changing circumstances may require. Further, it is good practice to ensure that all participants in the arbitration apply cybersecurity measures. For example, parties may want to incorporate measures in expert instructions or the terms of engagement for translators, transcribers, and other service providers who may have access to arbitral data.

A helpful source of more detailed guidance on cybersecurity in international arbitration is the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration ('**ICCA Protocol**').²⁴ The ICCA Protocol has four main objectives: (i) to raise awareness of cybersecurity risks and the importance of information security to maintaining user confidence in arbitration; (ii) to highlight digital interdependence of arbitral participants; (iii) to provide a risk-based framework for parties and arbitrators to determine reasonable cybersecurity measures for their arbitration; and (iv) to provide resources for both basic practice management and arbitration case procedures. The ICCA Protocol is organised in a series of Principles, Commentaries, and Schedules, which provide detailed guidance that is intended to be accessible to non-experts and capable of implementation without undue burden or expense.

The ICCA Protocol provides a non-exhaustive checklist of general cybersecurity measures (Principle 2 and Schedule A) as well as examples of specific security measures that parties may agree to or tribunals may impose (Principle 7, its Commentary and Schedule C). Adherence to reasonable cybersecurity practices in the everyday operation of participants' businesses will provide a firm foundation for the establishment of reasonable security measures in arbitration matters. Where all participants have followed these practices, it may be possible for parties and the tribunal to agree that their existing security measures are reasonable for the arbitration at hand.

The ICCA Protocol states the governing principle that the cybersecurity measures to be adopted for a particular arbitration should be reasonable in the circumstances of the matter (Principle 5), and provides guidance for the determination of such reasonable security measures (Principle 6 and Schedule B). The factors to consider in this risk analysis process may include the subject matter of the arbitration; the identity of parties, key witnesses, or other participants (including the arbitral institution and experts); the industry and/or subject matter of the dispute; the size and value of the dispute; and any consequences of a potential breach.

Principle 10 recommends that arbitral participants consider cybersecurity issues early in the arbitration process, preferably no later than the first 'case management conference' held in accordance with Article 24 of the ICC Arbitration Rules. Principle 11 provides that '[t]aking into consideration Principles 4-9 as appropriate, the arbitral tribunal has the authority to determine the information security measures applicable to the arbitration'.

²³ ICC Note to Parties and Tribunals, para. 121.

²⁴ Supra note 19.

The ICCA Protocol recognises party autonomy as a fundamental attribute of the arbitral cybersecurity process. Principle 9 suggests that parties should attempt to agree reasonable cybersecurity measures among themselves. The Commentary to Principle 11 further emphasises that the arbitral tribunal should defer to any reasonable agreement the parties have agreed between themselves ‘subject to overriding legal or other obligations ... and unless there are significant countervailing considerations’.

Specific security measures listed in Schedules A and C of the ICCA Protocol relate to the following areas:

- > **Asset management.** Parties and the tribunal should be familiar with the assets, infrastructure, and sensitive data that will be involved in the arbitration. It is important to minimise and protect sensitive data by redacting information or adding confidentiality designations to the names of documents or folders. It is also recommended that parties avoid maintaining unnecessary copies of digital or physical files and establish document retention and destruction practices.
- > **Access controls.** Arbitration participants should consider access control policies designed to limit access to information to individuals on a ‘need-to-know’ basis only. Appropriate protective measures may include the redaction or pseudonymisation of data, labelling confidential or sensitive data as such, limiting the information shared with the arbitral tribunal to that required for adjudicatory purposes, and the use of secure share sites or cloud platforms for the sharing and storage of arbitral documents (with provision for the secure sharing of passwords for such sites).
- > **Encryption.** Arbitration participants should consider encrypting data in transit, file-level encryption and enabling full-disk encryption to guard against unauthorised access of digital information due to loss or theft of a laptop or other mobile device. Files saved onto a cloud storage service also should be encrypted and, ideally, such services should employ zero-knowledge encryption, meaning that secured data can be accessed only by the subscriber and not by the service itself.
- > **Communications security.** Arbitration participants should make provision for procedures concerning communications between and among the tribunal, parties, and arbitral institution. Such procedures may include the requirement that only business or enterprise level e-mail accounts be used in the arbitration; restrictions on the use of e-mail files/ attachments to transmit confidential or sensitive information; requirements for the use of cloud platforms, including regarding user passwords, multi-factor authentication, and remote access protocols; and limiting or excluding the use of certain types of media, such as portable drives.
- > **Physical and environmental security.** Arbitration participants should also secure paper files, refrain from leaving documents/devices unattended and guard against ‘visual hacking’ when in transit or public places by installing privacy screens on laptops and mobile devices.
- > **Operations security.** Tribunals and counsel should consider a requirement that all participants use professional or commercial level products and tools and not share their devices and accounts. Arbitration participants should also guard digital perimeters by using measures such as firewalls, antivirus, and anti-malware and anti-spyware software, and install software updates and patches to their operating systems and other software applications.
- > **Information security incident management.** Tribunal and counsel may consider the need to develop in advance a response plan on how they would respond to any cybersecurity breaches.

3.4.1 Obligations concerning cybersecurity breaches

The ICC Note to Parties and Tribunals provides for certain notification obligations irrespective of whether the parties have agreed to a specific incident management plan in the arbitration:

Any breach of the security and confidentiality of personal data, such as unauthorised access to or use of personal data or inadvertent disclosure to persons who should not have been identified as recipients, must be reported immediately to the individual whose personal data may be affected and to the Secretariat. Pursuant to the applicable data protection laws and regulations, ICC, when it acts as data controller, must notify the competent supervisory authority and as the case may be the concerned individuals of such breach.²⁵

Further, in the event of breach, arbitral participants should comply with breach notification requirements and other obligations that may apply as a matter of law or regulation. Participants may be required to seek guidance regarding the requirements of more than one jurisdiction and potentially to reconcile differing requirements.

Parties may also consider regulating other implications of cybersecurity risks. For example, they may agree that evidence obtained through hacking activity shall not be admissible. They may also agree the forum where any dispute arising out of a security breach should be resolved.

3.4.2 Data protection obligations

Arbitral participants also are required to comply with data protection and privacy laws and regulations that may apply to the collection, retention, and processing of data in the arbitration. These include the European Union's General Data Protection Regulation (GDPR) and similar laws and regulations in other jurisdictions. Detailed guidance on data protection issues is available in the ICCA-IBA Roadmap to Data Protection in International Arbitration,²⁶ which focuses on nine principles that are common to modern data protection laws adopted around the world: 1) fair and lawful processing; 2) proportionality; 3) data minimisation; 4) purpose limitation; 5) data subject rights; 6) accuracy; 7) data security; 8) transparency; 9) accountability.

3.5 Allocation of costs

If the tribunal requires an IT solution to be used (e.g. an online case management platform), it may consider whether the reasonable costs incurred to comply with the tribunal's directions should be advanced by one or both parties and if such costs should be considered potentially recoverable from the losing party as part of the costs of the arbitration, unless the parties agree, or applicable rules provide otherwise.²⁷

The tribunal may also consider whether the cost of every IT solution that a winning party uses to present its case should automatically qualify as a cost of the arbitration subject to potential allocation. Among other factors, the tribunal may weigh whether a particular IT solution was adopted specifically for the matter at hand, whether it forms part of the regular infrastructure maintained by a party or its counsel, and whether the use of the solution is proportionate to the size and complexity of the matter.²⁸ IT that may be appropriate where the amount in controversy is US\$ 50 million but may not be appropriate where only US\$ 5 million is in controversy. Also, the confidentiality or sensitivity of the information presented may dictate the solutions that are needed to manage that information. A different solution might be used where the information is not commercially sensitive and where, for example, the case involves trade secrets.

25 ICC Note to Parties and Tribunals, para. 122

26 ICCA-IBA Roadmap to Data Protection in International Arbitration (Public Consultation Draft, Feb. 2020).

27 The vast and sometimes controversial subject of costs in international arbitration was studied in the ICC Commission and ADR's Report 'Decisions On Costs In International Arbitration', which readers are encouraged to consult given that most issues related to costs are beyond the scope of the present Report.

28 See ICC Report 'Managing E-Document Production', paras. 5.20-5.23.

The parties may prefer to agree early in the proceedings on how certain costs should be borne. In general, the tribunal should always encourage consensus before, or at, the initial case management conference. Otherwise, the tribunal may decide as the issue arises or in the final award allocating costs. For example, if one party wishes to use real-time court reporting with immediately displayed transcripts at the hearing, should this expense be part of the costs of the arbitration? The parties might agree that it should not. Ideally, any such agreement should be presented to the tribunal for approval and incorporated in a procedural order. In many instances, the tribunal may find it convenient to require the parties to share IT-related costs equally initially and reserve the ultimate allocation of IT costs to the final costs determination.

3.6 Technical problems during the arbitration

In anticipation of the possibility that technical issues arise during the arbitration, such as when an arbitrator has trouble accessing a memorial and exhibits from a file share site, it may be helpful for each party to designate technical support persons who may be contacted in case of technical difficulty, and in lieu of contacting the full distribution list of case participants. While each party should be on notice of the issue through notification to its representative and should be entitled to participate in the related discussion at its discretion, in most cases it will not be necessary to burden the full distribution list with technical support issues. (Sample procedural language to this end is included in **Appendix B.**)

In any event, at their own initiative, parties should promptly replace corrupted files, inoperable links, attachments that cannot be opened, and illegible copies as soon as they become aware of the problem and regardless of whether the tribunal or the other party has complained. However, parties should not unilaterally replace any documents (in a shared file repository, for example) that might compromise the arbitration record.²⁹ These same principles should apply to any other technical issues that may arise, such as the inoperability of required software and hardware, the availability of IT as needed during the arbitration, and the detection and remediation of other technical problems.

3.7 Technical tutorials or conferences during the arbitration

As necessary, the party that uses a particular form of IT may need to provide the tribunal and the other party with instructions or training on how to use it. For example, in a complex construction case, a party might wish to use an online demonstrative exhibit that allows the tribunal and the opposing party to view a photograph of the project and to access other relevant exhibits pertaining to different aspects of the project by clicking on the relevant parts of the photograph or model. The party producing the demonstrative exhibit should be responsible for providing basic instructions to the tribunal and the other party on how to access and use the exhibit.

As in any case that involves a technical issue, if the arbitrators need training regarding technology that will be used for the arbitration (such as a particular software), the tribunal should schedule a tutorial session (or sessions) before use of the technology is required. Optimally, the format and content of the training should be agreed by the parties and it should not be used as a platform for any party to introduce evidence or advocate its merits position in the arbitration. The trainers could be counsel, other representatives of the parties, or a third party. The third party could be someone whom the parties recommend, or an expert whom the tribunal appoints pursuant to Article 25(3) of the ICC Rules. Given the ease with which a virtual meeting may be convened using web-based videoconferencing technology such as Cisco WebEx, Microsoft Teams, or Zoom, parties and tribunals may consider conducting any such tutorials or training demonstrations as 'hands-on' conferences via videoconference.

²⁹ As suggested in the discussion on online case management platforms below (Section 4.2.4) it may be appropriate for parties and tribunals to adopt agreements or procedural orders pertaining to the steps to be taken in the event that data corruption is detected or suspected, in order to ensure that data integrity is not compromised.

Further, it is reasonable to anticipate that there will be an ongoing need to learn new technology and to procure new equipment, as illustrated by the collective experience during the pandemic when the arbitration community shifted to relying on web-based videoconferencing platforms to regularly convene case management conferences and evidentiary hearings, and most arbitral participants were forced to learn new technology and/or procure new equipment (e.g. webcams). This experience is a good reminder that rather than assuming that arbitral participants required to use specific technology will have adequate training, equipment, and resources — and to avoid technical disruptions with the potential to prejudice a party's ability to present its case — parties should confer regarding the technology that will be implemented in the matter, seek procedural directions as necessary from the tribunal, and confirm the technology approaches in a procedural order. In the case of virtual hearings, the tribunal will ordinarily ensure that advance technical testing is arranged with the parties and other participants, with each joining from the locations and devices they plan to use for the hearings, in order to ascertain for itself that the technology will be adequate to allow the parties to present their cases, and to identify whether any remedial measures will be required for a fair and effective process. (See the arbitrator's and counsel's 'Checklist to Prepare for Virtual Hearings', Checklists IV and V in **Appendix C.**)

4 Electronic Exchange of Communications, Exhibits, and Other Submissions

In the typical international arbitration procedure today, notifications and communications are exchanged electronically (most often, by e-mail) (see Section 4.2). Parties and tribunals also may wish to consider supplemental or alternative means of exchange (such as online case management platforms) as well as whether proceedings will be fully paperless or if hard copies sometimes may be required (e.g. for the hearing). The following section provides an overview of these related issues and is supplemented by sample procedural language that may be considered by parties and tribunals, in **Appendix B.**

4.1 Applicable arbitration rules and mandatory law

Various major arbitral institutions have revised their arbitration rules and practices to eliminate requirements to provide the institution with communications and filings in hard copy form (or to prohibit such submissions) and to permit (or require) notification of requests for arbitration and subsequent communications during the arbitration to take place electronically. In lieu of requiring hard copies 'sufficient for each party, each arbitrator and the ICC Secretariat', Article 3(1) of the 2021 ICC Rules provides for pleadings and written communications to be 'sent' to such persons, without specifying any form and Article 4(4) requires such hard copies only 'where the claimant requests transmission of the Request by delivery against receipt, registered post or courier'. Thus, subject to any mandatory rules of law, parties are free in ICC arbitrations to choose the form of their communications, but also encouraged to rely on electronic communications. Documents that may be exchanged electronically include: (a) correspondence (between counsel, among the tribunal and the counsel or the parties, among tribunal members, and with the arbitral institution); (b) pleadings; (c) exhibits and other documents disclosed; (d) hearing briefs, witness statements, and other written submissions; and (e) orders, awards, and other decisions.

A multi-jurisdictional analysis of the validity of e-mail and other means of telecommunication that provide a record of sending for the transmittal of notifications or communications during an arbitration proceeding is beyond the scope of this Report. The Working Group sent ICC National Committees a questionnaire asking whether they were aware of any mandatory law or rules in their jurisdiction that may preclude using e-mail or other means of telecommunication that provides a record of sending to: (i) commence an international arbitration; (ii) serve other notifications or communications during an arbitration proceeding; or (iii) notify Terms of Reference, an arbitral award, or other arbitral decision (such as a decision on interim measures). National Committees were also invited to identify any relevant court decisions.

Out of the 36 responses received to our country questionnaire,³⁰ a few reporters suggested that party consent to electronic communications and notifications should be recorded (e.g. in the Terms of Reference),³¹ but otherwise notes of caution about relying on electronic communications and notifications during arbitration proceedings (i.e. between initiation and award) were limited.³² Notably, reporters for Ghana and India commented that courts in their jurisdictions have favourably considered the validity of electronic communications and notifications by means other than e-mail, such as Facebook message, WhatsApp message, and text message.³³

In a few instances, the reporters either stated express requirements for giving hard copy notice of the commencement of an arbitration (i.e. in Nigeria, notification is to be made by post) or an award,³⁴ or suggested that doing so was recommended in addition to electronic notification even if not strictly required.³⁵ In addition, several reporters flagged potential issues with relying on electronic notification of an award due to legislative requirements for an 'original' or certified copy for recognition and enforcement purposes, and expressed uncertainty about whether the printout of an award notified electronically would be sufficient.³⁶ The Working Group observes that such uncertainty arises from questions about the legal validity of different kinds of (electronic) signatures, which is addressed separately below (Section 4.8).

4.2 Methods of electronic exchange

Methods of electronic exchange that may be used in an arbitration include those described below. Regardless of the mode of transmission, the sending party should take steps to verify that a given message has been received by the addressee. Receiving parties, including tribunal members, should promptly confirm both their receipt and successful access to electronic files. As discussed above, it may be convenient for each party to designate an IT contact to assist with technical difficulties at least in the first instance.

-
- 30 Responses were received from the following National Committees: Albania, Austria, Belgium, Brazil, Canada, China, Colombia, Costa Rica, Croatia, Czech Republic, Finland, Germany, Ghana, Greece, Hong Kong, India, Indonesia, Italy, Lithuania, Luxembourg, Macedonia, Malaysia, Mexico, Netherlands, Nigeria, Poland, Romania, Spain, Switzerland, Tanzania, Turkey, United Kingdom, United States, Venezuela, and Vietnam. The overview provided in this Report should not be taken as a complete and accurate statement of the law in any of these jurisdictions; rather, it is intended to assist parties and tribunals in identifying potential legal issues warranting further independent research and investigation.
- 31 China, Netherlands, Spain.
- 32 Special notification requirements were reported for Costa Rica (where a public notary must give notice of the commencement of arbitration proceedings) and the Czech Republic (pursuant to the Czech Arbitration Act, arbitrators are to serve Terms of Reference, decisions, and awards to data boxes for the parties (special electronic boxes for document service) or, if this is not possible, by e-mail; further, if a request for arbitration is notified by e-mail, follow-up service by hard copy sometimes may be required within three days).
- 33 The reporter for Ghana noted courts have held that notifications in court proceedings may be by Facebook message or WhatsApp. The reporter for India noted courts permitted service by way of e-mail as well as WhatsApp and text message in *Tata Sons Limited & Ors. v. John Doe(s) & Ors.* (2017 SCC Online Del 8355, para. 3).
- 34 In Thailand, awards and other arbitral decisions must be notified by registered mail. In Italy, an original or certified copy of an award must be mailed or delivered to parties within ten days.
- 35 The reporter for Indonesia stated that unless the parties' agreement expressly provides for e-mail notification, personal service of a request for arbitration is recommended. No comment was made about the effect of institutional rules permitting e-mail notification. The German reporter stated that Sect. 1054(4) of the German Code of Civil Procedure is intended to permit electronic transmission, but, in practice, awards are generally also sent by courier or mail.
- 36 According to the Belgium reporter, courts require an 'original' or certified original of an award for recognition and enforcement, as distinct from 'digital' copies of awards which are generally accepted for exequatur applications absent doubts about authenticity. Greece's reporter similarly noted that the Greek Arbitration Act provides that an 'original signed hard copy of the arbitral award should be communicated to each of the parties', but explained that it is unclear whether such signature must have been handwritten or could be electronic. Reports for Poland and Romania expressed uncertainty about whether the printout of an award notified by e-mail would be sufficient for recognition and enforcement.

4.2.1 E-mail

At present, e-mail is the predominant means of exchanging communications, exhibits, and other submissions in international arbitration. But e-mail presents certain risks and drawbacks, including that the confidentiality or integrity of the data may easily be compromised (e.g. by inadvertent forwarding) and file size limitations imposed by e-mail service providers sometimes preclude e-mail distributions. Most e-mail systems place an arbitrary limit on the size of attachments that can be sent or received (e.g. 50 MB or even less). As a practical matter, unless attachments are sent in separate batches or compressed³⁷ into a so-called archive (e.g. ZIP,³⁸ TAR³⁹ files), this means that e-mail is not an efficient means for sharing large volumes of data, and even compressed files may exceed size limitations.⁴⁰ Accordingly, it would be prudent to clarify at the outset of the proceedings whether any party or tribunal member is subject to technical restrictions on the size of e-mails/attachments that can be received. If so, the tribunal could specify a size limit for individual messages in a procedural order.

4.2.2 File share transfers

Given issues transmitting voluminous files by e-mail, it has also become common in international arbitration for parties to supplement or replace e-mail transmission of voluminous submissions via secure file share transfer sites, often referred to as FTP (file transfer protocol) sites. FTP servers and other web-based protocols present a convenient and arguably more secure alternative to physical data carriers. On the other hand, using FTP to upload and transfer extremely large volumes of data (e.g. in a construction arbitration) may cause some practitioners (or IT departments) to become impatient.

If the server is under the physical control of the uploading party, confidentiality should not be an issue. Typically, the uploading party's attorney would provide the other party's attorney and, in the case of formal submissions, the tribunal, with a link and password enabling them to download the data into their respective systems, copying ICC or other administering institution on the initial transmittal e-mail. Once the data has been downloaded, it can be removed from the FTP server.

