



South Carolina Bar

Continuing Legal Education Division

2026 SC BAR CONVENTION

International Law Committee

“International Legal Issues: 2025
Retrospective and Things to Come”

Thursday, January 22

SC Supreme Court Commission on CLE Course No. 260350

SC Bar-CLE publications and oral programs are intended to provide current and accurate information about the subject matter covered and are designed to help attorneys maintain their professional competence. Publications are distributed and oral programs presented with the understanding that the SC Bar-CLE does not render any legal, accounting or other professional service. Attorneys using SC Bar-CLE publications or orally conveyed information in dealing with a specific client's or their own legal matters should also research original sources of authority.

©2026 by the South Carolina Bar-Continuing Legal Education Division. All Rights Reserved

THIS MATERIAL MAY NOT BE REPRODUCED IN WHOLE OR IN PART WITHOUT THE EXPRESS WRITTEN PERMISSION OF THE CLE DIVISION OF THE SC BAR.

TAPING, RECORDING, OR PHOTOGRAPHING OF SC BAR-CLE SEMINARS OR OTHER LIVE, BROADCAST, OR PRE-RECORDED PRESENTATIONS IS PROHIBITED WITHOUT THE EXPRESS WRITTEN PERMISSION OF THE SC BAR - CLE DIVISION.

The South Carolina Bar seeks to support the ideals of our profession and believes that all Bar members have the right to learn and engage in the exchange of ideas in a civil environment. The SC Bar reserves the right to remove or exclude any person from a Bar event if that person is causing inappropriate disturbance, behaving in a manner inconsistent with accepted standards of decorum, or in any way preventing fellow bar members from meaningful participation and learning.

Disclaimer: The views expressed in CLE programs and publications do not necessarily reflect the opinions of the South Carolina Bar, its sections, or committees. The South Carolina Bar believes that all Bar members have the right to both meaningful learning and to the exchange of ideas in a civil environment. The Bar reserves the right to remove or exclude any person from a Bar event if that person is causing inappropriate disturbance, behaving in a manner inconsistent with accepted standards of decorum, or in any way preventing fellow Bar members from meaningful participation and learning.



South Carolina Bar

Continuing Legal Education Division

Immigration Changes in 2025: The Courts, the Consulates and CBP

Melissa Drennan

Brad Banias

Immigration Changes in 2025: The Courts, the Consulates, and CBP

Bradley Banias - Managing Partner, Banias Law

Christopher Richardson – President & General Counsel, BDV Solutions

Melissa B. Drennan – Senior Associate, Herbert Smith Freehills Kramer (US) LLP

Charleston, SC



**South
Carolina
Bar**

1

Preview



- **Litigation updates**
- **Updates on the U.S. consulates abroad issuing visas**
- **U.S. Customs & Border Protection (CBP) updates**

2

Litigation



- **Plenary Power v. Due Process:** Can EVERY immigration restriction be justified by a *claim* it impacts national security?
 - **Obvious Cases:** Challenges to ICE efforts, National Security, and habeas
 - **\$100k H-1B fee:** "The large-scale replacement of American workers through systemic abuse of the program has undermined both our economic and national security."
 - **Terminating F1 Students with No Notice:** "To eliminate vulnerabilities related to the nonimmigrant visa program . . ."
 - **Ending Automatic EAD extensions:** "The automatic extension therefore poses a security vulnerability that could allow bad actors to continue to work and generate income to potentially finance nefarious activities that pose an imminent threat to the American Public."
- We could see significant impact on separation of powers case law.

3

Litigation Updates



- **Birthright Citizenship:** "subject to the jurisdiction thereof."
- **ICE-related:** habeas cases (no bond hearings, re-detention), deployment of national guard, penalties for "sanctuary cities," and deportation under Alien Enemies Act
- **Temporary Protected Status (TPS)**

4

Consular updates



- **“Extreme vetting”**
- **Department of State guidance that visa applicants should only apply in their home country or country of residence. What does residence mean?**
- **Changes in interview waiver (drop box/mail in) policy**
- **Travel bans**
- **Public Charge**
- **Impacts on scheduling of J-1 and F-1 visas**
- **Increased scrutiny on O-1s**
- **Impacts of reduction/change in staff**
- **Increased focus on social media vetting, importance of making public**
- **Certain categories need to get DC approval (e.g., B-1 in lieu H-1B)**

5

CBP Border updates



- **Increased scrutiny at the border, lot of media attention**
- **Secondary inspection, electronic searches, DC review**
- **Carry documents, scrutiny on having proper work visa and parameters of B-1/WB visitors and risks**
- **\$1k parole fee and exemptions**
- **No right to attorney at the border**
- **USCIS versus border applications, awareness of border treatment (TNs, etc.), strategies for each port**

6

Questions? Comments?