As an alternative, some parties opt for free, consumer file storing and sharing services, such as Box, DropBox, Google Drive or Google Docs, Microsoft One Drive, FileSwap.com, hubiC, AjaXplorer, -okeanos, Firedrive, among others. Use of free consumer-oriented services for commercially sensitive information may raise concerns such as: Who really has access to the information? Can it be accessed by anyone without authorisation (whether through hacking or otherwise)? Once placed on the internet, can the information be completely deleted or otherwise rendered inaccessible? What rights does the service provider have under its terms of use? Is the use of the online services permitted by the professional rules to which the parties' representatives and the arbitrators are subject? Because many of these services are also available as professional business accounts that do not suffer from these risks, parties should always consider whether enterprise-grade rather than free consumer services are available.

Whenever choosing a secure FTP, the parties and the tribunal should carefully read the terms and conditions offered by the provider of the service. In particular, they should pay attention to the following: (i) the location of the secure server, which may impact the confidentiality of any data being stored (e.g. for purposes of the GDPR or other data protection law or regulations); (ii) whether the data stored on the server is encrypted; and (iii) the authentication procedures to access the data, i.e. multi-factor authentication (preferable) or simple password-protection.⁴¹

37 See https://en.wikipedia.org/wiki/Data_compression.

38 See <https://en.wikipedia.org/wiki/Zip>.

39 See https://en.wikipedia.org/wiki/Tar_%28computing%29.

40 Among other techniques, files attached to e-mails can be sent compressed and encrypted in a password-protected ZIP archive. To enhance security, the sender might provide all recipients with a single-use password of at least eight characters, sent separately by text message to their mobile telephones or, less ideally, in a separate e-mail.

41 Because it may be necessary to use the same site throughout the arbitration, it may be helpful to store any password in a secure password manager such as *1Password* or *LastPass*. Passwords should be stored in password management

4.2.3 Physical data carriers (e.g. flash drives, hard disks)

In the past, it was more common to provide documents on flash drives or other portable media than via FTP sites. Large volumes of data can be conveniently and inexpensively transmitted by copying the data onto a portable flash drive, which one party physically delivers by courier to the other party's counsel and the tribunal. Nevertheless, the use of portable media for this purpose has declined as this method presents risks of loss of the device itself, corruption of the files with malware, and other security risks and because of the wider availability of secure enterprise-level FTP services. Some law firms, corporations and institutions no longer permit the use of these external devices on their systems.

To the extent that these external drives are used, the parties and the tribunal should take reasonable steps to protect the data. Appropriate measures of protection could include: (i) using only reputable courier services, which can be trusted with the protection of the integrity of any packages and parcels; (ii) using encryption software on the external drive so that, if the drive does fall in the wrong hands, the data on the drive cannot be accessed; for instance, various manufacturers of USB drives (e.g. Kingston, Verbatim) offer several encryption solutions from the more common (password protection, with automatic deletion of data upon a number of unsuccessful password entries) to the more sophisticated (military-grade encryption); (iii) whenever receiving an external drive, the drive should be scanned for viruses and malware prior to its use; and (iv) the drive should be appropriately labelled for easy identification and stored in a safe location (preferably using password management software). A protocol also should be agreed for the disposal of the portable media at the conclusion of the arbitration, consistent with the retention provisions that apply to other materials in the case.

4.2.4 Online case management platforms

File sharing services are a key feature of online case management platforms. Unlike file sharing services, online case management platforms tend to be customised for the needs of the legal profession and consequently offer additional features expected to enhance workflow and improve security.

A secure case management platform administered by an arbitral institution or neutral third party allows parties to upload, share and store all documents for a case (e.g. correspondence, pleadings, witness statements and exhibits) in a single location, thereby avoiding the need to prepare hard copies of pleadings and evidence and facilitating case participants' ready access no matter where they may be located or whether they are traveling. Some platforms function merely as a joint repository for all written materials in a case, while other solutions have broader functionality and include features that permit evidentiary hearings with witness examinations to be conducted through the platform.

Parties opting for an online case management platform should look for more sophisticated features than those offered by general file sharing sites. These features best allow parties to enhance their understanding and presentation of the evidence, e.g. by creating hyperlinks to exhibits referenced in memorials or allowing comments and annotations on evidence to be viewable and accessible by all members of a counsel team. Typical features of online case management platforms may include automated upload and download notifications by e-mail, sophisticated administration of users' rights, sub-spaces accessible only to certain categories of users (e.g. properly restricting access to outside attorneys' eyes only documents), annotation and search functionalities, 24/7 technical support, etc. If a dispute arises over the authenticity or integrity of electronic copies of evidence, the tribunal can still permit inspection of the original documents or metadata, just like in cases where the parties submit printed copies of exhibits.

software by reference to simple and clear reference points (e.g. case number, names of the parties), as opposed to the ambiguous reference points (e.g. name of FTP site, which could be used by multiple senders but in different cases).

Interest in the use of online case management platforms as a means of exchange among the parties, tribunal, and administering body continues to grow, and we may see new (or even mandatory) initiatives in this respect from arbitral institutions in the future. The ICC, for example, is presently designing a secure digital platform for communications and file sharing, with phase 1 launch expected by June 2022.⁴²

If an arbitral institution launches its own case management platform, use of the platform is likely to become mandatory, at a minimum, for managing communications that involve the institution. In those circumstances, the institution can be expected to dictate general standards for the platform's use, such as for user access rights and other important cybersecurity controls, as well as default rules for the naming and organisation of documents that are uploaded to the platform. If, however, an institution has not launched its own case management platform, the parties and tribunal may decide whether to use such a platform and, if so, which platform is the most suitable. There are different third-party alternatives in the market such as Opus, Transperfect, Xbundle, and others.

To better assist parties and tribunals in navigating the various options⁴³ that may be available, **Appendix E** of this Report provides a short checklist of basic issues to be considered before selecting an online case management platform. When using a shared platform, three issues merit particular attention:

- (i) *Standardisation.* Unless the parties agree on (or the tribunal orders) specific protocols for the data to be uploaded (e.g. with respect to metadata and load files), standard file types for information in the database, and naming conventions for organising and uploading documents, the database may not be accessible or searchable with the degree of reliability that the parties and the tribunal require.
- (ii) *Control.* In an adversarial setting, it is not generally recommended that one party host and control a shared database as there is a risk of gamesmanship. If this does happen, however, the parties and the tribunal should consider how disputes over access to that database and its quality and reliability might be avoided.
- (iii) *Data integrity.* Using a joint set of data in a common database implies access by multiple users who are authorised to add and possibly modify data. Although there is a potential risk of unintended changes or even bad faith manipulation, the database platform normally will contain tools to maintain the format and integrity of documents and to detect and prevent data corruption. It may be appropriate, however, to include in the agreement or procedural order pertaining to use of the platform agreed steps to be taken in the event such data corruption is detected or suspected.

4.3 Exceptional circumstances warranting non-electronic exchange

The main advantages to exchanging documents electronically are convenience, reliability, and speed. Nonetheless, depending on the case's specific facts, it may be prudent to exchange some or all case-related materials through non-electronic means instead of, or in addition to, using electronic means of communication.

- (i) *Material concerns about confidentiality and cybersecurity that cannot otherwise be mitigated.* When sensitive data is transmitted, a party may have legitimate concerns that electronic communications could be intercepted (surreptitiously) by governmental authorities or other third parties. Although there are many cases in which heightened

42 Recently, various institutions have launched new digital case management platforms, including the HKIAC and SCC (for its cases as well as for *ad hoc* arbitrations).

43 A recently published **Protocol for Online Case Management in International Arbitration** (Nov. 2020, Working Group on LegalTech Adoption in International Arbitration) takes a deep dive into the benefits of online platforms and the spectrum of features that are available for use in arbitration. Parties that believe such a platform may be a viable solution for their case are encouraged to consult such publication for detailed guidance.

security measures such as the use of encrypted e-mails may be a solution, in extreme cases, legitimate concerns may remain. In these circumstances, the tribunal may consider giving the parties the option to transmit the sensitive information by courier or by another method (e.g. hand delivery, if feasible) where such a method appears more likely to ensure timely and secure delivery of the submission.

- (ii) *Legitimate concerns as to whether the electronic communications will be received.* If a party's counsel is in a country where e-mail communication is not reliable enough to ensure that e-mails sent to or from the country will be received by their intended recipients, e-mail should not be used. It may also be prudent to send hard copies via courier in instances where there is a defaulting party and it cannot be certain that e-mails have been duly received.

4.4 Whether hard copies will also (or sometimes) be provided

4.4.1 Tribunal members

Paperless proceedings are generally more efficient and cost-effective, but whether the tribunal will forego or require hard copies will depend on the circumstances of the case and the preferences of the tribunal or its individual members.

When the first version of this Report was issued, some anecdotes from arbitration practitioners suggested that there were arbitrators who refused to communicate by e-mail or at least were reluctant to do so.⁴⁴ Until recently, although communication via e-mail and other electronic means for routine communications and submissions had certainly become standard for nearly all parties, tribunals and ICC, the practice of parties sending all or at least some communications and submissions in duplicate hard copy (especially to one or more arbitrators) often persisted. This practice can probably be attributed, at least in part, to a lack of familiarity with both the range of IT tools that can be used in conjunction with a tablet and a stylus or digital pencil (or on a computer with the mouse or trackpad) to mimic the way one might mark-up paper submissions with highlighting or notes (including popular annotation software such as Adobe Acrobat Reader, Drawboard, iAnnotate, LiquidText, Notability, PDF Annotator, and PDF Expert) and with other IT solutions that can enhance paperless review, including e-briefs with embedded hyperlinks to cited exhibits and legal authorities and full-text searchability. However, some arbitrators may perceive that they absorb and recall more information when they read it in paper form rather than on a screen or simply prefer paper, which could potentially justify a combination of electronic and hard-copy submissions (e.g. paper copies of memorials might be required but not exhibits) rather than a fully paperless proceeding.

Because mail and courier services were sometimes disrupted during the pandemic, reliance on paperless proceedings has increased and more parties and arbitrators will have been exposed to the potential benefits and efficiencies of paperless proceedings than ever before. Since the Survey on IT use suggests that parties and arbitrators may be more willing to be all or mostly paperless in the future, it will be especially important to confirm going forward that old practices of sending duplicate hard copies and personal preferences of the tribunal are discussed, not assumed.

44 The results of work undertaken by an ICC task force to study and make recommendations on the use of information technology in arbitration proceeding were first published in 2004. ('Issues to be Considered when Using IT in International Arbitration'). See at '3.2 Electronic exchange of documents': 'Are the arbitrators willing to exchange documents electronically? If members of the tribunal lack access to the technology necessary to enable them to do so, or if they simply find IT inconvenient for their working method, the parties may be willing to exchange documents electronically between themselves even though the tribunal receives the documents by non-electronic means'. A second edition ('An Updated Overview of Issues to Consider when Using Information Technology in International Arbitration') was published in 2017. All ICC Commission on Arbitration and ADR Reports are available at <https://library.iccwbo.org/dr-commissionreports.htm>.

A distinction may also be made between courtesy copies during the ordinary course of the proceedings and in preparation for the hearing. Among other things, tribunal members may consider whether they require paper copies to prepare for the hearing or merely a compilation of core materials in one location, which could be done by electronic means. (See **Appendix B.III**, ‘Sample Wording for First Procedural Orders’, Examples III.4, III.5, and III.10.)

4.4.2 Hearing witnesses

Regardless of whether witnesses testify at a physical hearing or virtually, it is not uncommon for the witness to have paper copies of hearing exhibits while testifying, even if electronic copies of the same exhibits are projected on a screen. The provision of paper copies to the witness in a bundle or exhibit book may provide the witness the opportunity to flip through and consider the entire document, rather than merely view an electronic image of a single page of an electronic document. Paper copies of hearing exhibits also may be easier for some witnesses to see and thus read during their active testimony.

Electronic means are available to ensure that witnesses are able to read exhibits in full. Depending on the volume of exhibits at issue, for example, it may be more cost-effective and convenient to provide the witness with a handheld tablet that contains the exhibits. Or, if documents are screenshared using a videoconferencing platform, it may be possible to give the witness ‘remote control’ functionality permitting the witness to scroll through the document on their own.

4.5 Electronic file organisation and naming conventions

In any situation where data is shared electronically, the parties and tribunal should agree on an appropriate numbering and naming convention that will enable the parties to efficiently identify and retrieve particular documents. If the documents are exhibits, they should be indexed and the naming convention would usually have some or all of the following elements: exhibit number, date, description, and a bates-number range.

Especially in complex cases involving multiple claims and issues, agreeing on templates for the presentation of certain information or the description of documents (e.g. e-mails, spreadsheets, tables) in an agreed format may help the parties and the tribunal to manage certain information more efficiently and thereby save time and costs. (See **Appendix B**, ‘Naming conventions’ below Example III.4.)

4.6 Prescribed rules for file format

4.6.1 For convenience

Particularly in large, complex cases, it is typical to require that all exhibits or submissions are submitted in a text searchable format. Traditionally, this required that parties engage expensive third-party vendors to use optical character recognition (‘OCR’) technology to extract text from scanned paper documents or image files. Software such as Adobe Acrobat is now readily available to facilitate this process without significant time or expense, even in small cases. This feature (the conversion of documents into searchable text) may also be a tool that is included in online document management platforms.

E-briefs or e-bundles may also be considered (see Section 5.1).

4.6.2 Data integrity issues

Based on available anecdotal evidence, data integrity issues are rarely identified in arbitration proceedings, and usually do not cause any substantial disruption of proceedings. Nonetheless, this is a potentially critical aspect of IT use, and users need to be alerted to the possible risks, to which they sometimes surrender too readily in exchange for the ease and convenience of IT use.

Like printed information, electronically stored information can be improperly manipulated unless certain precautions are taken. Indeed, it is much simpler to manipulate electronic records. In most cases, however, many copies of the same file exist in different places, thus allowing comparisons to be made and falsifications detected whenever suspicions arise.

To preserve the integrity of the documents, the parties and the tribunal could use file formats that (i) guarantee that the formatting of the original document is maintained, and (ii) contain a protection against later modifications and/or facilitate tracking of any modifications.

To ensure that information is not altered *after* it has been produced in the arbitration, parties usually produce most information in a format that makes alteration more difficult, such as a Bates-numbered PDF or other graphical file format,⁴⁵ rather than in native format. For e-mails and other correspondence, this technique works well.

Where the information produced is from an Excel or other spreadsheet file, however, production in TIFF or PDF format may render the information comparatively difficult to read and also limit its usefulness. This is because production in TIFF or PDF format does not preserve the functionality (e.g. formulas and interactivity) that exists in native format. For this reason, the parties will often agree, or the tribunal will direct, that Excel and certain other files should be produced in native format, instead of or in addition to TIFF or PDF.

To ensure that the information produced was not altered *before* production, commercially available software can be used to verify an electronic 'signature',⁴⁶ which provides information as to whether the purported originator is the real author and whether the electronically signed file was modified after signature.

In some cases, the parties may also wish to have access to metadata (i.e. embedded data about the data and its properties)⁴⁷ that would show, for example, the time files were produced and accessed, and if and when they were altered. Unless the authenticity or possible alteration of data is a legitimately disputed issue in the case, however, most parties will not designate metadata as part of an exhibit. Nonetheless, as discussed above, the tribunal may consider it appropriate to require that data be produced in a format that facilitates rather than impedes review.

For documents and copies of documents that were created without an electronic signature, the use of IT raises no greater concerns in this respect than the exchange of hard-copy photocopies, which, for example, could have been made from a printout of an electronically manipulated, scanned document. Ultimately, the parties and the tribunal must retain the right to inspect the originals of any documents whose authenticity is disputed.

If there are sufficiently substantiated concerns regarding whether information may have been altered, the parties could agree or the tribunal could provide directions (i) on interoperable programs to be used electronically to sign and verify files; and (ii) on related matters such as the exchange of electronic trusted certificates or electronic keys required for signing and verification.⁴⁸ This would allow the originator of the signed file – but not necessarily of its content – to be identified and the integrity of the data to be verified as of the moment the file was electronically signed. No system is 100% secure or foolproof, however.

This type of issue is usually irrelevant in all but a handful of cases. Normally, the level of trust between the tribunal and the parties will be sufficiently high (or concerns about proportionality will dictate) that such additional directions would be unnecessary.

45 E.g., JPEG, TIFF, BMP. See http://en.wikipedia.org/wiki/Comparison_of_graphics_file_formats.

46 See <https://en.wikipedia.org/wiki/Authentication>; https://en.wikipedia.org/wiki/Electronic_signature and https://en.wikipedia.org/wiki/Data_integrity.

47 See <http://en.wikipedia.org/wiki/Metadata>.

48 See http://en.wikipedia.org/wiki/Electronic_signature; <http://en.wikipedia.org/wiki/Authentication> and http://en.wikipedia.org/wiki/Data_integrity.

4.7 Proof of service

Most systems of law and many contracts set out minimum requirements for proof of delivery, increasingly also in respect to electronic communications. Specific rules for proof of delivery may be included in relevant arbitration rules (e.g. Arts. 3(2) and (3), ICC Arbitration Rules) or may be issued by the tribunal. Under Article V.1(b) of the New York Convention (1958), these requirements affect the parties' rights to enforce the arbitral award, and thus should be verified before electronic communication is used to effect service.

Usually, the transmission and receipt of information by e-mail will not be controversial. If necessary, directions concerning some or all of the following precautionary measures could be considered: (i) duty to check electronic mailbox or website hosting a document repository at certain intervals (e.g. daily); (ii) duty to acknowledge receipt with copy to all, especially the tribunal; and (iii) directions regarding what happens if receipt is not acknowledged within a certain period of time.

Many e-mail programs can generate acknowledgements of receipt, which are electronically returned to the sender if this functionality is activated. Moreover, as a matter of courtesy and effective case management, it would be a simple matter to agree on the requirement that any recipient manually generate and send an electronic acknowledgement of receipt and confirm its successful access to the files. Internet-based document repositories/data rooms can make it possible to track access. If this functionality is not offered by an internet service provider, an appropriate procedure needs to be put in place.

Also, when receipt of e-mails may be a concern or becomes controversial due to strict interpretations of the right to a proper defense, technology provides alternatives in the form of certified e-mail services, which will confirm the delivery, receipt, content, chain of custody and chronological stamp of e-mails and contents. In such cases it may be advisable that from an early stage of the proceedings the tribunal and the parties agree on the use of such tools. Such tools include Certimail, eEvidence, E-Post, and eWitness. (N.B. These tools may not be available outside of particular countries and thus may have limited utility.) Further, at least to date, receipt of e-mails and other documents transmitted in the course of the arbitration is normally not an issue. The exception is where there is a non-participating party, but in these instances, delivery of hard copies by courier remains the most prudent option to secure proof of service.

4.8 Signature requirements

For documents that require a signature, such as the arbitral award or the Terms of Reference under the ICC Rules, it is important to consider formal legal requirements for validity before relying on an electronic form because requirements for a 'signed' document traditionally have been interpreted to mean a physical or 'wet ink' signature by the signatory on paper. Thus, although the printed name of the sender at the bottom of an e-mail or an electronic copy of a handwritten signature that is pasted into a document are ways for a person to 'sign' an electronic document in the everyday world, they may not qualify as signatures in certain specific legal contexts. This is because they are only digital reproductions and can be misused or manipulated by persons other than the signatory, and thus may give rise to legitimate doubts if there is a concern that the content of the electronic document may have been tampered with. There also are now widely available e-signature applications (such as DocuSign and an Adobe Acrobat tool) that manage the document signature process by providing signature capability, document routing, signer authentication, and security features to lock the signed document.

If the signature requirement⁴⁹ is established by a procedural order or the parties' agreement, the order or agreement could specify the electronic form that meets this requirement.

⁴⁹ This discussion does not cover formal requirements that may relate to the validity of the agreement to arbitrate or contracts or other documents concerning the substance of the dispute. These need to be scrutinised separately under the applicable laws.

If the signature requirement is established in the applicable institutional rules (e.g. Arts. 23 and 35 of the ICC Rules), the arbitral institution's public guidance on the construction of its rules will define what is formally required for the signature to be valid.

If the signature requirement is established in the *lex arbitri* or the law governing enforcement and recognition of arbitral awards (e.g. Art. 31, UNCITRAL Model Law; Arts. II and IV, New York Convention), the law governing electronic signatures at the place of arbitration or the place of enforcement will apply. In general, the issue will be whether an electronic signature qualifies as the full equivalent of the signatory's physical signature on a physically existing document.

If institutional rules or the *lex arbitri* require that the arbitrator's signature under the award must be certified (notarised) as the arbitrator's authentic signature, the process and form of notarisation normally will depend on the applicable law at the seat of the notary public. The same applies if the true certified copy is to be submitted in another country; the laws of that country should govern recognition of the certification. This will require a legalisation (normally carried out by the consular service of the destination country) or an Apostille for all member states of the *Convention of 5 October 1961 Abolishing the Requirement of Legalization for Foreign Public Documents* ('HCCH 1961 Apostille Convention').⁵⁰ Under the Convention, there is an electronic Apostille Programme ('e-APP').⁵¹

These issues raise questions for which internationally harmonised answers do not currently exist. For example, if local law would recognise an electronic signature to an arbitral award, may a notary public in that jurisdiction notarise an electronic signature? May the notary public use an electronic signature? If legalisation or an Apostille becomes necessary, is it possible to obtain an Apostille for an electronically signed notarisation of an electronically-signed arbitral award? The answers to these questions are likely to vary substantially from jurisdiction to jurisdiction.

The *ICC Note to Parties and Tribunals* provides that parties may agree to electronic notification of an arbitral award (where the award is signed in wet ink in counterparts and then scanned and compiled into one file) subject to any mandatory applicable law requirements.⁵²

If Terms of Reference or awards are to be transmitted and/or made electronically, it is best practice for this to be agreed by the parties and the tribunal in consideration of the issues discussed below and specifically noted in the Terms of Reference. (See sample procedural language in **Appendix B**.)

Although a multi-jurisdictional analysis of this issue is beyond the scope of this Report, the questionnaire to National Committees⁵³ included the question as to whether any mandatory law or rules in their jurisdiction may preclude the recognition and enforcement of Terms of Reference, an arbitral award, or other arbitral decision in an international arbitration if: (i) signed manually in counterparts and then scanned and assembled into one electronic file; or (ii) signed by other electronic means. National Committees were also invited to identify any relevant court decision. The 36 responses received revealed a wide range of responses, with many reporters noting that there was a lack of relevant jurisprudence on point.

⁵⁰ See <https://www.hcch.net/en/instruments/conventions/specialised-sections/apostille>; <https://www.hcch.net/en/states/hcch-members>.

⁵¹ See for status: <https://assets.hcch.net/docs/b697a1f1-13be-47a0-ab7e-96fcb750ed29.pdf>.

⁵² *ICC Note to Parties and Tribunals*, paras. 198-199.

⁵³ *Supra* note 30.

With regard to the practice of manually signing in counterparts, scanning the counterparts, and assembling into one electronic file, country reporters:

- > were unaware of any mandatory law or rules precluding the practice in Brazil, Canada, China, Colombia,⁵⁴ Costa Rica, Croatia, Finland, Germany, Ghana, Greece, India, Indonesia, Luxembourg,⁵⁵ Malaysia, Mexico, Nigeria, Spain, Switzerland, Tanzania, Thailand, Turkey, United Kingdom, United States, or Venezuela although some of these reporters qualified their answers by stating that the manually signed documents either should or must be available for inspection (e.g. China, Indonesia) or that authenticity of the electronic file must not be in dispute (Croatia);
- > sometimes distinguished between Terms of Reference and awards, opining that:
 - (i) the practice would be acceptable for Terms of Reference in Belgium (in case of business parties but not for private individuals or government entities), the Netherlands, and Poland, but that it is unclear whether the practice would be permitted for awards;
 - (ii) in the Czech Republic, the practice was only to be used for procedural orders and Terms of Reference with agreement of the parties, and would not be permitted for awards;
 - (iii) for awards, this practice could pose a risk that recognition and enforcement would be denied (Romania, Vietnam).
- > expressed uncertainty about whether the practice would be permitted (in Austria, Lithuania, Macedonia);
- > declared that the practice would not be permitted (Albania).

With regard to the use of electronic signatures, country reporters:

- > were unaware of any mandatory law or rules precluding electronic signatures in Brazil, Canada,⁵⁶ China,⁵⁷ Finland, Ghana, Mexico, Switzerland, Turkey, United Kingdom, United States, Venezuela;
- > suggested that electronic signatures complying with relevant local legislation (where applicable, qualified electronic signatures within the meaning of the EU 'Electronic identification and trust services regulation' ('eIDAS'))⁵⁸ likely would not pose recognition and enforcement issues in Austria, Belgium, Colombia, Costa Rica, Croatia, the Czech Republic (subject to issuance of a paper copy for purposes of archiving), Hong Kong, India, Indonesia, Luxembourg, Malaysia, the Netherlands, Nigeria, Romania, Spain, Tanzania, or Thailand; and
- > opined it was unclear whether such signatures would be accepted for recognition and enforcement of an arbitral award made in Albania, Germany, Greece, Italy, Lithuania, Poland, Vietnam or opined that such signatures would not be accepted (in Macedonia).

54 The reporter for Colombia noted that this is not the usual practice and there are no court decisions confirming the practice.

55 The reporter for Luxembourg noted that this is common practice in international arbitrations in Luxembourg and that the practice has not been challenged before Luxembourg courts.

56 It was noted, however, that in Quebec, Section 39 of the act to establish a legal framework for information technology provides that '[a] person's signature affixed to a technology-based document may be set up against that person if the integrity of the document is ensured and the link between the signature and the document was established at the time of signing and has since been maintained.'

57 The reporter for China nonetheless recommends advance written consent of the parties be recorded before implementing this practice.

58 Regulation (EU) N° 910/2014 and Directive 1999/93/EU

Given varying law and practice concerning these matters, parties and tribunals should consider potential mandatory law before relying on scans of manual signatures for Terms of Reference or awards (or, if arbitral rules allow, qualified electronic signatures). To that end, *the first step* in ascertaining formal signature requirements is the *lex arbitri*, i.e. the portion of the applicable arbitration law concerning signatures. If the law at the seat of arbitration does not establish the full legal equivalence of electronic signatures, it is most likely that a ‘simple’ electronic signature (e.g. a printed name, an electronic copy of a physical signature, etc.) will not satisfy the requirement for being a legal equivalent of a physical signature. If the law provides for equivalence, the type of electronic signature needs to be identified. It would not be sufficient to rely on simple assertions by professional providers of digital signature solutions, as may be seen – for example – from eIDAS in the EU and the European Economic Area.

In this sense, Article 25 eIDAS establishes that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature. But Article 3(12) provides that ‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures. In essence, this means that in the EU not any electronic signature will suffice to replace a physical signature in an award. Rather, only an electronic signature that relies on certain cryptographic means, comprising, *inter alia*, a certificate issued by a qualified trust service provider (see Art. 29 ff., eIDAS). Thus, unless it comprises a digital qualified electronic signature, inserting an electronic copy of a physical signature or inserting the name of the signor by other electronic means will not legally suffice in the EU. In other countries, including the US, legal requirements for valid electronic signatures may be more relaxed and thus (for example) an electronic copy of a physical signature may be valid. In countries where the *lex arbitri* has incorporated or is inspired by the UNCITRAL Model Law on Electronic Commerce,⁵⁹ electronic signatures are analysed using a functional approach, instead of a formal one. Under its Article 7, rather than a formal requirement for signature, any form or method that is reliable and gives certainty as to the originator of the message and its approval of the message’s content is acceptable. Arbitral awards or Terms of Reference are not commercial transactions; thus, even where a national law based on the UNCITRAL Model Law on Electronic Commerce has been enacted, it probably is inapplicable.⁶⁰ In any event, the mutual transnational recognition of electronic signatures is more than uncertain.

In a second step, the law concerning the equivalence of electronic signatures at the likely *place of enforcement* should be analysed. This is because the formal requirements under the local law governing enforcement or under the New York Convention will not be determined by reference to the *lex arbitri*, but under local law. Given that the mutual recognition of (qualified) electronic signatures in one legal system by other legal systems is unclear (to the extent that it exists at all), coupled with uncertainties as to the technical abilities of national courts and enforcement authorities, parties may find it prudent not to rely on electronically signed awards.⁶¹

At most, one may conclude that electronic signatures of awards, certifications of their authenticity and authenticity of true copies will require an advanced and qualified electronic signature as defined in the eIDAS or the equivalent thereof under other laws. Any other form of electronic signature may give rise to legal issues internationally. As of the date of publication of this Report, serious uncertainties concerning the recognition of any kind of electronic signature under arbitral awards persist.⁶² One cautious approach would be to produce and retain at least one hand-signed physical original of an award, of which certified

59 UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.

60 International commerce relies to a large extent on communications that are not hand-signed without any substantial degree of problems. This is because most commercial transactions are not subject to the same signature requirements as quasi-judicial acts such as awards. Where difficulties arise technologies such as block-chain increasingly are being used.

61 See ICC Note to Parties and Tribunals at paras. 196-200.

62 The reason is that the New York Convention does not define or provide guidance on what constitutes an ‘original’ electronic award or what would be an acceptable electronic ‘copy’ of such an award.

true copies can be made through hand-signed notarisations. This does not mean that electronic copies of an award or originals signed with qualified electronic signatures in accordance with the laws of the relevant country or countries could not *also* be communicated and used for other purposes.

5 Other Uses of Technology to Consider

5.1 E-briefs or e-bundles

Briefs with embedded electronic links ('hyperlinks') to cited exhibits, testimony and legal authorities are often referred to as 'e-briefs' or 'e-bundles.' E-briefs can make it more efficient for the tribunal to learn about and evaluate the case by making its review of submissions more interactive and holistic. They may also expedite the retrieval of documents at the hearing. With more paperless arbitrations and virtual hearings, e-briefs as well as linked indices, exhibits links and the similar, have become increasingly common in international arbitrations.

At the same time, it has been questioned if e-briefs and similar electronically-linked documents are too time-consuming and expensive for the parties to prepare. Thus, the tribunal may wish to undertake a rough cost-benefit analysis before ordering the presentation of e-briefs or similar documents. The number of documents is important for the assessment. If the case involves only a few documents, it is normally neither time-consuming nor expensive to prepare e-briefs, even when handled manually. For cases with a significant number of documents, modern software and technologies (e.g. ExhibitManager or Adobe Acrobat Pro) now allow briefs and similar electronically-linked documents to be generated efficiently and quickly at a lower cost, without necessitating that the task be outsourced to an outside vendor. Further, some law firms that regularly conduct arbitration or litigation have invested in such software for use across all their matters. Hence, the cost-benefit analysis may also depend on the parties' available technologies.

5.2 Machine learning artificial intelligence

Although electronic document production and its attendant issues are the subject of a separate ICC Commission Report,⁶³ the emergence of new technologies that change the ways in which disputes can be handled warrants some consideration in this Report. One such example is the use of artificial intelligence ('AI') and, more specifically, its application to disputes in the form of predictive coding. Predictive coding is a form of supervised machine learning AI by which relevant documents or documents responsive to a document request or a tribunal order are identified by an algorithm. The algorithm is trained by human generated 'coding' or tagging of the documents as relevant/not relevant or responsive/not responsive. When the precision is deemed appropriate and the estimated risk of error acceptable, the algorithm is applied to the entire set of electronic documents.

Predictive coding is often used in conjunction with other technology-assisted review techniques such as search terms and date ranges. Depending on the circumstances (including the nature of the case and issues in dispute as well as the volume of electronic documents), the potential benefits of predictive coding include cost and time savings, enhanced accuracy and transparency (provided that the use of predictive coding and the relevant parameters are disclosed to the other parties and the tribunal).

Predictive coding may be used to assess the merits of a party's own case and to identify the documents it may want to rely upon. Further, predictive coding may be used to identify documents responsive to a document request or a tribunal order. There are currently no rules or guidance on whether a party intending to use predictive coding in the context of a search for responsive documents must disclose that fact to other parties or the tribunal. Nor is there any guidance on whether the use of predictive coding must be agreed by other parties or approved by the tribunal. Accordingly, parties and tribunals may want to address the use of predictive coding during the case management conference, possibly as

63 See the ICC Commission Report on 'Managing E-Document Production' (2012), which provides an in-depth discussion of issues such as agreeing formats, procedures and training tribunals and counsel.

part of, or along with, a protocol whereby parties will agree and/or possibly involve the tribunal in fixing search terms, date ranges and/or predictive coding parameters. Generally, tribunal intervention will be required only to the extent necessary to clarify a party's disclosure obligations, approve the parties' agreement regarding disclosure protocols or resolve disputes, and to manage time and cost elements of the arbitration. Such use of predictive coding is expected to increase and, in some jurisdictions, there is legal authority upholding its use based on data supporting that it may be at least as accurate as human review.

Machine learning AI is also increasingly used to provide automatically generated translations of documents in other languages. Many parties will be familiar with Google Translate (for example), a free cloud-based service that instantly translates words, phrases, and web pages between English and 100 other languages. Although this type of web-based service may be used quickly and informally to assist a party in preparing its case, users should beware that the terms of service for such free services may include a user license to the developer to use any content that is uploaded. In practice, this may mean that content is stored to allow the developer to improve its vocabulary base. This could give rise to both confidentiality/security concerns and possible breaches of data privacy obligations. Accordingly, parties should generally avoid using free translation services for confidential or sensitive information and consider more secure, regulatory-compliant enterprise-grade services such as *DeepL.com* instead.

Although AI-generated translations are significantly cheaper than human-generated translations, they are also potentially less accurate in their current state of development. Thus, to the extent that a party intends to rely on AI-generated translations for exhibits that are submitted to the tribunal, it may be appropriate to agree on such use with the other party and to establish a protocol for a supplemental human-generated translation should the need arise.

5.3 Specialised hardware or software

If any special hardware or software is needed for the case, the users will need to consider the following.

Hardware interoperability. Except in unusual situations that require specialised hardware, hardware inoperability is generally not an issue. Nevertheless, all intended users need a minimum level of processing power with adequate data storage capacity and internet connectivity with sufficient bandwidth for communication using standard interfaces.

Software compatibility. The operating system and specific applications (e.g. word-processing, spreadsheet programs, and other special-purpose software) as well as scanned image formats should also be compatible. If off-the-shelf standard file formats (e.g. PDF, TIFF, RTF) are used, each user may not need to have the same programs as software interoperability also has greatly improved and problems with interoperability are today less likely to occur with the types of software generally used in a law firm's practice. Specialised software for industry sectors may pose different challenges.

Whether the technology tool is properly licensed. The intellectual property (IP) rights of third parties are not subject to agreements between the parties or orders from the tribunal. Accordingly, parties and arbitrators should ensure that any software or other technology tools that they are using for the arbitration are duly licensed. If it is envisaged that software or another technology tool will be shared, the parties will need to discuss and agree on who should make the required licensing agreements and how the associated costs should be allocated. In most instances, parties may appropriately expect that tribunal members will have their own licenses to standard tools for functions such as word processing, presentations software, spreadsheets, and PDF readers.

Adequate technical ability and resources. If the parties expect the tribunal to use specific IT, then each tribunal member must have sufficient technical ability and resources to transmit, receive, access, and use the data presented to them or training must be arranged (see Section 3.7). Equally, subject to the fairness and cost considerations discussed above (e.g. Section 3.3), the parties or their respective technical teams should collaborate in a way to advance and not impede the implementation of technology solutions.

6 Issues Relevant to Evidentiary Hearings

6.1 General considerations

6.1.1 Advance planning

Whenever a party intends to use IT during oral hearings, it should allow enough time to prepare and test the IT so that any technical problems can be identified and corrected before the hearing begins. The tribunal and the other party or parties should be informed of the planned use of IT before the hearing.

If only one party intends to use electronic means to present exhibits at the hearing, there normally should be no concerns. Nonetheless, if another party objects, the tribunal will need to provide directions.

6.1.2 Displaying electronic exhibits

In case of *physical* hearings, electronic documents may be displayed from one computer running the retrieval software, and either displayed to each participant via a local network of individual screens or projected onto a large screen for collective viewing. In *virtual* hearings, electronic documents may be displayed using a screensharing function.

As with printed exhibits, to increase efficiency and save time and costs, the tribunal may order the parties to eliminate duplicative exhibits and use only one version of identical exhibits at the hearing.

Some participants may want to pull up their own electronic copies of exhibits to review and annotate them even if they are shown on a screen. To facilitate this, it may be helpful to compile PDFs of individual exhibits into one or more volumes with bookmarks for the individual exhibits. It may also be useful to sequentially number all pages to facilitate pinpoint references. Others may find that linking the PDFs of the exhibits to an exhibit list is an equally or more efficient way to move back and forth among exhibits, particularly if they intend to use a computer rather than a tablet to review the documents. It is thus advisable to discuss individual preferences when determining how materials will be organised.

Other issues to be considered include:

- (a) Will the tribunal and the parties use electronic versions of the exhibits and other documents instead of, or in addition to, hard copies?
- (b) Will a specific software program be used to retrieve and project images of or otherwise show the exhibits at the hearing? If so, does the program have any special requirements? (For example, if audio or video recordings will be played, will it also be necessary to have portable speakers so that those in attendance can hear?)
- (c) May one side display electronic versions of exhibits if the other side does not wish to use electronic versions at all? While the tribunal has broad authority to conduct the proceedings as it considers appropriate, it is required to ensure that each party has a reasonable opportunity to present its case. Requirement to mandate that all parties use the same technology or present exhibits in the same way are not considered necessary.
- (d) Will the exhibits be available on a local or portable drive rather than through a cloud service, to avoid potential internet connectivity issues?

6.1.3 Visual presentation software

Unless the parties wish to make a joint presentation on certain issues, each of them should be responsible for any arrangements required to show videos, PowerPoint slides, illustrative charts, computer graphics, animations and other material. Typically, the tribunal will provide directions regarding the extent to which exhibits used solely for demonstrative or illustrative purposes must be disclosed in advance of the hearing.

6.1.4 Real time transcripts

A professional service provider can usually provide real-time transcripts that are viewable during the hearing on a device provided by the stenographic service or on any other device that is connected to the internet. Like all direct verbatim transcripts, real-time transcripts are expensive. It is also possible to rely on digital recordings that are transcribed later at less expense, but they are not as convenient and may not be as accurate as live transcription as it is not always evident on a recording who the speaker is and counsel lacks the ability to interrupt with immediate corrections. As automated voice recognition improves, the next decade may see the advent of inexpensive, automated verbatim transcription solutions. Indeed, live transcription of this nature is already available at no extra cost when using Zoom, provided that the feature is enabled by the host. Although such technology is convenient, it may not be sufficiently advanced to be relied upon for an accurate record. It also raises the same concerns about confidentiality, security, and data protection of the content being transcribed raised above in connection with the use of AI-generated translations. Further, search capabilities associated with the technology may be limited or lacking altogether.

6.2 Virtual hearings

6.2.1 Factors to be considered before proceeding with a virtual hearing

During the pandemic, lockdowns and the imposition of various health restrictions by jurisdictions around the world rendered virtual hearings quasi-ubiquitous. After a very steep learning curve, the arbitration community has adapted and has added this new tool to the arbitration toolbox. Although virtual hearings may not always be the best option, they may offer significant savings of time and travel which recommends them, in particular, for smaller cases, urgent matters, procedural hearings and less evidence-heavy hearings. As discussed below, the Survey data suggests that parties may also be open to considering the advantages of virtual hearings in more substantial matters. In many instances, virtual hearings will also be more cost-effective and may facilitate greater participation by business representatives in the proceedings by making it possible for them to leave and join hearings as their schedules permit.

The Survey on the use of technology in international arbitration contained extensive questions about the effectiveness of virtual hearings compared to physical hearings, willingness to conduct fully virtual or hybrid hearings, factors favouring whether a hearing should be convened virtually (in whole or in part), as well as preferences about videoconferencing platforms and important features. Among the detailed results on these issues set forth in **Appendix A**, three are highlighted below:

- (a) Most respondents believed there should be no presumption in favour of physical, hybrid, or virtual hearings; rather, the tribunal should decide what is appropriate based on the individual circumstances of the case.
- (b) When asked about what considerations, if any, are significant barriers to convening fully virtual hearings or hybrid hearings post-pandemic, the circumstances most commonly identified by respondents included: strong preference for human interaction, concern about the integrity of witness testimony, time zone issues, poor technological infrastructure and/or equipment, inadequate ability to assess eye contact and body language, fatigue, information security and/or data protection concerns, and unfamiliarity with technology.
- (c) Respondents also expressed concern about whether a virtual hearing is as effective as a physical hearing, with the most significant concerns being the cross-examination and witness conferencing of fact and expert witnesses, ensuring the integrity of witness testimony, interaction between counsel team members, and potential opportunities for settlement.