- Questions?
- Thoughts?
- Feel free to email us,
 - Bradley Bantias – brad@baniaslaw.com
 - Christopher Richardson – crichardson@bdvsolutions.com
 - Melissa B. Drennan – Melissa.Drennan@hsfkramer.com



South Carolina Bar

Continuing Legal Education Division

Interesting Times: Trade and Foreign Business Transactions

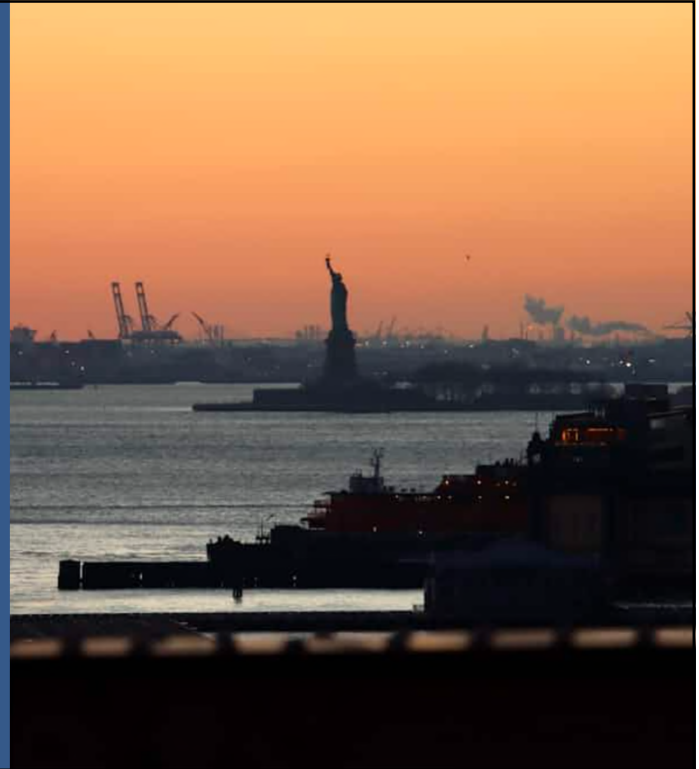
*Ford Graham
Jay Rogers
&
Doug Fraser*

Tariffs: Practical Approaches to Navigating the New New Landscape

James L. (Jay) Rogers

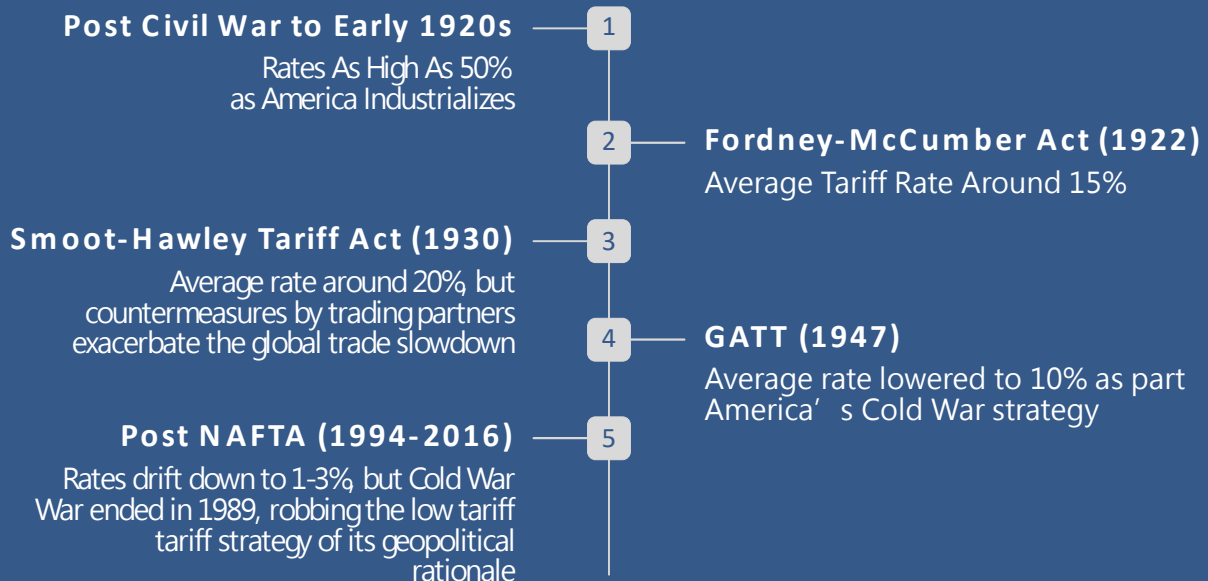
| Partner, Nelson Mullins

jay.rogers@nelsonmullins.com



1

Historical Average US Tariff Rates



2

Current Average U.S. Tariff

As of August 2025: **10.5% overall**, but China at **39.2%**. Also...

39.8%

Steel/Aluminum

21%

Automotive

Source: Wharton School of Business at U. Penn

3

Who Pays Tariffs?

- Technical Answer: Importer of Record
- More Complete Answer: It Depends

4

Tariff Mitigation Strategies for Your Clients

3 Basic Themes

Country of Origin

COO turns on place of last Substantial Transformation or Tariff Shift

Valuation

Since most tariffs are ad valorem, lowering customs value of goods will lower the tariff

Classification of Goods

Under the Harmonized Tariff of the United States (HTSUS)

5

Tariff Exemptions and "Inclusions"

No Formal Exemption Process

No formal exemption process exists, in contrast to first Trump term

Inclusions Are Possible

"Inclusions" are additions to the Copper, Steel, and Aluminum derivative products lists at the specific request of U.S. Companies and/or Industry Groups, with a **90% plus success rate** thus far for U.S. Industry

- ❑ Some Administration voices acknowledging that exemptions are needed for goods not made in U.S. (e.g. - Scott (e.g. - Scott Bessent)