Tribunals should thus give due weight to these factors when deciding whether to convene a virtual, physical, or hybrid hearing.

Of course, virtual hearings are only useful if they provide the same or equivalent due process protections as a regular hearing. Protecting the integrity of witness testimony is one aspect of this. As discussed below, tribunals should implement measures to avoid witness tampering (Section 6.2.3) and should not hesitate to police compliance throughout the hearing. Other issues that may raise due process concerns include the total hearing time (which may differ from a physical hearing due to technological fatigue, odd hearing times and the need for additional breaks) and, crucially, the quality of the audio and video transmission throughout the hearing.

Tribunals should consider how such concerns could be mitigated. For example, the tribunal may need to adjust the hearing schedule not only to accommodate varying time zones, but also to consider fatigue. If one or more of the parties does not have satisfactory access to technology or infrastructure (such as reliable internet connectivity), organising hearings virtually may raise due process concerns and be inappropriate, as it could threaten the validity of the award, its recognition and enforcement. However, such concerns may not be dispositive if a third-party service provider can adequately address the technological issues. The discussion on hybrid hearings below (Section 6.3) suggests that, going forward, greater institutional investment in regional hearing facilities and/or more inter-institutional cooperation to maximise access to high-quality hearing facilities could help to level the technological playing field in regions where there is poor infrastructure and optimise virtual hearing experiences.

As regards audio and video quality, tribunals should adopt measures in their procedural directions to account for technical difficulties during the hearing. These might include: backup technical solutions (e.g. a telephone conference if the technical difficulty is short-lived); using real-time transcripts that can be consulted quickly and easily if someone briefly drops off the hearing or has intermittent connectivity issues; suspending the hearing; or even aborting the hearing altogether if the quality of the audio and video transmission is suboptimal and cannot guarantee that the parties can be properly heard (e.g. when the sound suffers continuous interruptions that distract from the witness' testimony or counsel's argument). Additional concerns may arise in the context of hybrid hearings, as discussed separately below (Section 6.3).

In ICC cases, when tribunals have proceeded with virtual hearings by agreement of the parties, they have sometimes incorporated language in their procedural orders confirming the parties' waiver of the right to object to the enforceability of the award on the basis of the hearing taking place virtually.

When an evidentiary hearing is convened by videoconferencing notwithstanding the objection of a party or without the agreement of the parties,⁶⁴ concern sometimes arises about potential challenges to the recognition and enforcement of an ensuing award. To allay enforceability concerns with respect to virtual hearings, several of the major arbitral institutions, including ICC, have revised their rules to explicitly confirm the tribunal's authority to conduct hearings by telephone, videoconference, and other remote means of communication, or to provide more generally for the use of technology in the tribunal's discretion.⁶⁵ By agreeing to arbitrate under the rules of ICC and other institutions that have adopted similar provisions, parties agree that the tribunal may decide the manner in which any evidentiary hearing will be conducted.

64 See ICC Guidance Note on Possible Measures Aimed at Mitigating the Effects of the COVID-19 Pandemic ('ICC Guidance Note on COVID-19'), which has now been incorporated in the ICC Note to Parties and Tribunals. Para. 100 of the ICC Note to Parties and Tribunals provides: 'If an arbitral tribunal determines to proceed with a virtual hearing without party agreement, or over party objection, it should carefully consider the relevant circumstances, including those mentioned in paragraph 99, assess whether the award will be enforceable at law, as provided by Article 42, and provide reasons for that determination.'; See also, **Guidance Note on Remote Dispute Resolution Proceedings** (CI Arb, 2020) at para. 7.4 (noting some courts may reject enforcement of arbitral awards if they were produced solely via digital means).

65 See, e.g. ICC Rules, Art. 26(1): 'The arbitral tribunal may decide, after consulting the parties, and on the basis of the relevant facts and circumstances of the case, that any hearing will be conducted by physical attendance or remotely by videoconference, telephone or other appropriate means of communication'.

Nonetheless, to assess whether there is any meaningful risk of non-recognition or non-enforcement in the event of a party's objection to a virtual hearing, it will be necessary to consider: (i) whether the language in the parties' arbitration agreement forecloses the possibility of a virtual hearing absent the parties' further agreement; and (ii) any applicable mandatory law at the place of arbitration and any likely places of enforcement.⁶⁶

As concerns the latter, judicial decisions considering remote arbitration proceedings in the context of recognition and enforcement proceedings have been limited to date, but judgments in Austria⁶⁷ and Switzerland⁶⁸ have upheld tribunal decisions to convene virtual hearings despite the objection of a party.⁶⁹

Parties and tribunals may also refer to a project undertaken by ICCA compiling national reports from New York Convention jurisdictions exploring whether a right to a physical hearing either expressly exists or may be inferred from the relevant national arbitration law.⁷⁰ Although none of the surveyed jurisdictions contained any express provision granting a right to a physical hearing, the project identified jurisdictions where (i) such a right may be inferred (e.g. in Ecuador, Germany, Tunisia, Venezuela, and Vietnam) or the law is unsettled (e.g. Benin, Norway, Tunisia); (ii) holding a remote hearing absent party agreement could potentially lead to set aside of the award (in some jurisdictions, subject to showing that the breach of the parties' agreement had a material impact on the outcome of the case or caused substantial injustice); and (iii) considerations of fairness and efficiency (especially in the context of the COVID-19 pandemic) could justify overriding a parties' agreement and avoid the setting aside of an award.

The project is also noteworthy for drawing attention to jurisdictions where virtual hearings may be impractical or impossible. The report on Kenya, for example, pointed out that the country faces challenges with uneven internet accessibility while the report on Zimbabwe described challenges with power outages, poor internet connection, the high cost of internet use, and the absence of other technological, legal, and security requirements. Reports on Sri Lanka, Tunisia, and Zimbabwe additionally noted that during the pandemic, few or no court hearings were conducted remotely. Thus, even though mandatory law in such jurisdictions may not preclude convening a hearing by videoconference, these reports serve as a reminder to parties and tribunals that inadequate infrastructure including unreliable internet access may or may not be easily remedied (e.g. by hiring a third-party service provider) and could lead to recognition and enforcement issues if a party is unable to present its case.⁷¹

66 See generally M.S. Abdel Wahab, 'Arbitration: Pandemic pathway', *The Resolver*, Vol. 2021, issue 1, proposing a pathway of considerations regarding tribunal authority to order a virtual hearing when parties do not agree.

67 See M. Scherer, F. Schwarz, H. Ortner, J.O. Jensen, 'In a 'First' Worldwide, Austrian Supreme Court Confirms Arbitral Tribunal's Power to Hold Remote Hearings Over One Party's Objection and Rejects Due Process Concerns' (Kluwer Arbitration Blog, 24 Oct. 2020) (Supreme Court, 23 July 2020, original in German).

68 See D. Franchini, F. Spoorenberg, 'Arbitral tribunal's refusal to postpone hearing is not violation of right to be heard' (Lexology, 7 Oct. 2021) (Supreme Court, 4A_530/2020, 15 June 2021, original in French.)

69 See also *Eaton Partners LLC v. Azimuth Capital Management IV Ltd.*, 2019 WL 5294934, at *11-12 (US District Court, Southern District of New York, 24 Sept. 2019) (refusing to vacate an ICDR arbitration award where it was alleged the arbitrator was guilty of misconduct for allegedly refusing to postpone the hearing when a witness was unavailable, stating appearance by video 'would not have constituted a deprivation' of the 'right to a fundamentally fair hearing').

70 The research project 'Does a Right to a Physical Hearing Exist in International Arbitration?' comprises national reports from 78 New York Convention jurisdictions, available at <https://www.arbitration-icca.org/right-to-a-physical-hearing-international-arbitration>.

71 Issues with unreliable internet connectivity and inadequate bandwidth are not always limited to remote geographical locations. This was a notable issue in metropolitan areas like Melbourne and Sydney in Australia during the pandemic when usage at 11 a.m. grew by over 70% from 28 Feb. to 3 April 2020. See D. Tait et al., 'Gateways to Justice II: Guidelines for Use of Video in Justice Hearings' (Nov. 2020) at p. 58.

While the power of tribunals to order virtual hearings has been confirmed in ICC and other institutional rules, tribunals exercising their discretion may find useful to consider arguments parties opposing virtual hearing have raised in *recent ICC cases*, including:

- > the potential violation of their due process rights, including the right to present one's case;
- > technological limitations due to the participation from different locations and countries, (e.g. internet access and slow speed of the connection for witnesses who may live in remote areas) and participants of certain age being less technically savvy;
- > issues of confidentiality and time zone issues, which limited the possibility of finding appropriate slots;
- > additional costs for holding a virtual hearing, having an electronic bundle; and difficulties in displaying or following evidence virtually;
- > difficulties relating to witness preparation; and
- > 'screen fatigue' and the need to shorten the virtual hearing days.

Parties objecting to a virtual hearing have relied on a myriad of authorities, including (i) relevant provisions of the *ICC Rules* (Arts. 22, 25, 26), and the *ICC Guidance Note on COVID-19* (now incorporated in the *ICC Note to Parties and Tribunals*); (ii) the applicable *lex arbitri*; (iii) the arbitration agreement providing for the place of arbitration or any language as to where the hearings and meetings of the tribunal are to take place; (iv) the Terms of Reference, or rules or guidelines incorporated in the Terms of Reference including the *IBA Guidelines on the Taking of Evidence in International Arbitration* and *IBA Rules on Party Representation in International Arbitration*; (v) relevant national court decisions in support of their arguments, even if those decisions pertained to court proceedings as opposed to arbitration proceedings;⁷² and (vi) generally, to the *New York Convention* and arguments that an award of the tribunal following virtual hearings may be subject to enforcement or annulment proceedings.

In ruling on these issues (generally by procedural order), some tribunals have addressed their duty to decide the case fairly and impartially, and to ensure that each party has a reasonable opportunity to present their case and is treated equally. At the same time, tribunals have expressed their duty to conduct the proceedings in an expeditious and cost-effective manner and weighed the different factors/duties and possible prejudice to the parties. To support their decisions, tribunals have referred to Article 19 ('Rules Governing the Procedure'); Article 22 ('Conduct of the Arbitration'), Article 25 ('Establishing the Facts of the Case'), Article 31(1) ('Time Limit for the Final Award') of the *ICC Rules* as well as to the *ICC Guidance Note on COVID-19*.⁷³ In some instances, the tribunals compared the different language versions of the Rules (comparison between the English, French or German version of the Rules) and concluded that there is no duty to hold a physical hearing under Article 25.⁷⁴ Other factors tribunals have considered are:

- > whether any overriding mandatory provisions require the conduct of in-person (physical hearing) in the *lex arbitri*;
- > whether a separate or subsequent parties' agreement requires a physical hearing (by looking at the arbitration agreement and any other separate agreements between the parties);
- > the complexity of the dispute (complexity of the matter itself but also whether it is a multi-party dispute) and whether it would warrant a physical as opposed to a virtual hearing;
- > the possibility to present one's case without causing prejudice to any of the parties; and

72 For example, the Swiss Federal Tribunal, Decision 4A_180/2020 of 6 July 2020 (in **German**).

73 Supra note 64.

74 Most notably, Art. 25(2) provides '[t]he arbitral tribunal may decide to hear witnesses, experts appointed by the parties or any other person, in the presence of the parties, or in their absence provided they have been duly summoned' and Art. 25(6) provides '[t]he arbitral tribunal may decide the case solely on the documents submitted by the parties unless any of the parties requests a hearing'.

- > factors related directly to the pandemic, including the uncertainty of the constantly changing situation and evolution of the pandemic, ensuring the safety of the participants (i.e. minimising the risk of infection of participants), the need for social distancing, quarantine procedures for parties coming from different countries and the fact that travel restrictions keep evolving and may not change in the foreseeable future or there would still be some restrictions including for travel, limit of people in the same room/building, etc.

6.2.2 Organisation of virtual hearings

Organising a hearing by video conference presents other challenges than a physical hearing. Significant guidance has emerged with respect to best practices,⁷⁵ including from ICC, whose guidance is incorporated in its *Note to Parties and Tribunals* and its *Checklist for a Protocol on Virtual Hearings*.⁷⁶

In general, it is recommended that parties attempt to reach agreement on the virtual hearing procedure, subject to approval by the tribunal and any requirements of the administering institution. The arrangements should then be recorded in a virtual hearing procedural order, which is sometimes referred to in practice as a 'hearing protocol' or 'cyber-protocol.' To make the vast array of guidance readily available for quick reference, **Appendix C** contains the following organisational checklists: (I) Considerations for parties when choosing a third party service provider as host; (II) Pre-hearing checklist for parties and tribunals for coordinating hearing preparations with virtual hearing host; (III) Counsel's pre-hearing checklist for preparing individual witnesses; (IV) Arbitrator's checklist to prepare for virtual hearing; and (V) Counsel's checklist to prepare for virtual hearing. In addition, distilled recommendations for hearing procedures (such as advance technical testing) are included in a detailed template procedural order in **Appendix D**, and special concerns are highlighted below.

6.2.3 Special issues relating to witnesses

Both counsel and arbitrators need to consider specific issues if witnesses are to be heard in a virtual setting. As counsel, the witness should be well prepared for attending the virtual hearing. (See Checklist Appendix C, III. 'Counsel's pre-hearing checklist for preparing individual witnesses'.) This starts with ensuring that the witness has the technical ability to participate (e.g. access to suitable equipment and technology), and performing a check with the witness prior to the hearing to prevent any technical glitches during the hearing. When it comes to (cross-)examining a witness at the hearing, counsel should, among other technical issues, consider their screen settings and how this may impact their advocacy (e.g. whether screen settings should remain the same, whether to disable the own view and/or switch to speaker view on at least one of the screens).

Arbitrators face two different challenges when witnesses are heard in a virtual setting. The *first challenge* is protecting the integrity of the proceedings and preventing witness tampering. Thus, arbitrators should check that the witness is not accompanied by unauthorised persons in the room where he/she is testifying and that they do not have access to unauthorised materials (e.g. counsel notes, live chat with counsel through e-mail or web-based communication services). Two sets of cameras is one possible solution to ensure compliance. Tribunals can and may check at any time during the witness' testimony whether compliance with these requirements is continuous.

⁷⁵ A list of resources, including guidelines, checklists, protocols, model procedural orders, case materials, legislation reviews, survey reports, and webinars is also available at <https://delosdr.org/resources-on-virtual-hearings/>.

⁷⁶ The ICC Checklist for a Protocol on Virtual Hearings, and Suggested Clauses for Cyber-Protocols and Procedural Orders dealing with the Organisation of Virtual Hearings sets out in Annex I, a Checklist for a Protocol on Virtual Hearings, and in Annex II, Suggested Clauses for Cyber-Protocols and Procedural Orders Dealing with the Organisation of Virtual Hearings.

The *second challenge* is technical. As part of the hearing preparations, depending on the circumstances of the case, tribunals may wish to organise the pre-hearing test with counsel only, or with counsel, witnesses and experts. The first option is swifter and more flexible in terms of organisation. It also puts the burden on counsel for familiarising the witness with the technical requirements and the atmosphere of a hearing in a virtual setting. The second option may be advisable if the tribunal and/or the parties believe that a pre-hearing test with all the participants can be helpful with the interaction between the tribunal and the witnesses and experts.

Tribunals should also ensure that the procedural order they render prior to a virtual hearing is up to date. **Appendix D** contains a template procedural order to that regard which needs to be adapted to the specific case. During the hearing, as regards witnesses and their cross-examination, arbitrators should ensure that the witness' face is clearly visible when testifying and potentially have the witness use two cameras for testifying. If the witness testifies in a language other than the one used in the arbitration and language interpretation is necessary, there might be additional technical issues to consider (e.g. in case of simultaneous translation, availability of headsets with microphones and set-up of multiple language channels).

6.2.4 Recordings

Hearings in international arbitration matters are often transcribed or recorded for future reference. The *lex arbitri* may require a record of any arbitration hearing, in which case the format of the record should comply with mandatory formal requirements of the *lex arbitri*. In international arbitration, especially for hearings of some duration during which witnesses are examined, verbatim transcripts have evolved into a preferred format. In certain instances, these verbatim transcripts are displayed to the arbitrators and counsel in real time on a computer screen using dedicated programs ('real-time' or 'live' transcripts). All this comes at a cost that may be prohibitive in smaller or medium sized cases. Alternative methods of producing records of a hearing may therefore be sought. The available methods and some of their advantages and inconveniences are identified below.

a) Records by court reporters. Subject to a good quality, stable broadband connection to the virtual hearing room, court reporters may connect to any remote hearing as any other participant and provide their services remotely. Their work product can be shared online after the hearing or in real time. Although it is an additional expense, the latter is especially useful in a virtual hearing because it allows participants to keep apace and avoid interrupting the hearing because of brief, intermittent connectivity issues.

Reporters should connect not only via an audio stream but also via video so that they may identify the respective speakers. For this purpose, they can be provided with a photograph, the full name and the function of all persons who will be on record. Technical requirements and offers for improving the service should be discussed as well as the steps required to ensure full availability of the service on the hearing day.

b) Video recording with sound. Whilst video records of a hearing do not offer the same level of user friendliness and searchability (as, for example, live verbatim transcripts), in some cases they may provide a viable alternative that comes at a lesser cost. Common video conferencing platforms normally comprise a video recording functionality and the records made by the session host can be easily copied and distributed to parties and arbitrators. Post hearing briefs may, but need not, include printed citations of relevant sections, given that precise references are possible to the minute and second within the record. Post hearing briefs in e-brief format also may include clips from the relevant minutes of the hearing. Notwithstanding, as would also be the case for audio records, many parties prefer printed transcripts because this suits their working habits and facilitates searching the record for relevant matter. Subsequent transcripts may be produced with ease because the video record allows for an easy identification of the speakers.

It is good practice to constantly monitor that the video conferencing function works properly. This should be delegated to a technical person who must alert the tribunal if non-expected errors occur that impair recording or the quality of the digital records. Because the video record will at least be temporarily stored on the system of the video conferencing service provider, precautions should be taken in relation to the protection of personal data and confidentiality in the same way as with any other service provider (see Section 3.4). It is essential to pay attention to security and data privacy issues, including restricted access controls, the location of the host server, and auto-deletion after a set-time period.

Although it is technically possible also to store the video record during recording on the service provider's system or on the sole arbitrator's or chair's system, this requires some technical capabilities and knowledge which, if absent, can lead to deficiencies of the video record.

c) Sound recordings. Digital sound recordings are easily made, consume less storage space than video recordings. Relevant parts can also be referred to by indication of the minute and second of the hearing or embedded as sound clips in e-briefs that are submitted as post hearing briefs. However, working with audio records is less convenient, because it will not always be as simple to identify or retrieve each speaker in the record. A request to all participants to state their name each time they speak is likely not to be always followed.

d) Voice recognition. Both video recordings and sound-only recordings may be processed with voice recognition programs that automatically transcribe what was said. These programs have evolved dramatically in recent years, and today provide an impressive level of reliability without lengthy hours of training by the speaker. Problems with the quality of automated transcripts still may arise and require subsequent substantial human editing (e.g. due to automated speaker recognition and the challenges coming with the different voice characteristics of the participants).

e) Technical precautions. Regardless of the technical solutions chosen for recording remote hearings, and the often-perceivable differences in technical capabilities of the participants in an arbitration, the chosen solution should be tested ahead of time and, if required, technical shortcomings cured. Ideally, an alternative mode for establishing the record of a hearing should be available in the event unexpected problems materialise (e.g. in the case of a video record, a parallel audio record).

6.2.5 Hearings with large numbers of participants

Organising a hearing by video conference can present different challenges, depending on whether the hearing involves numerous participants or relatively few. The parties and tribunal should consider whether it is advisable, for a large hearing, to split hearing participants into 'active' and 'passive' participants to maximise the quality of the video and audio feed. In such a scenario, 'active' participants (e.g. tribunal, lead counsel) would receive audio and video links to the hearing, which will allow them to appear on the video platform screen, to speak and be seen by the other participants. In contrast, 'passive' participants (e.g. counsel who are not actively participating; paralegals) would only receive a live video and audio feed of the hearing, but would not appear on the screen, would not be visible to the other participants and would not be able to speak.

6.2.6 Technical testing

There are numerous issues to consider when preparing for a technical test prior to a virtual hearing, most of which depend on the specificities of a certain case. **Appendix C** contains checklists for counsel and arbitrators and **Appendix D** includes template wording in a procedural order. (See **Appendix D**, IV. 'Technical capabilities and pre-hearing testing'.) From a tribunal's perspective, the main question is whether to perform the test with everybody involved (i.e. party representatives, counsel, witnesses, experts, translators, etc.) or only the party representatives. If the latter, party representatives should be briefed by the tribunal on prior test(s) with their 'side'.

Also, if a third-party service operator is involved, the tribunal should consider whether that service provider should also be responsible for, or at least also participating in, test run(s). The purpose of the test is to allow (all) participants to assess the quality of their audio and video transmissions and to adjust as necessary. Also, the participants should be able to experience the key features of the service provider/platform used at the virtual hearing itself to be able to mute/unmute, use break-out rooms, display options, screen sharing and other possible features to hopefully have the virtual hearing itself proceed smoothly.

6.2.7 Intra-tribunal and intra-party communications

Anytime individual groups of participants (such as members of the tribunal or members of a counsel team) are not joining the hearing from the same location, it is necessary to consider a means of secure and private communication to mimic the passing of notes, whispers, and physical nudges that ordinarily occur at physical hearings. Various options may be considered, but it will generally be preferable, where available, to choose a dedicated and exclusive communications channel with appropriate security restrictions such as passwords and encryption. For example, some online case management platforms incorporate private communication windows that can be left open during the hearing alongside an exhibits database and real-time transcript. Counsel teams may also be able to communicate with each other using ordinary business channels (such as a Microsoft Teams group, for example). These will have the advantage of being familiar and already vetted from a security perspective.

Where such options are not available, a popular choice for 'internal' hearing communications are instant messaging services such as Signal, WhatsApp, or even cellular text messaging. It is important, however, to exercise caution when using such applications, to ensure that the level of security provided is appropriate for the circumstances of the case,⁷⁷ and settings are adjusted accordingly (e.g. to prevent the application from accessing all of a user's contacts).⁷⁸ From a practical perspective, it will be necessary to consider whether the proposed application is equally available to all who will use it (e.g. as applicable to Android and iOS users), any associated costs (e.g. to receive text messages), and the device(s) on which the participants would prefer to be able to send and receive messages (e.g. Signal has desktop and mobile versions).

Although a common and convenient feature of videoconferencing platforms is a chat function that allows individual recipients to be selected via a drop-down menu, there is significant risk that this means of communication during a hearing will result in the inadvertent sending of confidential and/or privileged communications to unintended recipients. It also may not be possible to use the chat function to communicate with a select group of recipients only (typical choices include chat with everyone, the host, or a particular individual). Accordingly, reliance on chat is not recommended and it is best to disable its use altogether. While e-mail may be another convenient option, messages on unrelated matters are likely to be distracting and is also therefore best avoided.

6.3 Hybrid hearings

Depending on the circumstances, tribunals and parties may decide to organise hearings with some participants being present in person, and others joining via videoconference or teleconference (so-called 'hybrid hearings'). Hybrid hearings have characteristics in common with both physical hearings and virtual hearings, and may be organised in a variety of ways (e.g. counsel for both parties being present at the hearing venue, and the tribunal members joining remotely; the tribunal and some counsel on either side present at the hearing venue, and other counsel joining remotely; the tribunal and counsel present at the hearing venue, and witnesses and experts joining remotely etc.). It is difficult to generalise and set out all practical manifestations of hybrid hearings, as there are infinite options that parties

77 Further guidance is available in the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration (2020 Edition).

78 See e.g. Z. Doffman, 'Yes, You Can Still Use WhatsApp—But Change These 3 Critical Settings First' (Forbes, 12 Jan. 2021).

and tribunals can choose from in order to best suit their case. (See the checklists for virtual hearings in **Appendix C**, select options as applicable to the hearing and make adaptations as necessary to the template procedural order in **Appendix D**.)

Experience in the pandemic and the Survey data suggest that hybrid hearings may become a prevalent approach over time for manifold reasons: a witness who has limited things to say may be far away; maybe some people can travel to and from the hearing venue and others cannot for health or other reasons; or maybe the tribunal and/or the parties are aiming at keeping travel and accommodation costs to a minimum, which might lead to only the main participants being present in person.

When deciding to organise hybrid hearings, tribunals should be mindful that hybrid hearings may raise additional challenges in terms of the fairness and equal treatment of the parties (e.g. if the tribunal and counsel for only one party is present at the same physical hearing venue, but counsel for the other party is only able to join remotely). Thus, depending on the circumstances of each case, tribunals may need to take steps to ensure that both parties are treated equally. In the example above, where the party attending remotely objects, the tribunal might consider whether it is appropriate to have both parties appear remotely, and only the tribunal present at the hearing venue. Questions of fairness and equality of the parties may also arise in instances where both parties can be physically present at the hearing venue, but only some (but not all) of the tribunal members are able to do so, with the other arbitrator(s) having to join remotely. In such instances, in order to safeguard the award from potential challenges, it may be worth discussing whether it is advisable that all tribunal members participate in the hearing remotely.

Even if there is no objection related to an 'imbalance' and the tribunal decides it is appropriate to proceed, it may be prudent to record the parties' acknowledgement/agreement regarding the physical locations from which the participants will join the hearing in the pre-hearing procedural order, and draw attention to the discrepancies. (Sample procedural language is included in the template procedural order in **Appendix D**, III. 'Hearing notice and authorised attendees'.)

As with virtual hearings, potential technological disparities among the participants may pose another challenge. To cope with this reality, it seems likely that greater institutional investment in regional hearing facilities and/or more inter-institutional cooperation will be required if we are to ensure that parties from around the world have equal opportunity to take advantage of the benefits that remote hearing participation may offer in an international arbitration and that those from regions with less reliable infrastructure are not at a perennial disadvantage. Such development and cooperation would also be welcome to ensure that when participants attend hearings by remote videoconference they are supported with optimum technology and support services.

Another issue to be considered is the configuration of the hearing venue. Ideally, remote participants will be afforded a wide view of the persons present in the hearing room (in addition to close-ups as appropriate for tasks such as witness testimony) so that all participants in the hearing have the opportunity to see and hear people when speaking and have a sense of the overall environment. To the extent possible, consideration may also be given to the ideal placement of screens displaying remote participants in the hearing venue, particularly during witness testimony, in a way that may facilitate the impression of eye contact between counsel and the witness. Although such 'design' issues are unlikely to create genuine fairness or due process concerns, research concerning virtual court proceedings suggests that thoughtful attention to the way in which technology is set up for hybrid hearings may improve judicial proceedings and better ensure effective participation by all participants.⁷⁹

79 See e.g. D. Tait, et al., *supra* note 71.

Appendix A – Key Findings from the Survey on Use of IT in International Arbitration

1) About the Survey

The ICC Commission on Arbitration and ADR conducted a Survey⁸⁰ to better understand the current state of technology in modern international arbitration practice. The survey was disseminated to all members of the Commission and its Task Forces, and more broadly throughout the international arbitration community via the ICC Global Network and social media.⁸¹

In drawing conclusions, the Working Group is mindful that the reliability of the survey data is limited by the questionnaire design, the demographic characteristics of the respondents, as well as survey administration methodology, which did not follow formal social research methods.

Between February to July 2021, 520 responses were received, mostly from those whose primary role in international arbitration proceedings is as counsel (36%) or arbitrator (35%), or whose time is split relatively equally between those two roles (19%). Input from in-house counsel and corporate representatives was limited (5%). Most respondents have at least ten years of experience in international arbitration, and 31% have more than 20 years. Just under half of all respondents (45%) practice primarily in Europe, and the remaining respondents are mostly divided in roughly equal shares between those who practice primarily in North America (17%), Latin America (15%), or Asia-Pacific (12%). Few respondents practice primarily in the Middle East (5%), Africa (5%) or the Caribbean (2%). One important caveat to consider is that there were limited responses from geographic regions where ready access to technology tools and resources may be more constrained. In addition, greater participation by corporate users potentially could have revealed differences in attitudes and preferences from practitioners.

The key findings of the Survey are summarised below. Parties and tribunals will find results on specific issues helpful, for example when choosing a videoconferencing platform (e.g. which platforms are preferred by others, and what features tend to be deemed essential).

2) General views on the use of IT over the past three years

Asked about their **general perceptions about the use of IT**:

- > 93% of respondents agreed that technology has improved the efficiency and cost-effectiveness of the process.
- > 83% agreed that technology has been underutilised in the arbitral process.
- > 64% disagreed that cost or inadequate infrastructure and resources posed barriers to incorporating technology effectively in the arbitration cases that they typically handle.
- > 74% disagreed that technology has created or exacerbated concerns about fairness and/or equal treatment of the parties; yet respondents were nearly evenly split as to whether technology has levelled the playing field between the parties, with 51% agreeing that it has and 49% disagreeing.

80 See the Introduction to this Report (Section 1.1) for a description of the survey objectives, respondents, and limitations.

81 Through its network of world chambers and National Committees, ICC brings together companies of all sizes and sectors in more than 100 countries. More information at <https://iccwbo.org/about-us/global-network/>.

Asked about the **usefulness of IT-related guidance** in their international arbitration practice, many users were not familiar with resources that others reported were very useful or somewhat useful, including:

- > *IBA Technology Resources for Arbitration Practitioners* (48% not familiar, compared to 47% very or somewhat useful).
- > *ICCA-New York City Bar-CPR Protocol on Cybersecurity in International Arbitration* (48% not familiar, compared to 48% very or somewhat useful).

3) Pre-pandemic experience with IT solutions

Asked about their **pre-pandemic use of various IT solutions**:

- > 96% always, often, or sometimes used e-mail for the exchange of communications and submissions, but 83% also always, often, or sometimes used hard copies for the exchange of communications and submissions.
- > 85% always, often, or sometimes used audio teleconferencing for a case management or other procedural conference.
- > Of those who experienced a reported information security incident, 82% did not believe the incident threatened the integrity of the process, and 80% believed the incident was inconsequential.
- > 79% always, often, or sometimes used USB drives or other portable storage media.
- > 73% always, often, or sometimes used cloud file sharing sites for the exchange of document disclosure, exhibits, or voluminous submissions.
- > 75% always, often, or sometimes used real-time transcription during the evidentiary hearing.
- > Only 2% of respondents always used online case management platforms or virtual data rooms for the exchange of all or most communications and submissions, but 68% often or sometimes did so.
- > 69% always, often, or sometimes experienced trial graphics or multi-media presentations during the evidentiary hearing.
- > 57% always, often, or sometimes used hyperlinked submissions/e-briefs or e-bundles.

4) Expectations regarding post-pandemic use of IT solutions

95% of respondents believe that during the initial case management conference, tribunals should routinely discuss with the parties how IT may be used to increase the efficiency of, or otherwise enhance, the arbitral proceedings.

Asked about **which IT solutions** they were likely to use after the pandemic, considering the typical size and nature of disputes handled in their international arbitration practice, *more than half of respondents* reported:

The IT solutions they would use 'more often' included:

- > Videoconferencing for a case management or other procedural conference (83%), a limited number of participants during the evidentiary hearing (78%), all or most participants during the evidentiary hearing (75%).
- > Online case management platform/virtual data room for exchange of all or most communications and submissions (71%).

- > Cloud file sharing site for the exchange of document disclosure, exhibits, or voluminous submissions (68%).
- > Agreement among counsel and the tribunal to adopt specific measures, such as encryption, to safeguard the privacy and security of arbitration-related information in electronic form (65%).
- > Paperless arbitration, except for the hearing (63%).
- > Hyperlinked submissions/e-briefs or e-bundles (58%).
- > Paperless arbitration, including the hearing (57%).

The IT solutions they would use the 'same as before the pandemic' included:

- > E-mail for the exchange of communications and submissions (59%).
- > Realtime transcription during the evidentiary hearing (68%).
- > Trial graphics/multi-media presentations during the evidentiary hearing (63%).
- > Technology-assisted review/predictive coding for document review (53%).

The IT solutions they would use 'less often' included:

- > Hard copies for the exchange of communications and submissions (74%).

Asked about whether **technological competence** will be an important consideration going forward when participating in the selection of arbitrators, 51% responded 'yes' and 40% responded 'it depends'.

5) Experience with virtual meetings

Asked about their experience with case management or other procedural conferences or oral arguments via videoconference ('virtual meetings'):

- > 89% participated in virtual meetings during the pandemic.
- > 90% agreed that virtual meetings were conducted effectively as opposed to teleconference or other means typically used pre-pandemic.
- > 88% agreed that it should be the norm post-pandemic to conduct case management and other procedural conferences as virtual meetings.

6) Experience with virtual hearings during the pandemic

78% of respondents reported experience with evidentiary hearings during the pandemic where all or most participants appeared via videoconference ('virtual hearings').

Asked about recommended, preferred, and most used **videoconferencing platforms**, respondents reported that:

- > They were very or somewhat likely to recommend the platforms as follows: Zoom (72%), Microsoft Teams (51%), Cisco WebEx (38%), Google Meet (16%), Skype (15%), Bluejeans (11%), LogMeIn GotoMeeting (7%), Lifesize (5%), BigBlueButton (4%), VidyoConnect (3%).
- > They were not at all likely to recommend the platforms as follows: BigBlueButton (25%), Bluejeans (25%), Skype (24%), Lifesize (23%), VidyoConnect (23%), LogMeIn GotoMeeting (21%), Google Meet (20%), Cisco WebEx (16%), Microsoft Teams (11%), Zoom (2%).

- > Although 14% reported insufficient experience with different platforms to have a preference among them and 9% reported experience with multiple platforms but no preference, 59% identified Zoom as their preferred platform, followed most closely by 9% who identified Microsoft Teams and 3% who identified Cisco WebEx.
- > The platforms used most frequently in the pandemic (in order) have been Zoom, Microsoft Teams, and Cisco WebEx.

Asked to rate 60 **general characteristics and specific features** when choosing a videoconferencing platform for an effective virtual hearing:

- > Easy to access (93%) was the characteristic or feature most designated as 'essential/must have,' followed next by user friendliness (72%).
- > Other characteristics or features identified by at least 50% or more of respondents as 'essential/must have' were: robust meeting controls for host, including in particular access controlled by host, host control over who can record, and ability to mute participants; robust security features, including in particular password protection, notice to all participants when recording is on, and end-to-end encryption; break-out rooms; name display; screensharing; virtual waiting room; recording features; and alerts when participants join or depart meeting.

79% were either highly likely (51%) or somewhat likely (28%) to recommend to others that a neutral third-party service provider be engaged to host and facilitate a virtual hearing, as opposed to the hearing being hosted by an arbitrator or tribunal secretary, whereas 14% reported no experience with third party service providers and only 7% reported that they were not at all likely to make such a recommendation.

61% reported that participants sometimes or often experienced technical difficulties in the virtual hearings they participated in, but 64% did not believe that such difficulties caused any party to suffer prejudice in the presentation of its case.

Asked about **how effective** a virtual hearing is compared to a physical hearing (for different aspects of a virtual hearing):

- > 32% believe virtual hearings are less effective overall than physical hearings.
- > There was no aspect of an evidentiary hearing that at least half of respondents agreed is less effective by video.
- > Aspects that over 25% agreed to be less effective by video were: cross-examination of fact witnesses (49%), ensuring the integrity of witness testimony (49%), interaction between counsel team members (46%), cross-examination of expert witnesses (40%), witness conferencing/hot-tubbing (43%), potential opportunities for settlement (42%), tribunal deliberations and interaction (37%), direct examination of witnesses (32%), simultaneous and/or consecutive interpretation of testimony in another language (27%), tribunal assessment of the evidence (27%).

7) Expectations regarding virtual hearings post-pandemic

56% of respondents believed that there should be no presumption in favour of physical, hybrid, or virtual hearings. The tribunal should decide what is appropriate based on the individual circumstances of the case. A further 28% leaned towards partially virtual or 'hybrid' hearings.

Looking ahead to post-pandemic circumstances, if any, that may favour a tribunal exercising its authority to convene a fully virtual or hybrid evidentiary hearing over the objection of a party:

- > 9% responded that it is never appropriate to order a virtual hearing over the objection of a party.

- > At least half identified urgency of the matter (58%) and general considerations of cost and convenience (53%) as circumstances that might favour such a decision.
- > Circumstances that less than 10% believed might favour such a decision were where the amount in dispute is over ten million dollars (6%) and where the length of the hearing is expected to be two weeks or longer (7%) or three to five days (8%).

Asked about what considerations, if any, are **significant barriers** to convening fully virtual hearings or hybrid hearings post-pandemic:

- > Considerations identified by more than 25% of respondents were: strong preference for human interaction (49%), concern about the integrity of witness testimony (42%), time zone issues (45%), poor technological infrastructure and/or equipment (44%), inadequate ability to assess eye contact and body language (36%), fatigue (35%), information security and/or data protection concerns (26%), and unfamiliarity with technology (31%).

Appendix B - Sample Procedural Language Relating to Technology Tools and Solutions

The sample language in this Appendix is for guidance only and should be adapted to the facts and circumstances of each case. It is not intended to be exhaustive and does not constitute or operate as a substitute for legal advice on any matters of applicable law. Square brackets are used where different options may be considered.

I. Sample Procedural Directions in Preparing for the First Case Management Conference

Example I.1 - Proposing a case management conference via videoconference

Unless either Party would prefer to convene the case management by telephone, in which case the conference will proceed in that manner, the Tribunal proposes that the conference be convened via videoconference. In addition, unless the Parties notify the Tribunal by *[date]* that they have agreed to alternative arrangements, the Tribunal proposes that *[the President]* host the videoconference via the *[identify videoconferencing platform to be used]*.

Example I.2 - Inviting consideration of how technology will be used to enhance the arbitral process

In order to ensure effective case management pursuant to Article 22(2) of the ICC Rules, in advance of the case management conference, the Parties are invited to confer and consider how technology tools and solutions may be used to help move the arbitration forward efficiently and to save time and costs. Matters that the Parties may wish to consider are described in the ICC Report 'Leveraging Technology for Fair, Effective, and Efficient International Arbitration Proceedings'. In particular, the Parties are invited to consider:

- (a) The means of electronic exchange to be used for communications, exhibits, and other submissions, including whether this case would benefit from a shared case management platform.
- (b) Whether hard copies may be dispensed with or will also or sometimes be provided.
- (c) Prescribed rules for electronic file organisation, naming conventions, and file format.
- (d) Whether the Terms of Reference and/or awards and other decisions may be signed in counterparts and scanned for electronic transmittal to the Secretariat, subject to any requirements of mandatory law.
- (e) Whether the Tribunal and other Party will be required to use any specialised hardware or software in connection with a Party's presentation of case, and, if so, whether any related technical tutorials or conferences should be scheduled.
- (f) Whether any subsequent case management conferences should be conducted by physical attendance or remotely via videoconference or teleconference (and if by videoconference, any preferences regarding the platform to be used, conference host, and/or platform security or other settings).
- (g) Possible use of e-briefs or e-bundles.
- (h) Whether there are any other technology tools or practices that may facilitate the arbitration.
- (i) Any concerns about cost, inadequate access to infrastructure or resources, or fair and equal treatment of the Parties.

- (j) Data protection and information security (addressed further below).
- (k) If there is to be an evidentiary hearing, whether it should be conducted by physical attendance or remotely by videoconference, telephone or other appropriate means of communication (with further details to be addressed at a pre-hearing conference).