6

Refunds of IEEPA Tariffs?

“False Claims Act” Relator/Qui Tam
Actions for Unpaid Tariffs



South Carolina Bar

Continuing Legal Education Division

Development in International Dispute Resolution

*Usher Winlett
Kathleen Paisley
Henery Parr
&
Kate Gonzalez*

It's The Result That Matters

By Usher Winslett



The purpose of arbitration is elegantly summarized in the introduction to the CPR Non-Administered Arbitration Rules: “The primary objective of arbitration is to arrive at a just and enforceable result, based on a private procedure that is fair, expeditious, economical, and less burdensome and adversarial than litigation.” While most arbitrators would take no issue with this statement, if asked to summarize an arbitrator’s primary obligation, they would reflexively respond, “to render an enforceable award.” But note that the word “award” appears nowhere in the CPR’s mission statement. Indeed, CPR conspicuously avoids using the phrase “enforceable *award*.” By using “enforceable *result*” instead, it puts priorities in the right place. The end result of the arbitration need not be a final award, but it must be fair, expeditious, economical – and, of course, enforceable.

While issuing an enforceable award is certainly an essential goal, it vastly diminishes the arbitrator’s role to call it the *primary* objective. After all, no final award is issued in the overwhelming majority of cases. And the parties are generally better served when their disputes can be resolved without the need for a final award. So, an arbitrator’s foremost, overarching responsibility is to provide parties with the most efficient and economical way to resolve their disputes – which may include, but involves much more than, rendering an enforceable award.

To varying degrees, all arbitral institutions encourage the possibility of a result other than a final award and have incorporated explicit requirements for efficiency and economy in their arbitration rules:

- Article 26 of the DIS (German Institution of Arbitration) Rules provides: “Unless any party objects thereto, the arbitral tribunal shall, at every stage of the arbitration, seek to encourage an amicable settlement of the dispute or of individual disputed issues.” And Article 27 states: “The arbitral tribunal and the parties shall conduct the proceedings in a time- and cost-efficient manner. . . .”
- Article 17 of the UNCITRAL Arbitration Rules provides: “The arbitral tribunal. . . shall conduct the proceedings so as . . . to provide a fair and efficient process for resolving the parties’ dispute.”
- Article 22(1) of the ICC Arbitration Rules states: “The arbitral tribunal and the parties shall make every effort to conduct the arbitration in an expeditious and cost-effective manner”
- The introduction to the ICDR International Dispute Resolution Procedures states: “The ICDR Procedures reflect best international practices that are designed to deliver efficient, economic, and fair proceedings.”

So, when parties agree to have their cases arbitrated under these various rules, they have specifically demanded an efficient, economical dispute resolution process, regardless of whether the tribunal will ever issue a final award. Arbitrators and arbitral institutions need to go beyond lip service to economical and efficient dispute resolution and adjust – or perhaps overhaul – their procedures to make sure those goals are the primary focus.

Don't get me wrong, I am not suggesting that an arbitrator should actively take a mediator's role or that the tribunal should strongarm parties into settling. Rather, arbitrators and arbitral institutions need to modify arbitration procedures to put economy and efficiency first – providing opportunities for the parties to engage in productive settlement discussions throughout the process and incentivizing tribunals to foster early dispute resolution.

How do we do that? The key elements include:

- Maximize client (decision-maker) involvement from the beginning.
- Schedule an “early arbitration review” (with decision-makers present), which may set the stage for settlement discussions.
- Build a settlement discussion window into the schedule.
- Give arbitrators the tools and incentives to promote early dispute resolution.

From my experience as a litigator, mediator, and arbitrator, early settlements typically occur when decision-makers personally weigh costs and benefits, so their involvement is essential.

No mediator I know would consider conducting a mediation without the ultimate decision-makers in the room. There is a good reason for that. The decision-makers need to understand the case not only from their lawyers' perspective but from the other side's perspective and a neutral perspective. The decision-makers also need to get a glimpse of the process. Once they see the sausage being made, they will likely lose their taste for it.

Arbitration rules permit – or even encourage – client participation. For example, Article 24(4) of the ICC Rules allows the tribunal to “request the attendance at any case management conference of the parties in person or through an internal representative.” Nonetheless, arbitrators rarely use this essential tool.

Before beginning my point-by-point description of the procedures I am proposing, I should note that everything I am suggesting should be done with the recognition that ar-

bitration is a party-driven process. And arbitrators should not force or coerce the parties into procedures they do not want. But, that said, these procedures are within the letter and spirit of all major arbitration rules, and offering them to the parties is not just an option – it is an obligation.

Initial Case Management Conference – With Client Participation

Step One: The tribunal should strongly encourage client representatives (preferably the ultimate decision-makers) to participate in the initial case management conference. This will allow the clients to better understand the case and the procedure from the outset. It will give the tribunal the opportunity to convey the option of mediation or non-mediated settlement discussions directly to the parties. And if nothing else, the decision-makers will have a front-row seat to the discussions on how the arbitration will play out. In my experience, when clients are exposed to the minutia of arbitration procedures, they see not only the monetary expense but also the productivity cost – and case fatigue can begin to set in quickly.

At the initial case management conference, the tribunal should encourage the parties to incorporate into the schedule an early arbitration review, followed by a mediation window (or settlement discussion pause) – each discussed below.

Early Arbitration Review – With Client Participation

Before the initial case management conference, the parties will have provided the tribunal, and each other, with their pleadings or the equivalent. Soon after that conference, the parties should produce and provide to the tribunal the documents they plan to rely on at the hearing. Once the tribunal reads the pleadings and the reliance documents, it should have a good initial understanding of the case.