Example I.3 – Inviting consideration of data protection and information security

In accordance with [paragraphs 115 and following of the [ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration Under the ICC Rules of Arbitration](#) (1 Jan. 2021) / *other applicable guidance or rules*], the Tribunal reminds the Parties that the European Union Regulation 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 (the ‘General Data Protection Regulation’ or ‘GDPR’) and/or other data protection laws and regulations apply to the arbitration and that their personal data may be collected, transferred, published and archived pursuant to the arbitration agreement or the legitimate interests to resolve the dispute and arbitration proceedings operate fairly and efficiently. (See [ICC Data Privacy Notice for ICC Dispute Resolution Proceedings](#).)

Accordingly, the Parties should be prepared to discuss issues of information security and data protection at the case management conference and are invited to consider the [ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration](#) and the [ICCA-IBA Roadmap to Data Protection in International Arbitration](#) for guidance.

Following the case management conference, the Tribunal may give further directions to the Parties regarding preparation of a data protection protocol for the arbitration to ensure that:

- (a) The Parties, their representatives, as well as their witnesses, party-appointed experts and any other individual appearing on their behalf or in their interest in the arbitration are aware that their personal data may have to be collected, transferred, published and archived for purposes of the arbitration.
- (b) Applicable data protection regulations, including the GDPR are complied with.
- (c) Appropriate technical and organisational measures are put in place to ensure a reasonable level of security appropriate to the arbitration, taking into account the scope and risk of the processing, the state of the art, the impact on the data subjects, the capabilities and regulatory requirements of all those involved in the arbitration, the costs of implementation, and the nature of the information being processed or transferred, including whether it includes personal data or sensitive business, proprietary or confidential information.
- (d) Breaches of the security and confidentiality of personal data, such as unauthorised access to or use of personal data or inadvertent disclosure to persons who should not have been identified as recipients, are reported as may be required by applicable data protection laws and regulations, including to the individual whose personal data may be affected and to the Secretariat.

II. Sample Wording for Terms of Reference Regarding Electronic Notifications and Communications

Example II.1 - Notifications and communications

- (a) Pursuant to Article 3 of the Rules, the Parties and the Tribunal must send copies of all written correspondence directly to all other Parties’ representatives, each arbitrator and the Secretariat simultaneously to the addresses indicated on page [__].

- (b) Communications shall be sent to the Party representatives' e-mail addresses as set out above on or before any date set by the Tribunal and by courier only when required.
- (c) Documents must be sent to the Secretariat in electronic form only.
- (d) *[Any requirement regarding notification and/or depositing of an award at the place of arbitration may need to be addressed.]*
- (e) Subject to any requirements of mandatory law that may be applicable, and unless the Parties agree otherwise, (i) the Terms of Reference may be signed in counterparts and (ii) such counterparts may be scanned and communicated to the Secretariat pursuant to Article 3 of the Rules by e-mail or any other means of telecommunication that provides a record of the sending thereof.
- (f) Likewise, subject to any requirements of mandatory law that may be applicable, the Parties may agree (i) that any award be signed by the members of the Tribunal in counterparts and/or (ii) that all such counterparts be assembled in a single electronic file and notified to the parties by the Secretariat by e-mail or any other means of telecommunication that provides a record of the sending thereof, pursuant to Article 34 of the Rules.

III. Sample wording for first procedural orders

Example III.1 – Communications via e-mail and file share

All submissions and other written communications shall be submitted via e-mail directly to the Arbitral Tribunal, provided that each Party's counsel and the ICC Secretariat are copied simultaneously at the e-mail addresses specified below: *[insert list of names and e-mails]*.

Electronic communications are deemed to be validly made as of the date and time sent.

The Parties agree that e-mail attachments such as submissions and exhibits may be transmitted via Counsel's secure file share sites. In order to facilitate smooth and secure transmissions, any e-mail providing the link for a submission that has been uploaded to a file share site shall: (i) include the name and contact information of a technology support person who members of the Tribunal and opposing Counsel may contact directly in the event of, and for the sole purpose of addressing, any individual difficulties accessing the file share site; (ii) if applicable, state the date on which use of the link will expire; and (iii) identify the specific documents being transmitted (e.g. exhibits CX1-43). Each Party shall designate one person who is to be copied on any communications with the other Party's technology support person and it shall not otherwise be necessary that such communications be copied to the full distribution list.

Example III.2 – Electronic communications (general)

All submissions shall be sent: (i) via e-mail to all Parties and the Tribunal, with copy to the Secretariat, using the e-mail addresses specified below; (ii) where the Parties agree, via a case management website or other service provider; or (iii) via any other means agreed by the Parties.

Example III.3 – Electronic communications via file repository or case management platform

- (a) The Parties shall cooperate with a view to setting up by *[dd/mm/yyyy]* a secure online case management platform.
- (b) Unless otherwise allowed by the Tribunal upon agreement between the Parties, the platform shall be provided by a service provider with an established track record whose terms and conditions ensure that only authorised users may access stored information and that agents or employees of the service provider will have no writing/reading/deletion rights unless the

Tribunal provides written authorisation for the purposes of the individual case. The service provider must be subject to the standards governing the protection of personal data in [country].

- (c) The software environment within which the platform operates must generate logs for (i) access details and (ii) read, write and delete operations concerning each user, which the Tribunal can request from the service provider at any time. Whenever a file is uploaded or downloaded, the system shall automatically send an e-mail containing the pertinent user information to an address to be specified by the Tribunal. Any file upload shall trigger a notification e-mail to all Parties and members of the Tribunal, with a link to the repository where file or files have been uploaded.
- (d) Each member of the Tribunal and each counsel will be assigned a personal user ID and password which only he/she may use and must keep strictly confidential.
- (e) The file repository shall have the following subdirectories:
 - (i) **Arbitral Tribunal.** In this subdirectory, the Tribunal will upload all communications for the Parties, such as procedural orders and letters. Each arbitrator shall have the right to write and read files in this subdirectory. The [President/Sole Arbitrator] shall also have the right to delete files. Any Party shall have the right to read files, except those that are for the Arbitral Tribunal only, such as communications among its members.
 - (ii) **Claimant.** In this subdirectory, the Claimant shall upload all of its written submissions. It may store and download but not alter or delete any files already uploaded in its section. Any deletions must be requested, and will be made only by the Tribunal. The Respondent and the Tribunal shall have the right to read and download files from this subdirectory.
 - (iii) **Respondent.** In this subdirectory, the Respondent shall upload all its written submissions. It may store and download but not alter or delete any files already uploaded in its section. Any deletions must be requested, and will be made only by the Tribunal. The Claimant and the Tribunal shall have the right to read and download files from this subdirectory.
 - (iv) Each of the subdirectories shall include **further subdirectories** (to be created when a submission is made) stating in their file name the date of upload. Within each such subdirectory, the uploading party shall store the submission. Unless a different file structure is technically required for e-briefs, files with attachments to the written submission shall be stored within that same subdirectory.
 - (v) Files uploaded in the repository must be in **searchable PDF** format unless otherwise directed by the Tribunal. The following file formats are also permitted: *[insert file formats]*.
- (f) The access rights specified in subsection (e), (i)-(iv) above shall be implemented technically by the service provider. The Tribunal may direct the service provider to create for its internal communications a private subdirectory from which the Parties are fully excluded. The Parties hereby renounce and waive any right to be given direct or indirect access to this subdirectory in any legal proceedings. If a Party attempts to obtain such access, the members of the Tribunal shall be held harmless and shall bear no direct or indirect cost associated therewith.
- (g) Any difficulty in uploading, downloading, or accessing the file repository must be notified to the Tribunal immediately and in no event later than 48 hours after the first occurrence was noticed. The Tribunal may issue any directions to any Party or the service provider that the Tribunal deems appropriate under the circumstances. The Parties shall provide the Tribunal with the required authorisations, declarations and signatures that the Tribunal may require in order to issue instructions to the service provider.

- (h) The Parties agree that upon completion of the arbitration proceedings, the online file repository may be taken off-line and all stored files deleted from the internet server, subject to a full copy of all files in the repository having been stored on an appropriate data carrier before deletion. This includes the log files. The data carrier shall be stored for a period of [] from the conclusion of the proceedings with [the President of the Arbitral Tribunal/ notary public/ other service provider bound to observe strict confidentiality].
- (i) Costs associated with setting up and maintaining the file repository shall be paid [in equal shares/ *describe any other appropriate proportion of payment*] by the parties and become part of the costs of the arbitration that are to be allocated in the final award. The Tribunal is authorised to issue directions in regard to the payment of costs as it deems fit (Art. 38 of the ICC Rules). This includes an order that a specific deposit be paid for this purpose.
- (j) The Tribunal has the power to amend or change the above as it deems fit if this is required in its view by the circumstances that may arise. Before issuing such directions, the Tribunal will consult the parties.

Example III.4 – E-mail filing followed by upload to file sharing platform, including naming conventions for files; directions for compilation of materials to be provided immediately before the evidentiary hearing

- (a) By the relevant filing date, the parties shall submit by e-mail to the Tribunal Secretary and the opposing party an electronic version of the pleading with witness statements and expert reports; and
- (b) One working day following the filing date, the parties shall upload the pleading with all the supporting documentation and updated index to the file sharing platform that will be created for purposes of this case.
- (c) Electronic files of pleadings, witness statements, expert reports, exhibits and legal authorities shall be text searchable (i.e. OCR PDF or Word).
- (d) All pleadings shall be accompanied by a cumulative index to all the supporting documentation that the party has submitted up to the date of the pleading. The index shall indicate the document number and the pleading with which it was submitted. [*Please follow the naming conventions contained below*].
- (e) At the conclusion of the written phase of the proceeding, on a date to be determined by the Tribunal, or at any other time the Tribunal so requests, the parties shall courier to each Member of the Tribunal a USB drive containing an electronic copy of the entire case file (including pleadings, witness statements, expert reports, exhibits, legal authorities and Tribunal decisions and orders to date) with a 'Consolidated Hyperlinked Index' of all documents.
- (f) The official date of receipt of a pleading or communication shall be the day on which the electronic file is sent to the Tribunal Secretary by e-mail.

Naming conventions

Please follow these guidelines when naming electronic files and for the accompanying Consolidated Hyperlinked Index. The examples provided (in *italics*) are for demonstration purposes only and should be adapted to the relevant phase of the case.

All pleadings and accompanying documentation shall indicate the language in which they are submitted (e.g. SPA=Spanish; FR=French; ENG= English). Such indication should be reflected both (i) in the name used to identify each individual electronic file and (ii) in the Consolidated Hyperlinked Index (which shall be attached to each submission).

For cases with a single procedural language, the 'LANGUAGE' designation may be omitted, except for documents in a language other than the procedural language and the corresponding translations.

Submission Type	Electronic File Naming Guidelines
Main Pleadings	Title of Pleading-LANGUAGE
	<i>Memorial on Jurisdiction-FR</i>
	<i>Counter-Memorial on the Merits and Memorial on Jurisdiction-SPA</i>
	<i>Reply on Annulment-FR</i>
	<i>Rejoinder on Quantum-ENG</i>
Supporting Documentation Exhibits	C-####-LANGUAGE R-####-LANGUAGE To be produced sequentially throughout the case.
	Claimant's factual exhibits
	<i>C-0001-ENG</i>
	<i>C-0002-SPA</i>
	Respondent's factual exhibits
	<i>R-0001-FR</i>
	<i>R-0002-SPA</i>
Legal Authorities	CL-####-LANGUAGE RL-####-LANGUAGE To be produced sequentially throughout the case.
	Claimant's legal authorities
	<i>CL-0001-ENG</i>
	<i>CL-0002-FR</i>
	Respondent's legal authorities
	<i>RL-0001-SPA</i>
	<i>RL-0002-ENG</i>
Witness Statements	Witness Statement-Name of Witness-Name of Submission-LANGUAGE
	<i>Witness Statement-Maria Jones-Memorial on Jurisdiction-SPA</i>
	<i>Witness Statement-Maria Jones-Reply on Jurisdiction-[Second Statement]-ENG</i>
Expert Reports	Expert Report-Name of Expert-Type-Name of Submission-LANGUAGE
	<i>Expert Report-Lucia Smith-Valuation-Memorial on Quantum-ENG</i>
	<i>Expert Report-Lucia Smith-Valuation-Reply on Quantum-[Second Report]-ENG</i>
Legal Opinions	Legal Opinion-Name of Expert-Name of Submission-LANGUAGE
	<i>Legal Opinion-Tom Kaine-Counter-Memorial on the Merits-FR</i>
	<i>Legal Opinion-Tom Kaine-Rejoinder on the Merits-[Second Opinion]-FR</i>

Exhibits to Witness Statements, Expert Reports, Legal Opinions	Witness/Expert Initials-####
	<i>For exhibits filed with the Witness Statement of [Maria Jones]</i>
	<i>MJ-0001</i>
	<i>MJ-0002</i>
	<i>For exhibits filed with the Legal Opinion of [Tom Kaine]</i>
	<i>TK-0001</i>
	<i>TK-0002</i>
	<i>For exhibits filed with the Expert Report of [Lucia Smith]</i>
	<i>LS-0001</i>
	<i>LS-0002</i>
Indices	Consolidated Hyperlinked Index
	Index of Exhibits-C-#### to C-####
	<i>Index of Exhibits-C-0001 to C-0023</i>
	Index of Legal Authorities-RLA-### to RLA-###
	<i>Index of Legal Authorities-RLA-0001 to RLA-0023</i>
Other Applications	Name of Application-[Party]-LANGUAGE
	<i>Preliminary Objections under Rule 41(5)-SPA</i>
	<i>Request for Bifurcation-ENG</i>
	<i>Request for Provisional Measures-[Respondent]-SPA</i>
	<i>Request for Production of Documents-[Claimant]-SPA</i>
	<i>Request for Stay of Enforcement-FR</i>
	<i>Request for Discontinuance-[Claimant]-ENG</i>
	<i>Post-Hearing Brief-[Claimant]-SPA</i>
	<i>Costs Submissions-[Respondent]-ENG</i>
<i>Observations to Request for [XX]-[Claimant]-SPA</i>	

Example III.5 – Limitation on hard copies; naming and organisation of pre-hearing submissions, including compilation of materials immediately before the evidentiary hearing

The Tribunal will require hard copies only of witness statements (if any), expert reports, and legal memoranda, but not exhibits or legal authorities, which shall be provided only in electronic format. Absent further instruction, the Tribunal does not require and will not accept submissions on physical media such as thumb drives. All submissions shall be made via secure e-mail and password protected, uploaded electronically to a secure FTP site, or as otherwise agreed.

All substantive submissions, including letters, shall be accompanied by electronic copies of the principal case and other legal authorities relied upon, which shall be premarked with highlighting to identify the portions of the authority to which the Party is specifically referencing. The Parties are not required to supply authorities they have supplied previously or every authority in a string cite.

All submissions (including exhibits and legal authorities) provided in electronic form shall be text searchable, i.e. OCR PDF (not flattened) or Word.

Prior to the hearing the Parties shall also provide the Tribunal with an electronic hearing compilation containing an index of the case record (with hyperlinks to the extent feasible without incurring undue time or expense). The hearing compilation shall be organised into the folders and files listed below. **Each exhibit shall be separately numbered and shall be accessible as a separate document.**

Folder **1**: Parties' Pleadings and Submissions (including key substantive correspondence)

Folder **2**: Procedural Orders

Folder **3**: Witness Statements

Folder **4**: Expert Reports

Folder **5**: Claimant's Factual Exhibits

Folder **6**: Respondent's Factual Exhibits

Folder **7**: Claimant's Legal Authorities

Folder **8**: Respondents' Legal Authorities

Folder **9**: Reserved for Opening Statement Slides and Demonstrative exhibits, if any

Example III.6 – Naming and organisation of pre-hearing submissions

- (a) Electronic versions of written submissions (briefs, memorials, witness statements and expert reports; for fact exhibits and legal authorities, see paragraphs (b)-(d) below) shall be submitted in a fully text-searchable format (preferably PDF) and, if possible, in an e-brief version, containing hyperlinks to the witness statements, exhibits, and legal authorities cited.
- (b) Electronic versions of witness statements and exhibits shall be submitted in text-searchable (scanned or non-scanned) PDF format, together with a list describing each of the exhibits by exhibit number, date, name of the document, author and recipient (as applicable).
- (c) Legal authorities shall be submitted in electronic format only (unless a hard copy is specifically requested by the Tribunal), following the directions provided for witness statements and exhibits.
- (d) Each witness statement, exhibit or legal authority shall constitute a single electronic document. Electronic versions of exhibits shall commence with the appropriate letter and number ('C-01' or 'CLA-01', and 'R-01' or 'RLA-01'), so that they may be ordered consecutively in the electronic file.

Example III.7 – Designation of technical support person

- (a) Each Party shall designate one person for the duration of the arbitration as an initial point of contact for technology issues (the 'IT Point Person').
- (b) The IT Point Person shall be reasonably available during office hours:
 - > to troubleshoot and resolve technical errors with file share sites or any other software or technology tools jointly being used by the Parties and the Tribunal to facilitate the arbitration; and
 - > to test and ensure the proper functioning of such technology.
- (c) Provided that both Parties' IT Point Persons are copied on communications, it shall not be necessary to direct communications about technology issues to the full distribution list.

Example III.8 – Document production requests

In preparing their document requests, the Parties are encouraged to consider addressing:

- (a) proposed search parameters for electronically stored documents; and
- (b) in order that any concerns about information security and/or technological capability can be addressed appropriately, (i) the proposed format of production (e.g. PDF vs. native format, OCR-searchable or not) and (ii) the proposed means of exchanging documents (e.g. via file transfer site communicated by e-mail) and any associated passwords.

Example III.9 – Use of electronic presentation technologies

- (a) If it wishes to do so, a Party may project a true and accurate image of an exhibit onto a screen in the hearing room. The image must be visible to all counsel, the Tribunal and the witness, and must be large enough to be legible.
- (b) Any counsel who intends to examine a witness about a particular exhibit should offer to provide the witness with a paper copy of the exhibit.
- (c) If both Parties wish to project images, they should cooperate to ensure that they both have equal access to the technology and that duplicative projection equipment is not necessary.

Example III.10 – Joint hearing bundles on tablet

The entire record shall be placed on tablets. The Parties will share equally the cost of four tablets: three for the members of the Tribunal and one for the Tribunal Secretary. The Parties may order additional tablets at their own cost for their own use and for use with the testifying witness. The tablets will be distributed to the Tribunal and the Tribunal Secretary, as requested [*at the hearing venue*] and shall be returned to the Parties at the end of the hearing.

Appendix C – Organisational Checklists for Virtual Hearings

I. Considerations for parties when choosing a third-party service provider as host

- ❑ Experience and reputation
- ❑ Cost and billing arrangements (including amount and timing of deposits)
- ❑ Geographic location/time zone
 - > Can the vendor accommodate early or late hours in its time zone if required? Are there any limitations on this, such as potential cost consequences?
 - > If case participants are located in different regions than the vendor and will require equipment, how will that be handled (e.g. does the vendor have additional locations or partners that can be used to reduce shipping costs)?
- ❑ Data privacy, security, and confidentiality
 - > Enterprise-grade platform license
 - > Compliance with applicable data protection regulations
 - > Willingness to sign confidentiality agreement
 - > Back-up protocols
- ❑ Pre-hearing technical support and equipment
 - > Basic platform orientation and audio/video troubleshooting
 - > Technical support for devices and other software, if needed
 - > One (or more) technical rehearsals with counsel and tribunal
 - > Additional technical rehearsals with individual witnesses and other participants as necessary
 - > What equipment can be provided to case participants, if needed (e.g. cameras, screens, laptops, tablets, microphones, headsets)?
- ❑ Hearing support services
 - > Virtual hearing manager
 - Trained in platform
 - Experience with arbitration
 - > Additional technical support on call
 - Ability to provide local, in-person technical support/equipment when telephone support is inadequate.
 - > Exhibit management
 - What platform will be used to host exhibits? Does it have any special features (e.g. integrated transcript and/or private team chat function)?
 - > Ability to provide other support services (e.g. stenographer, language interpreters).