At this point, the tribunal should hold an early arbitration review, giving each party the opportunity to summarize its case and answer questions from the tribunal. This step is like what has become known as a Kaplan Opening, but with a few significant differences. Most importantly, I recommend client participation. I also propose holding the early arbitration review a bit earlier than a standard Kaplan Opening, which is sometimes referred to as a “mid-arbitration review.” In addition, I suggest that the tribunal structure the early arbitration review with a focus on setting the stage for – but not forcing – productive settlement discussions. And finally, unlike Kaplan's proposal, I suggest that the early arbitration review be followed by a pre-scheduled settlement discussion break, such as a mediation window (discussed below).

The tribunal should actively participate in the early arbitration review. The more questions the better. Tribunal questions are, of course, essential to educating the arbitrators, but

they will also focus the advocates' attention on the issues the arbitrators care about and could assist the parties in assessing their likelihood of success.

This procedure will yield multiple benefits: First, as I noted above, it should set the stage for productive settlement discussions. The lawyers, the tribunal, and most importantly, the clients will leave the early arbitration review with a much better understanding of the case. The lawyers and clients will also have a window into the tribunal's early views, based on their questions. And the clients will have another look at the internal workings of the sausage factory. All of this should encourage the parties to take a hard look at settlement.

Even if the early arbitration review does not result in productive settlement discussions, it provides multiple other benefits that should lead to a more efficient and economical dispute resolution. In sum, it will ensure that the tribunal is fully up to speed at an early stage, which will lead to more efficient and better decision-making as the case proceeds. And, through the arbitrators' questions, it will focus the lawyers' attention on the issues that are most important to the tribunal, providing a roadmap for a more streamlined case presentation.

Settlement Discussion Window

One of the biggest impediments to settlement is fear of perceived weakness. Neither side wants to broach the subject out of concern that the mere mention of the idea may damage its negotiating position. Arbitrators can – and should – provide a way for parties to avoid such a standoff. This can be achieved easily by the tribunal raising the idea of a settlement discussion window at the initial case management conference. If the tribunal treats a settlement discussion window as standard operating procedure, then neither side will need to worry about appearing weak by agreeing to it. And once the settlement discussion window is memorialized in the tribunal's procedural order, it will be automatic, so neither side will be inclined toward tactical hesitation.

Ideally, the settlement discussion window should immediately follow the early arbitration review. At that point in the proceedings, each side will have just heard a summary of the other side's case and the tribunal's questions to both sides. Assuming the decision-makers from each side participated in the early arbitration review, they will be well informed and should be able to rationally analyze the costs and benefits of settling versus arbitrating.

I am using the term "settlement discussion window" instead of "mediation window" because I believe the tribunal should try to incorporate a time for the parties discussing settlement into the schedule even in cases where the parties may not want to incur the cost of retaining a mediator. Nonetheless, the most productive settlement discussions

usually involve a mediator, so I suggest encouraging a "mediation window" and using a "settlement discussion window" as a fallback.

Assuming the parties elect to use a mediator, the next question is who will serve in that capacity? The parties may try to recruit the arbitrator or a member of the tribunal, assuming they can save time and money by using someone who is already familiar with the case. I suggest foreclosing that option at the outset. It is too fraught and, if the case does not settle, could result in a challenge to the award.

In sum, I recommend raising the idea of a settlement discussion window (or mediation window) at the initial case management conference, treating it as standard operating procedure, coupling it with the early arbitration review, and incorporating both into the tribunal's first procedural order.

Give Arbitrators the Tools and Incentives To Promote Early Dispute Resolution

The arbitration rules and guidelines of major arbitration institutions provide for a mediation option and expressly encourage arbitrators to shepherd the parties toward settlement. Nonetheless, arbitrators rarely incorporate the steps necessary to encourage settlement into their procedures, so we need significant structural changes in terms of both education and incentives.

Arbitration institutions must implement policies to ensure that arbitrators use all available tools to set the stage for productive settlement discussions. The institutions should educate arbitrators on their overarching obligation to resolve disputes in the most efficient and economical way. They need to provide arbitrators with procedural order templates that include things like early arbitration reviews and settlement discussion windows. And perhaps most important, they should modify their fee structures to incentivize – or at least minimize disincentivizing – early dispute resolution.

Although arbitrators routinely put their own interests behind those of the parties, the arbitration institutions, and the arbitral process, it is still an undeniable fact that the compensation structures of most arbitration institutions create a financial disincentive for early dispute resolution. And we need to at least consider the possibility that those existing structures may be hindering adoption of early dispute resolution methods.

I am not suggesting that arbitrators are consciously prolonging arbitrations to benefit themselves. But I am suggesting that arbitration institutions, like any efficiently run business, should align their financial incentives with their goals. And since their primary goal should be efficient, economical dispute resolution, it would benefit both the parties and the

arbitrators to financially incentivize that result to the extent possible and practical.

In a system that is largely billed by the hour, it is difficult to incentivize efficiency, and I do not have a silver bullet solution, but a non-hourly compensation system like the one used by the ICC could hold the answer if properly applied. The current ICC Rules include enough flexibility to incentivize efficient early dispute resolution. Article 2(2) of Appendix III to the ICC Rules provides that “[i]n setting the arbitrator’s fees, the [ICC] Court [of Arbitration] shall take into consideration the diligence and efficiency of the arbitrator, the time spent, the rapidity of the proceedings, [and] the complexity of the dispute,” among other things. Unfortunately, even with that flexibility, the ICC rarely compensates arbitrators in a way that puts an appropriate value on a quick, efficient resolution.

Another possibility would be for arbitration institutions to follow the lead of law firms – which routinely front-end load their compensation. When taking on a new case, many law firms will require a recoupable-but-non-refundable retainer payment. The retainer payment addresses the fact that the firm incurs significant transaction costs when initiating a new representation. Among other things, the firm must clear conflicts, and the attorneys who will be working on the new matter must allocate time on their schedules. As a result of both, the firm might lose work from other clients, so it is only fair that a chunk of the firm’s compensation is paid up front. Moreover, if the matter is resolved quickly, everybody

wins: the client avoids the cost of a prolonged dispute, and the lawyers are compensated above their hourly rate.

All the above is also true for arbitrators, but the fee structures of most arbitration institutions include nothing akin to the front-end loading of a recoupable-but-non-refundable retainer payment for arbitrators.

Different institutions may choose different procedures, but the bottom line is that arbitration institutions need to revamp their rules – including their compensation structures – to put the proper focus on efficiency and economy.

Conclusion

To summarize, encouraging client involvement, holding an early arbitration review, scheduling a settlement discussion window, and incentivizing arbitrators to promote settlement are key to arriving at a just and enforceable *result*. But tribunals must also use all available cost-saving tools, like bifurcation, dispositive motions, streamlined procedures (like having the chair alone oversee all issues that arise between the initial case management conference and the evidentiary hearing), and emerging technologies. Bottom line: economy and efficiency should be the overarching consideration in every decision the tribunal makes. If arbitrators focus solely on their mandate to issue an enforceable award, they run the risk of overlooking the broader goals of arbitration. By adhering to the principles already enshrined in institutional rules and employing the procedures discussed here, arbitrators can conduct proceedings in a way that will serve the parties’ fundamental aims. After all, it’s the result that matters.

Usher Winslett has been an ADR professional since 1996, handling more than 140 international and domestic disputes as an arbitrator or mediator of commercial, intellectual property, employment, insurance, and entertainment claims. He is based in New York and South Carolina but works internationally and remotely.

DATA PROTECTION AND CYBERSECURITY CONSIDERATIONS FOR CANADIAN ARBITRATION PROFESSIONALS

*Kathleen Paisley **

International arbitration as practiced today is largely a digitalized process. Documents are exchanged virtually, whether through email or by way of digital platforms, and hearings and case management conferences are increasingly held remotely. This trend has been greatly amplified by the COVID-19 pandemic, which created a need to move swiftly to on-line platforms not only for the exchange of documents but for all aspects of the proceedings including merits hearings. The agility that was displayed by everyone from counsel to arbitrators to institutions is a testament to the flexibility of international arbitration as a dispute resolution mechanism.

The wide-spread use of technology has brought wide spread benefits to international arbitration in terms of time, cost, and other efficiencies, as well as reducing the impact on the environment. However, while technology certainly acts as a great facilitator of international arbitration, it also poses constraints on the process, including those related to data security and associated regulations. While these risks and regulations are not unique to arbitration, it is important that they be addressed and managed during international arbitration proceedings.