II. Pre-hearing checklist for parties and tribunals coordinating hearing preparations with virtual hearing host

- ❑ Proposed platform settings
 - > Who will be designated as host and co-host?
 - > Preferences regarding key features (chat, raise hand, recording, closed captioning/live transcripts, data centre regions, global dial-in countries).
- ❑ Technical rehearsal(s)
 - > Use proposed settings and identify any issues,
 - > Test audio/video connections using same location and equipment that will be used for the hearing,
 - > Platform software updated,
 - > Orientation to key functionality (rename, display settings, mute, break-out rooms, waiting room, screensharing, annotation/remote control),
 - > Language interpretation,
 - > Ensure any live transcript can be accessed (e.g. consider whether a special application must be downloaded).
- ❑ Hearing invitation
 - > Consolidated list of names, e-mail addresses, and roles of authorised attendees (tribunal, counsel, witnesses, institutional case managers, corporate representatives, stenographers, interpreters; other support personnel),
 - > Telephone contact details for host and any technical support for the Parties,
 - > Security measures (e.g. password provided separately, avoid party names, no forwarding),
 - > Send invitations for the hearing that start at least 30 minutes earlier than the beginning and end at least two hours later than what is scheduled.
- ❑ Exhibits, witness statements, demonstratives
 - > How will exhibits be organised and called out (e.g. marked as C1, R1, etc., consolidated PDF bundles with bookmarks for individual exhibits and continuous page numbers, exhibit list with individually-linked PDFs)? When and how documents will be provided to host?
 - > Identification of any documents in file formats other than PDF (e.g. video clips).
 - > Features to be used with documents (screenshare, remote control, annotation).
- ❑ Procedures upon joining/departing hearing
 - > Merging phone and video connections where a participant joins audio separately,
 - > Re-naming participants to show full names and roles (e.g. John Doe, Arbitrator, and not jdoe),
 - > Order of witnesses,
 - > Procedures for witnesses waiting to testify/sequestration issues.
- ❑ Means of communicating with host during hearing
- ❑ Organisation of participants into break-out rooms
- ❑ Back-up protocols/contingency plans
- ❑ Review procedural order

III. Counsel's pre-hearing checklist for preparing individual witnesses

Install or update software	Instruct the witness to install the videoconference application on a desktop or laptop computer that will be used for the hearing or, if downloaded, that the latest version is being used. If necessary, the witness can use a mobile device and possibly connect through a web browser, but functionality may be limited.
Witness technical training – same location and equipment	Organise a technical training session with the witness prior to the hearing using the same remote location and equipment that will be used when the witness testifies.
Audio/video quality and related equipment	Check that the witness has a good quality computing device (desktop or laptop), camera (preferably, high-resolution external webcam; if required by the tribunal, a pan-tilt-zoom, 360-degree camera, second camera, or mirrors) and audio (headset with built-in microphone, or microphone and loudspeaker of good quality) from which to connect to the hearing. If necessary, consider providing equipment to the witness.
Optional second screen and document display tools	Test screensharing and any other tools, such as remote control (for scrolling through documents) and/or annotation, that may be used when displaying documents. Check whether the witness has (or consider providing) a second screen that can be used for viewing documents.
Sound settings	If using two cameras with integrated microphones and no separate microphone, verify that the sound is captured by the camera facing the witness. Disable the microphone in the second camera and, if necessary, the computer's own microphone. A separate microphone placed in front of the witness may be preferable.
Conference room settings	If joining from a conference room where other participants will be present, test for audio feedback from other devices.
Camera placement and lighting	Check that the witness' camera is placed at eye level and not too far away from the witness' face. Light should shine on the witness' face (with any light source located behind the camera), as opposed to coming from behind the witness. Check whether blinds or drapes will need to be closed. If using two cameras, verify that the other camera is behind the witness, offering a view of the entire room and the witness' table.
Eye contact and speaker view	Instruct the witness to answer questions by looking straight into the camera and not at the images of other participants. Alternatively, try moving the image of the examining lawyer directly below the camera and use speaker view. Test preferences, and if preferred, ask the witness to disable viewing his/her own image.
Video background	Instruct the witness not to use a virtual background during his/her examination and that the real background be as plain as possible (e.g. white wall; an office setting). The table or desk in front of the witness should be clean and clear of other materials.
Distraction-free environment and business dress	Choose a location for the witness testimony that is distraction free. Instruct the witness to wear business clothes for the hearing. Turn off other devices and programs. Turn off/silence mobile devices and landline upon connecting to the hearing.
Reliable internet connection	Check that the witness is not using a public internet network (i.e. a network to which anyone can connect) and has access to a good quality internet connection, preferably through Ethernet cable. If necessary, consider providing required room/equipment/internet connection tools to the witness. Turn off background software and programs before connecting to the hearing.

Back-up plans	Remind the witness to plug in equipment and have a back-up device to connect to the hearing such as a mobile phone or tablet with an internet hotspot. Provide contact information of persons they should contact in the event of technical difficulty.
Procedural order	Review any special procedures that may be required by the tribunal or, if applicable, instructions for hard copy bundles sent to the witness in advance.
Hearing day check <i>Double-check the above (software updates should be checked several hours in advance).</i>	

IV. Arbitrator's checklist to prepare for virtual hearing

Install or update software	Install the videoconference application on a desktop or laptop computer that will be used for the hearing. Ensure that the latest version is being used.
Audio/video quality and related equipment	Have a good quality computing device (desktop or laptop), camera (preferably, high-resolution external webcam or point, tilt and zoom camera) and audio (headset with built-in microphone, or microphone and loudspeaker of good quality) from which to connect to the hearing. Obtain equipment if necessary.
Number of screens	Consider one or more screens: one for the participants / speakers (counsel, witness, expert, fellow arbitrator); one to see any documents that are being shared; and, if applicable, one for the transcript and/or to show any application being used by the tribunal to communicate privately. Alternatively, a large or wide screen may be sufficient. A tablet may also be useful to pull up copies of exhibits and take notes.
Camera placement and lighting	Camera should be placed at eye level and not too far away from your face. Light should shine on your face (with any light source located behind the camera), as opposed to coming from behind you. Check whether blinds or drapes will need to be closed.
Video background	Turn off any virtual background and ensure that the real background is as plain as possible (e.g. white wall) or professional (an office setting; be careful not to display any confidential materials).
Reliable internet connection	Ensure you have a good quality internet connection, preferably through Ethernet cable.
Back-up	Plug in equipment and have a back-up device to connect to the hearing such as a mobile phone or tablet with an internet hotspot.
Intra-tribunal communications	If applicable, coordinate with co-arbitrators regarding how the tribunal will communicate privately during the hearing (i.e. using a different channel such as telephone, e-mail, messaging, separate video conference room).
Local copies of exhibits	If possible, have exhibits accessible locally rather than via the cloud.
Hearing day – 30 min to one hour prior	
Double-check individual set-up	Double-check the above, ensuring that operating system and videoconferencing software are up to date several hours prior to the hearing.
Mobile phone	Either switch off or mute your mobile phone and/or landline prior to the hearing.
Background software and programs	Turn off background software and programs not needed for the hearing.

Co-host designated	Check that the host designated the co-host.
Audio/video connections verified	Before the hearing starts (ideally 15-30 mins prior), through the hearing co-host, check that the hearing participants are properly connected and set up for the hearing.
Verify connection to live transcript	If applicable.
Hearing day – Joining procedures (as may be specified in pre-hearing order)	
Verify authorised attendees only	<p>Ask all attendees to turn on their cameras and verify visually who is in attendance.</p> <p>Review the participants list in the platform.</p> <p>If anyone has connected separately by audio, ensure the audio and video lines are merged by the host.</p> <p>Ensure the host re-names participants as necessary to show full names and roles (e.g. John Doe, Arbitrator and not jdoe).</p>
Break-out rooms	After verifying attendees and their respective roles, ask the host to set-up break-out rooms so that they are ready when needed and confirm that they have been established correctly.
Etiquette reminders	<p>Mute your microphone if you are not speaking.</p> <p>Address any planned early departures or late joining by individual participants to avoid disruption.</p> <p>Only one person may speak at a time.</p> <p>If chat or raise hand features are enabled, remind participants of agreed protocol.</p> <p>No unauthorised recording or screenshots.</p>
Recording	Recording is on, if applicable.
Hearing day – Witness reminders	
Eye contact	The witness should be instructed to answer questions by looking straight into the camera.
Camera placement and lighting	Check that the witness' camera is placed at eye level and not too far away from the witness' face. Light should shine on the witness' face (with any light source located behind the camera), as opposed to coming from behind the witness. Check whether blinds or drapes will need to be closed. If using two cameras, verify that the other camera is behind the witness, offering a view of the entire room and the witness' table.
Language interpretation	Instruct the witness to take regular breaks while speaking, and to wait for the interpretation to be completed before answering a question or finishing his/her answer.
Breaks in testimony	If the witness' testimony is not completed before a break, take steps to ensure that the witness has no unwarranted contacts with other persons. If the testimony of the witness is not completed before the end of the hearing day, instruct the witness in the usual way not to communicate with counsel and the party until his/her testimony is complete.

V. Counsel's checklist to prepare for virtual hearing

Install or update software	Install the videoconference application on a desktop or laptop computer that will be used for the hearing. Ensure that the latest version is being used.
Audio/video quality and related equipment	Have a good quality computing device (desktop or laptop), camera (preferably, high-resolution external webcam or point, tilt and zoom camera) and audio (headset with built-in microphone, or microphone and loudspeaker of good quality) from which to connect to the hearing. Obtain equipment if necessary.
Number of screens	Consider one or more screens: one for the participants/speakers (counsel, witness, expert, arbitrators); one to see any documents that are being shared; and, if applicable, one for the transcript and/or to show any application being used by your team to communicate privately. Alternatively, a large or wide screen may be sufficient. A tablet may also be useful to pull up copies of exhibits and take notes.
Camera placement and lighting	Camera should be placed at eye level and not too far away from your face. Light should shine on your face (with any light source located behind the camera), as opposed to coming from behind you. Check whether blinds or drapes will need to be closed.
Video background	Turn off any virtual background and ensure that the real background is as plain as possible (e.g. white wall) or professional (an office setting, be careful not to display any confidential materials).
Reliable internet connection	Ensure you have a good quality internet connection, preferably through Ethernet cable.
Back-up	Plug in equipment and have a back-up device to connect to the hearing such as a mobile phone or tablet with an internet hotspot.
Team and client communications	Establish a means for secure private messaging during the hearing (i.e. using a different channel such as telephone, e-mail, messaging, separate video conference room).
Local copies of exhibits	If possible, have exhibits accessible locally rather than via the cloud.
Hearing day – 30 min to one hour prior	
Double-check individual set-up	Double-check the above, ensuring that operating system and videoconferencing software are up to date several hours prior to the hearing.
Mobile phone	Either switch off or mute your mobile phone and/or landline prior to the hearing.
Background software and programs	Turn off background software and programs not needed for the hearing.
Verify connection to live transcript	If applicable.
Verify intra-team communication channel	Use separate devices for intra-team communications to avoid accidentally sharing your internal communications with the other participants to the hearing.
Hearing day – Joining procedures (as may be specified in pre-hearing order)	

Etiquette reminders	<p>Re-name yourself as necessary to show full name and role (e.g. John Doe, Claimant’s Counsel).</p> <p>Mute your microphone if you are not speaking.</p> <p>Give notice of any planned early departures or late joining.</p> <p>Only one person may speak at a time.</p> <p>No unauthorised recording or screenshots.</p>
Verify break-out rooms	If break-out rooms are set in advance to starting the hearing, verify that participants have been accurately assigned.
Recording	Recording is on, if applicable.
Hearing day - Before examining witness	
Change display when examining witnesses	When cross-examining a witness or speaking, consider disabling viewing your own image, as it can be distracting.
Witness verifications	If using two cameras for witness testimony, check the images on the second camera as appropriate and/or consider assigning a team member to watch the additional camera.

Appendix D – Template Procedural Order for Conduct of Evidentiary Hearing via Videoconference

Note. This template pre-hearing Procedural Order only includes language that parties and tribunals may consider using to address specific issues and challenges that may arise in connection with organising a hearing through videoconference.¹ Parties and tribunals should consider any additional language that may be appropriate for matters that regularly arise during hearings (e.g. scope of witness cross-examination, method of time keeping).

Two situations are envisaged:

- > **Option 1**, where the parties and tribunal use the services of a third-party service provider to offer technical support throughout the hearing; and
- > **Option 2**, where no such vendor is engaged.

If no third-party service provider is engaged, the parties and tribunal may wish to consider appointing a tribunal technical assistant for the hearing (e.g. a representative from the arbitral institution, the tribunal secretary, a paralegal in the President's law firm). The tribunal technical assistant would assist the Tribunal in managing the technical issues that arise during a hearing (e.g. reconnecting disconnected participants to a virtual hearing) so that the Tribunal's attention can remain focused on the substantive issues discussed during the hearing.

I. Hearing via videoconference

1. The Tribunal has determined that the evidentiary hearing will be conducted substantially in accordance with the following procedures, subject to any modifications as it may consider appropriate in the exercise of its discretion under Article 26(1) of the ICC Rules.
2. Before issuing this Order, the Parties were invited to review a draft and to comment on various logistical and procedural issues during a pre-hearing conference held on [date] via [video platform], hosted by [option 1: Third Party Service Provider] / [option 2: Tribunal President].

II. [Video platform] hosting and platform settings

3. The evidentiary hearing will be convened via [video platform], hosted by [option 1: Third Party Service Provider] / [option 2: Tribunal President]. The hearing will be deemed to take place at the seat of arbitration, which is [___]. (See ICC Rules, Art. 18(2).)
4. [Option 1: A hearing technician from Third Party Service Provider will be designated as the 'host' of the hearing and will facilitate the hearing, acting under the direction of the Tribunal. As a backup and to avoid disruption in the event that the hearing technician is disconnected, the Third-Party Service Provider will designate [a secondary technician/ the Tribunal President] as a 'co-host'.]

¹ This template builds on hearing procedures suggested by others. See e.g. S. Cohen, 'Draft Zoom Hearing Procedural Order', *TDM* (14 Apr. 2020); AAA-ICDR, 'Model Order and Procedures for a Virtual Hearing via Videoconference' (2021); R.F. Ziegler, 'Draft Procedural Order to Govern Virtual Arbitration Proceedings', *TDM* (9 Apr. 2020).

[**Option 2:** The Tribunal President will be designated as the 'host' of the hearing and will facilitate the hearing, with a Tribunal technical assistant acting as 'co-host' under the direction of the Tribunal President.]

5. In general, the hearing 'host' and 'co-host' will assist in verifying attendees, managing participants' access to the Main Hearing Room and Break-Out Rooms, monitoring departures from the hearing, displaying demonstratives and exhibits, and providing technical support.
6. The [*video platform*] settings that will be used for the hearing, as well as options to be applied when managing Break-Out Rooms, are set forth in Exhibit A to this Procedural Order.
7. The settings in Exhibit A have been made in consideration of preferences expressed by the Parties after discussion with [**option 1:** Third Party Service Provider and the Tribunal] / [**option 2:** the Tribunal], as well as new settings added to the [*video platform*] since then, if applicable. The Parties are responsible for verifying that Exhibit A accurately reflects the settings discussed with the Tribunal. In the event that [*video platform*] changes any available settings after the date of this Order, [**option 1:** Third Party Service Provider will endeavor to draw such changes to the Tribunal's attention] / [**option 2:** the Tribunal will draw attention to any changes for discussion with the Parties and will determine how to apply the new or changed settings].
8. The Parties acknowledge and agree that they have made their own investigations into the suitability, adequacy, and risks of the [*video platform*] and these settings for the evidentiary hearing, including the risk that there will be mistakes in applying the settings in Exhibit A.

III. Hearing notice and authorised attendees

9. In accordance with Article 26(3) of the ICC Rules, the hearing shall be private.
10. By [*date*], the Parties shall submit to the Tribunal a list of the names and e-mail addresses of the persons who will be attending the hearing on their behalf, including counsel, corporate representatives, witnesses, and any support personnel, as well as the physical location they will be joining the hearing from. The Parties shall also include the names and e-mail addresses of the stenographer(s) and language interpreter(s) they have agreed to engage for the hearing.
11. [**Option 1**] The Tribunal will send a consolidated list of authorised hearing attendees to Third Party Service Provider.
12. Before the hearing, [**option 1:** Third Party Service Provider] / [**option 2:** Tribunal President] will e-mail a [*video platform*] weblink, 'Meeting ID,' and passcode to each person whom the Tribunal identifies as an authorised attendee. Unless the Tribunal determines otherwise, only those persons shall be authorised to attend the hearing, subject to any rules on witness sequestration.
13. E-mail invitations shall be unique to each attendee and shall not be shared with others.
14. The Parties acknowledge and agree that unless either Party requests otherwise by [*date*], the passcode may be provided by [**option 1:** Third Party Service Provider] / [**option 2:** the Tribunal President] in the same communication as the [*video*] weblink and Meeting ID.
15. The hearing invitation will also contain the contact information (name, e-mail, and telephone number) of [**option 1:** the Third Party Service Provider personnel who will facilitate the hearing] / [**option 2:** the Tribunal technical assistant].

16. [*Revise as applicable*: The Parties acknowledge and agree that some attendees will join the hearing from their own, individual locations while others may join the hearing from the same location. This means that some witnesses may testify in the presence of counsel (and others not), some counsel teams may be together (and others not), and some counsel and client representatives may be together (and others not). No attendees will be present at the same location as the Tribunal.]

IV. Technical capabilities and pre-hearing testing

17. [**Option 1**: Counsel shall discuss whether Third Party Service Provider will provide equipment to any hearing participant.] / [**Option 2**: The Parties shall be responsible for their own technical equipment.]
18. To optimise the video hearing, dual monitors are recommended, with the [*video platform*] running on one screen.
19. A [*video platform*] test among [*Include as applicable*: all participants/counsel, the Tribunal, witnesses, experts interpreters, stenographers] [**option 1**: and Third-Party Service Provider] was conducted on [*date*], as part of the pre-hearing conference on [*date*].
20. The purpose of the test was to allow the hearing participants to assess the quality of their audio and video transmissions and to make necessary adjustments, as well as to experience key platform functions, including microphone muting, display options, transitions between the Waiting Room, Hearing Room, and Break-Out Rooms, and screensharing.
21. If the Tribunal determines following the test that [*video platform*] will be inadequate to allow the Parties to present their cases, the Tribunal reserves discretion to determine that the evidentiary hearing will be conducted by other means.
22. Before the hearing, each Party shall be responsible for testing the [*video platform*] with its witnesses, client representatives, and any other persons attending the hearing on its behalf to ensure that such persons: (i) have suitable equipment to use [*video platform*] and participate in the hearing; (ii) are familiar with basic features of the [*video platform*]; and (iii) that they are familiar and comply with all logistical and other requirements of this Order. In particular, as concerns witnesses, each Party shall advise its witnesses of this paragraph [22] and of the further provisions in paragraphs [24-26] regarding connecting to [*video platform*] and paragraphs [38-41, 43] with respect to testifying.
23. The Parties also undertake to take reasonable steps to confirm with the stenographer(s) and interpreter(s) that they have suitable equipment to use the [*video platform*] and participate in the hearing and that they are familiar with the basic features of the [*video platform*] and any applicable requirements of this Order.
24. Hearing attendees shall be responsible for ensuring that the [*video platform*] application on their device is up-to-date. As of the date of this Order, the latest version of [*video platform*] is [___].
25. To safeguard the privacy of the video hearing, no participant shall join from a public setting or use unsecured, public Wi-Fi.

26. Hearing participants shall make reasonable efforts to ensure that there will be clear video and audio transmission during the hearing. Among other things, participants should consider:
- (a) Accessing the [*video platform*] through whatever device or combination of devices that provides the best combination of audio and video quality, including (as appropriate) using a phone (rather than a computer) for audio and, if there is to be simultaneous language interpretation, a headset with microphone.
 - (b) Steps that may establish a more reliable, high-speed internet connection, including:
 - > using a hard-wired rather than wireless internet connection; and
 - > turning any unnecessary computer applications off rather than leaving them running in the background.
 - (c) Steps that may improve audio transmission, such as:
 - > using the computer microphone and reserving the optional dial-in number in case of poor quality internet access;
 - > considering whether a headset would improve transmission;
 - > eliminating foreseeable background noise and warning any unauthorised persons in close proximity that a hearing will be taking place and is not to be disturbed.
 - (d) Steps that may concern camera positioning and lighting to optimise video images, such as:
 - > avoiding sitting near a window;
 - > positioning lights in front of (not behind) the camera; and
 - > raising the webcam to eye level.
 - (e) Whether computing devices and related equipment such as headsets are adequately charged and whether power cables or back-up batteries are available as may be necessary.
 - (f) Steps that may accommodate multiple participants joining from the same endpoint, including optimum seating arrangements, camera positioning, and checking for potential negative audio feedback or static arising from multiple devices.

V. Hearing exhibits

27. [*Counsel to discuss whether some or all witnesses will be sent packages with exhibit binders to be opened on camera OR whether exhibits will only be displayed electronically via screenshare. Counsel should also consider whether a different protocol is appropriate for expert witnesses. If hard copies are necessary, a protocol such as the following might apply.*]

The Parties have agreed as follows with respect to providing witnesses with clean, unannotated exhibits and witness statements prior to the hearing, for use during the hearing:

- (a) By [*date*], Counsel shall coordinate providing each witness with one or more binders containing: (i) a clean, unannotated hard copy of the witness' witness statement(s); and (ii) a clean, unannotated hard copy of each of the exhibits which Counsel intends to show the witness on either direct or cross-examination ('Hearing Bundle').
- (b) The Hearing Bundle should contain all documents that, before the hearing, Counsel reasonably believes will be shown to the witness. However, a full set of the exhibits will also be available electronically and displayed by [**option 1**: Third Party Service Provider] / [**option 2**: the Tribunal technical assistant] via screenshare during witness examinations.
- (c) If a witness will attend the hearing outside the presence of Counsel, that witness will be provided with the Hearing Bundle in a sealed package or envelope that must remain sealed until the witness is instructed to open it, on camera, at the commencement of the witness' testimony.

28. [**Option 1:** Counsel to discuss with Third Party Service Provider and the Tribunal: (i) timing and means of submitting electronic exhibits and demonstratives to Third Party Service Provider; (ii) whether there will be exhibits in different formats (e.g. Excel, video clips, etc.); (iii) shared nomenclature for pulling up exhibits (e.g. individual exhibit number plus page number).]

VI. Hearing schedule

29. The hearing schedule below includes [] hours of time in reserve, to be used in the event of unforeseen technical problems that may occur during the video hearing.

VII. Procedures upon joining the hearing

30. To ensure a timely start of the hearing, on at least the first day of the hearing (or the first day for any witness) participants should access the [video] hearing using the credentials provided by [**option 1:** Third Party Service Provider] / [**option 2:** the Tribunal President] at least [] minutes before the scheduled start time. Before the scheduled start time, participants will be directed to a virtual Waiting Room where they will remain until the Tribunal is ready to start the hearing and directs [**option 1:** Third Party Service Provider] / [**option 2:** the Tribunal technical assistant] to admit the participants to the Hearing Room.
31. When it appears that all participants have established their audio and video connections and are ready to begin, the Tribunal will verify who is in attendance visually and with reference to the [video platform] participants list. Anyone connecting by telephone will be asked to speak and confirm their identity and, if also connecting separately by video, may have their connections 'merged' so that they are listed only once as a participant. Attendees may also be renamed to display first and last name and role/affiliation (e.g. 'Jane Doe, President' or, in case of multiple attendees at one location, 'Claimant Room').
32. Participants may not use a 'Virtual Background'. Instead, the remote room in which they are located must be visible.
33. After verifying who is in attendance, the Tribunal will ask that all hearing participants: (i) mute their microphones unless they are speaking or need to interject; and (ii) turn off their video feeds. Notwithstanding the foregoing, the following persons shall leave their video feed on during the hearing, unless determined otherwise by the Tribunal:
- > lead Counsel;
 - > any witness who is testifying;
 - > the interpreter, if language interpretation is being provided; and
 - > the Tribunal.²
34. [**Option 1:** Third Party Service Provider] / [**option 2:** the Tribunal President] may mute participants if necessary (e.g. to reduce background noise from someone who has neglected to mute).

2 By controlling whose video feed is operational in this manner, all attendees will be able to optimise their view of key participants by choosing 'hide non-video participants' in their individual 'video settings' (available from the drop-down menu next to the video camera icon in the lower left-hand side of the screen).

35. To avoid unnecessary disruption during the hearing as well as concern about whether an attendee is experiencing difficulty establishing or maintaining technical connection to the hearing, the Tribunal expects that hearing attendees shall make best efforts to avoid joining the hearing late or departing from the hearing without prior warning (to be given at an appropriate time such as at the beginning or end of a break).

VIII. Hearing record

36. Except as provided herein, no recordings (whether audio, video, or screenshot) shall be permitted. No unauthorised persons shall be given access to live video or audio feed of the proceedings.
37. The Parties agree that the stenographer will transcribe and provide the official record for the proceedings and acknowledge that the stenographer may record the proceedings in connection with his or her regular business practices to prepare the final transcript. From time to time, the stenographer may intervene to clarify items for the record.

XIX. Witness examination procedure

38. **Witness camera and remote venue set-up.** Witnesses' faces must be clearly visible while testifying. To the extent possible, a witness' webcam should be positioned at face level, relatively close to the witness (e.g. by positioning a laptop on a stack of books).
39. If two cameras are used for the purpose of examining a witness, the second camera shall be placed behind the witness, in a location that allows a view of the entire room, as well as of the witness' desk or table.
40. Witnesses should give evidence from a clear desk or table. If this is not strictly possible, the Tribunal may ask a witness to orient their webcam to provide a closer view of any materials in the witness' environment in order to verify that the witness is not referring to or relying upon unsanctioned information while testifying.
41. At any time, the Tribunal may ask a witness to orient their webcam to provide a 360-degree view of the remote venue in order to confirm that no unauthorised persons are present and that no unauthorised devices or notes are being used or relied upon.
42. **Language interpretation.** By [*date*], the Parties shall inform the Tribunal: (i) whether the interpreter will attend in the same or a remote location from the testifying witness; (ii) whether certain materials such as witness statements or an agreed glossary of terms will be provided to the interpreter for preparation purposes prior to the hearing; and (iii) whether the interpreter will be provided Hearing Bundles or only view exhibits and witness statements electronically via screenshare. As noted above, the interpreter will have access to the real-time transcript.
43. **Instructions.** The Tribunal will instruct the witness regarding the following and seek the witness' confirmation that:
- (a) The witness will not rely on any notes while testifying or receive any assistance with his or her testimony.
 - (b) The witness will not make any recordings or screenshots of the proceedings or provide access to the live audio or video to any person.

- (c) In the case of any witness who is testifying outside the presence of Counsel:
 - > no one else is present in the remote room where the witness is testifying;
 - > except for any device being used to connect to [video platform], all other devices in the witness' presence (including smartphones, computers, and tablets) are turned off; and
 - > any device being used to connect to [video platform] shall not be used for any other purpose during the hearing unless permitted by the Tribunal;
 - (d) In the event of a disconnection or other technical difficulty, the witness understands how to contact [option 1: Third Party Service Provider] / [option 2: the Tribunal technical assistant] (i.e. using the information provided in the hearing invitation).
44. The Parties agree that Counsel shall be prohibited from conferring with any witness from the time that witness begins being cross-examined until the time he or she is dismissed, including during any breaks in his or her testimony.

X. Private communications

45. The 'Chat' function in [video platform] will be disabled.
46. To avoid delay and difficulty reconnecting, hearing attendees should not disconnect from the [video] hearing during any recess. Ordinarily, the Tribunal will direct that participants be separated into 'Claimant', 'Respondent', 'Tribunal', 'Interpreter', and 'Stenographer' Break-Out Rooms (or such other Break-Out Rooms as may be appropriate) to facilitate private conversations during recesses. Any witness who is testifying will remain in the Main Hearing Room.
47. [Video platform] settings that will apply when Break-Out Rooms are used are set forth in Exhibit A and include the following:
- (a) Participants will be moved to Break-Out Rooms automatically upon being assigned to a room by Third Party Service Provider.
 - (b) When a Break-Out Room is closed, a countdown of 60 seconds shall apply before participants are returned to the Main Hearing Room. Once the countdown begins, participants may return to the Main Hearing Room on their own.

XI. Technical support

48. [Option 1: Third Party Service Provider] / [option 2: the Tribunal technical assistant] will provide the Parties with technical support during the hearing.
49. Technical support from [video platform], including video tutorials that cover the basics of using [video platform], is available at [link]. The [option 1: Third Party Service Provider] / [option 2: Tribunal technical assistant] shall provide a telephone number where they can be reached throughout the Hearing.

50. In the event that a participant is disconnected from the videoconference or experiences some other technical failure:
- (a) upon being alerted to the issue, the Tribunal may take steps to ‘pause’ the hearing and ask [option 1: Third Party Service Provider] / [option 2: the Tribunal technical assistant] to assist the participant with reconnecting or resolving the technical issue;
 - (b) the participant suffering from technical failure should immediately seek to re-connect and to contact [option 1: Third Party Service Provider] / [option 2: the Tribunal technical assistant] by phone or e-mail if his or her initial attempt to re-connect is unsuccessful;
 - (c) once the disconnected participant has re-joined the hearing, if necessary, the Tribunal will recap what the participant missed; and
 - (d) if, in a timely manner, connection cannot be re-established or the issue cannot be resolved, the Tribunal may consider other measures, including but not limited to moving participants into Break-Out Rooms, taking a recess, or directing participants to dial-in to a back-up audio conference line.
51. If the Tribunal deems it unfair to any Party to continue the video hearing because of a technical failure, or otherwise determines that the platform does not permit the Parties to adequately present their cases, the Tribunal may terminate the videoconference at any time and take such other steps as may be necessary to ensure the fairness and integrity of the proceedings.

[date]

SO ORDERED

[Arbitrators]

Appendix E - Checklist of Issues to Consider When Choosing an Online Case Management Platform

Definitions	<p>For the purpose of this checklist, the following terms are defined as follows:</p> <ul style="list-style-type: none"> > 'OCMP': online case management platform > 'Users': parties, arbitral tribunals, administrative secretaries, the institution and, as the case may be, experts > 'Communications': e-mails, messages, correspondence, any type of document (submissions, exhibits, witness statements, expert reports, procedural orders, decisions, awards) > 'OCR': optical character recognition > 'DRO': dispute resolution organisation
Core service to be provided by an OCMP	<p>The cornerstone to successfully motivate the Users to make use of an OCMP is its capability to standardise and centralise information, and to make that information easily accessible. An OCMP secure system should offer the possibility to generate, send, receive, store, retrieve, exchange or otherwise process Communications (including, but not limited to, large sensitive documents) used in an arbitration, as well as tracing of the Communications.</p>
Other services offered by an OCMP	<p>The platform should initially present general information to any visitor and user:</p> <ul style="list-style-type: none"> > Video or other tutorial of the platform's basic functions and features. > News informing about any upgrades and additional services offered. > Whether technical support is available 24/7. > Whether there is a default folder structure available and the nature thereof. > The OCMP's level of security in all aspects and whether the platform benefits from a security certifying body (i.e. ISO standard) and displays the certificate logo of such certifying body. > The applicable data protection regulation (i.e. governing jurisdiction) and geographical location of primary storage of data and backup storage (where servers and/or encryption keys are located). > Whether the transfer of any data and document is end-to-end encrypted during transfer and whether stored data is encrypted. > Service and maintenance of the OCMP without access to readable content. > Whether the service employs zero-knowledge encryption: (i) who has access to the encryption keys (the DRO and/or third-party OCMP supplier or possibly a DRO; and (ii) can the encryption keys be deposited with a third party in another jurisdiction (to protect the parties against court orders generated by third parties or authorities outside the ongoing arbitration case). <p>.../...</p>

<p>Other services offered by an OCMP (continued)</p>	<ul style="list-style-type: none"> > Format of materials which may be uploaded (for example, .docx, .xls, .pdf, .jpeg, .mov, .mp4) and whether it takes compressed files, locked PDFs etc. (the arbitral tribunal may wish to request both locked and searchable versions of documents in a procedural order). > Maximum size accepted for each material. > Languages recognised by the OCR. > Whether keyword search and filtering is possible. > Whether the OCMP has an integrated hearing facility, including break-out rooms, recording, etc. (see checklist on virtual hearings) and whether it offers any troubleshooting assistance during hearings. > Whether Users can create their own individual space within the case to prepare material for a hearing and for personal notes to be saved in such space, with mark-up tools. > The provider's procedure for entering into the contract and which participant(s) to the arbitration will be signatories to the contract with the OCMP provider. > Information on the login techniques for registered individuals.
<p>Terms and conditions of service</p>	<p>The OCMP's terms and conditions may be non-negotiable but must be acceptable to all Users of the platform.</p> <p>The OCMP should undertake to take reasonable steps to remedy any interruption of the system as quickly as possible, if such interruption is on its/their system. However, the following exclusions of liability are typical: exclusion of liability for the content of Communications uploaded by the Users on the platform; exclusion of liability for any internet interruption, speed, performance or otherwise, which cannot be guaranteed, or for any problem of connection or any other technical problem unrelated to the services offered by the OCMP.</p> <p><u>Terms and conditions</u> should indicate the default period during which parties and the arbitral tribunal may still access their case on the OCMP at the end of the arbitration. However, the parties and the arbitral tribunal may agree on a shorter or longer period (see 'Document retention' below).</p>
<p>Agreement and Commitment to use the OCMP for the arbitration</p>	<p><u>Commitment to use the OCMP</u> should be recorded in an agreement by the parties and/or a procedural order that addresses the following.</p> <p><u>Scope of use</u>: parties and the arbitral tribunal should decide if they wish to use the service for complete management of the case online (e.g. built-in secure videoconferencing, e-bundling of documents), or if they wish to use it only as a repository, i.e. for upload, download and storage of Communications.</p> <p><u>Document retention</u>: The parties and the arbitral tribunal may agree on a shorter or longer period than the default retention period for data by the OCMP. At the end of the period during which access to the case is possible, the OCMP may destroy any data and documents uploaded.</p> <p><u>Other procedural agreements</u>: consider procedural aspects such as who will bear the costs, exclusions of liability, or rules concerning access rights and security.</p> <p><u>Default rules for organising documents and uploading files</u>: naming conventions for folders and files must be standardised for the OCMP to be of maximum benefit. (See below for sample structure.)</p>

Acceptance by the DRO, if applicable	If there is an administering institution, it should agree that use of the OCMP is acceptable to it.
Equipment	Users should ensure they have the necessary equipment enabling them to access the OCMP, including but not limited to suitable software, hardware and internet connection.
Access credentials	Users should keep their access credentials strictly confidential.
Confidentiality and authorised Users	Access to the case on the OCMP should be limited to the parties and/or their representatives, the arbitral tribunal, any administrative secretary, and the DRO. A list of such Users must be established and shared with the Users or simply listed in the OCMP. (See below, organisation of sections of the OCMP.)
Uploading of documents	Parties and the arbitral tribunal should commit to upload on the OCMP any Communication, unless otherwise agreed by the parties and the arbitral tribunal where Communications would preferably be transmitted in hard copy due to their size or legibility (e.g. construction plans or large spreadsheets). Once uploaded on the OCMP, no Communication should be deleted, recalled or amended in any way (similarly to sending documents by post).
Alerts following upload	The OCMP should send automatic alerts to the Users in an arbitration for every Communication uploaded by any User. Such alerts should be sent to the intended recipients of the Communication. The arbitral tribunal and the parties should discuss the issue of proof of opening a message and downloading of a document being provided to the sender of the Communication (e.g. proof of downloading procedural directions by the parties vs. proof of downloading the parties' exhibits by the arbitral tribunal). In addition to indicating the e-mail address they wish to use in the arbitration, Users must ensure that the e-mail address sending alerts is whitelisted and does not land in a spam-box. Users should also regularly check the OCMP to make sure they have not missed a communication and to verify the various procedural dates.
Authors of uploading	Documents should be uploaded directly by their authors. The OCMP does not upload documents on behalf of a party or the arbitral tribunal. Tracing the author of an uploading, the date and time such uploading took place is important and must be ensured by the OCMP.
Default rules for organisation of case information, folders and uploaded documents	Consideration should be given to organisation of the following, which may be done by default by the OCMP or subject to customisation by the Users. <u>Overview of the case:</u> names of parties, their representatives and arbitrators, as well as administrative secretary, global amount in dispute, place of arbitration, applicable law, language of arbitration, stage of the procedure. <u>Contact details</u> of all Users in a case. <u>Arbitral tribunal:</u> names, who appointed them, date of their appointment, access to their CV and statement of independence, including comparable data for the administrative secretary. ... /...

<p>Default rules for organisation of case information, folders and uploaded documents</p> <p>(continued)</p>	<p><u>Financial aspect</u> of the case, including amounts in dispute, payments of the advance made by the parties, expenses incurred by the arbitral tribunal, fees of the arbitral tribunal and any administrative secretary.</p> <p><u>Timetable</u>: all deadlines fixed in a procedure, any extension granted and if the expected performance was met.</p> <p><u>Correspondence</u>: all correspondence uploaded by any User.</p> <p><u>Submissions</u>: upload should only be made available to parties.</p> <p><u>Exhibits</u>: upload should only be made available to parties.</p> <p><u>Procedural orders</u>: upload should only be made available to the arbitral tribunal, and any administrative secretary.</p> <p><u>Terms of reference and awards</u>: upload should only be made available to the arbitral tribunal, any administrative secretary.</p> <p><u>Index of all documents</u>: all documents uploaded on the platform in a chronological order.</p> <p><u>Common bundle</u>: if parties produce a common bundle for a hearing.</p> <p><u>Forums</u>: as follows to allow defined separate groups of Users to communicate amongst themselves (with the exclusion of other Users) without leaving their secure arbitration environment and avoiding any mistaken recipient.</p> <p><u>Sorting order</u>: all sections with documents, financial aspect and timetable should offer the possibility of sorting information and documents in various orders, such as newest to older date and vice-versa, only documents posted by a given author, only types of documents uploaded (example submissions), only formats of document (for example, .pdf).</p> <p><u>Referencing of documents</u>: when uploading Communications, the system should allow dropdown menus of standard information to be selected for uploading documents:</p> <ul style="list-style-type: none"> > date format: yyyy-mm-dd for year-month-day > case reference used by a DRO or proposed by an OCOMP > an abbreviation for each type of User (e.g. 'C' for claimant) > an abbreviation for document type (e.g. 'L' for letter; 'Ex.' for exhibit; 'WS' for witness statement; 'ER' for expert report) > brief further description (e.g. 2021-10-10 ICC 12345 C L time to cross-examine witnesses; 2021-09-17 ICC 23456 R Reply on Jurisdiction)
---	---

ICC COMMISSION ON ARBITRATION AND ADR

As a unique think tank in the world of international dispute resolution, the Commission on Arbitration and ADR raises awareness and understanding on practical issues in arbitration and ADR in the form of Commission Reports. The Commission also provides input on proposed modifications of rules applied in ICC Dispute Resolution Services (including the ICC Rules of Arbitration, the ICC Mediation Rules, Expert Rules and Dispute Board Rules).

This ICC global commission brings together experts and practitioners in the field of arbitration and ADR has currently over 850 members from some 100 countries. The Commission holds several plenary sessions per year, at which proposed rules and Commission Reports are discussed, debated, and voted upon. Between these sessions, the Commission's work is often carried out in smaller **task forces**. The Commission's products are made available on the [ICC website](#) and [digital library](#).

What the Commission does:

- In its research capacity, produces reports on legal, procedural and practical aspects of dispute resolution and other relevant topics in the field.
- Develops tools for efficient and cost-effective dispute avoidance and settlement by means of arbitration, mediation, expertise and dispute boards and enables ICC dispute resolution to respond effectively to users' needs.
- Creates a link among arbitrators, mediators, experts, academics, practitioners, counsel and users of dispute resolution services from all over the globe and a forum to exchange ideas and experiences with a view to improve dispute resolution services.

ICC Commission on Arbitration and ADR

www.iccwbo.org/commission-arbitration-ADR

commission.arbitrationADR@iccwbo.org

T +33 (0)1 49 53 30 43

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 100 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

www.iccwbo.org

Follow us on Twitter: [@iccwbo](#)