* Kathleen Paisley is an international arbitrator based in the US and Europe with significant experience in commercial and investor-State arbitration under all the major arbitration rules; she is triple qualified in law (Yale Law School), finance (MBA), and has passed the certified public accountancy exam (CPA); an expert in technology, life sciences, data protection and cybersecurity, she is co-chair of the ICCA-IBA Joint Task Force on Data Protection in International Arbitration, which authored the ICCA-IBA Roadmap to Data Protection In International Arbitration, and is a member of the ICCA-NYC Bar-CPR Working Group on Cybersecurity in Arbitration, which developed the Cybersecurity Protocol for International Arbitration.

For arbitration professionals based in Canada, the first consideration in terms of how data protection and cybersecurity requirements may apply to you is the Canadian *Personal Information Protection and Electronic Documents Act* (“*PIPEDA*”), which applies to organizations that collect, use, or disclose personal information in the course of commercial activities in Canada.¹ This encompasses arbitrations to the extent the activities being undertaken are considered commercial, which includes lawyers and likely arbitrators in their daily practice.²

Many of the *PIPEDA* requirements find their genesis in the European Union (“EU”)³ Data Protection Directive, which has now been replaced by the *General Data Protection Regulation* (“*GDPR*”).⁴ Since its entry into force in 2018, the application of the *GDPR* to international arbitration proceedings has been the

¹ *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]. As discussed in footnote 9, this law is currently in the process of being amended, which may provide an opportunity for arbitration professionals to clarify the application of the Canadian data protection laws to international arbitration.

² *Ibid*, s 4 (1).

³ This article refers throughout to the “EU”, but the scope of application of the *General Data Protection Regulation* actually extends to the European Economic Area (“EEA”), which includes the 27 EU Member States plus Iceland, Liechtenstein, and Norway. Since the United Kingdom’s withdrawal from the EU, the applicable data protection laws in the UK are the *Data Protection Act 2018* [UK DPA 2018], and the UK *General Data Protection Regulation* [UK GDPR].

⁴ EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, OJ L 119, 4.5.2016, [2016] OJ, L 119 [GDPR]. OneTrust DataGuidance and Edwards, Kenny & Bray LLP have published an excellent comparison of the *PIPEDA* and the *GDPR*, see OneTrust DataGuidance & Edwards, Kenny & Bray LLP, “Comparing Privacy Laws: *GDPR* v. *PIPEDA*”, online (pdf): *OneTrust DataGuidance* <www.dataguidance.com/sites/default/files/GDPR_v_PIPEDA.pdf>.

source of debate and some confusion. As non-compliance with the *GDPR* may trigger civil and/or criminal liability, including potential fines up to 4% of global gross revenue or 20 million Euros, whichever is higher. It is therefore important for arbitration professionals to consider the extent to which the *GDPR* applies to proceedings in which they are involved and, if so, what efforts should be taken to comply.

The *GDPR* is mandatory and there is no arbitration exception. However, while the *GDPR* applies to arbitration in principle, it says nothing about the means by which it should be applied to arbitration. The same is true of the *PIPEDA*, the UK DPA 2018, the UK *GDPR*, and most other data protection laws that may apply to international arbitration. Arbitration professionals subject to the data protection laws are therefore left to decide what data protection compliance requires in their cases, keeping in mind that even if one participant in an arbitration is subject to the *GDPR* or *PIPEDA*, this may impact the conduct of the arbitration as a whole.

Importantly, for those subject to the *PIPEDA*, compliance with the *PIPEDA* allows data to transfer freely to and from the EU, which is a significant competitive advantage for Canadian-based arbitration professionals when undertaking cases where the data processing is subject to the *GDPR*.

As explained in more detail below, the EU has recognized only fourteen countries, including Canada when the *PIPEDA* applies, as having data protection regimes that are equivalent to the *GDPR* such that personal data can transfer freely.⁵ As a result, when a Canadian arbitration professional is involved in a case with EU-based participants, data can be exchanged with

⁵ The European Union considers that the data protection laws of Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom, United States (Privacy Shield only) and Uruguay are adequate. At the time of writing, South Korea is in the process of adequacy discussions as part of its trade deal with the European Union.

him or her without concerns being raised about *GDPR* compliance. The same is not true for arbitrators based, for example, in the United States. This means that when EU-based parties are considering appointing arbitrators, those based in Canada would not pose data protection challenges during the arbitration in the way that arbitrators from countries that are not considered adequate may. However, this advantage comes at the price of *PIPEDA* compliance.

The importance of data protection to international arbitration led the International Council for Commercial Arbitration (“ICCA”) and the International Bar Association Arbitration Committee to create a guide to these issues, which is now being finalized. The ICCA-IBA Roadmap to Data Protection in International Arbitration and its annexes seek to identify the data protection issues that may arise before, during, and after international arbitration proceedings, as well as the solutions that may be adopted to address them (“Draft ICCA-IBA Roadmap” or “Roadmap”).⁶ The Roadmap is not focused on a single data protection regime, but rather looks generally at the data protection rules applicable to arbitrations when a data protection regime built on the European principles (like *PIPEDA*) applies, regimes which are referred to here as “EU-based”. The Roadmap includes examples and practice tips, and is accompanied by a set of annexes that provide greater detail, practical information, and checklists, as well as samples of data protection notices and a data protection protocol.

While the Roadmap will be the best guide to how data protection principles impact international arbitration proceedings, the purpose of this article is to synthesize that advice for Canadian arbitration professionals about when the data protection laws may apply to them and their cases and

⁶ “The ICCA-IBA Roadmap to Data Protection In International Arbitration (Public Consultation Draft)”, online (pdf): *International Council for Commercial Arbitration* <www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf> [“Draft ICCA-IBA Roadmap”].

what this means in practice, taking *PIPEDA* into consideration. While the Roadmap is still in draft form and cannot be cited specifically for its content, reference is made generally to the Draft Roadmap where it would be applicable when finalized.

This article is set out in three Parts, as follows:

- Part 1 describes *PIPEDA*'s scope of application to arbitration professionals;
- Part 2 sets out the various ways in which data protection laws may apply to arbitration proceedings; and
- Part 3, the bulk of this article, explains the considerations that arbitration professionals should keep in mind in order to comply with data protection laws and how those rules may apply in the context of an arbitration proceeding with a focus on Canada.

This article draws examples from the *GDPR* because of its wide-ranging application and from the *PIPEDA* because of its importance to arbitration professionals based in Canada. For the convenience of readers, the *PIPEDA*'s list of "Fair Information Principles" and the text of the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration are included as annexes.

An important word of caution before proceeding: this article is not intended to provide legal advice about compliance with *PIPEDA*, the *GDPR*, or any other specific law, but rather to give arbitration professionals a general understanding of the issues and how they may impact their practices and cases. If an arbitration professional has questions about the application of the data protection laws to them, they should seek legal advice.

I. WHEN DOES *PIPEDA* APPLY TO ARBITRATION PROFESSIONALS?

The nature of arbitration is such that significant amounts of personal data, sometimes including sensitive and criminal data,

is exchanged, often across borders. Such data exchanges and transfers are essential for the international arbitration process to function; however, they should be lawful under the applicable data protection laws and procedures put in place to ensure compliance with those laws throughout the proceedings.

The application of the *GDPR* to international arbitration has been the subject of significant discussion and publications, but the potential application of *PIPEDA* to international arbitration has thus far escaped scrutiny.⁷

PIPEDA is the Canadian federal data protection law. Adopted almost 20 years before the *GDPR*, it follows the principles established in the previous EU Data Protection Directive,⁸ which was also the basis for the *GDPR*. Although *PIPEDA* does not apply to certain commercial activities undertaken solely within certain Canadian provinces, it applies to interprovincial or international transfers of personal information and hence is potentially applicable to international arbitration.

It is important to recognise that *PIPEDA* is currently under review and may be replaced with new legislation that is intended to better address the current digital reality.⁹ These

⁷ See e.g., “Draft ICCA-IBA Roadmap”; Clara-Ann Gordon, “The Impact of *GDPR* on International Arbitration—A Practical Guideline” (2019) 74:4 *Disp Resol J* 27; David Rosenthal, “Complying with the *General Data Protection Regulation (GDPR)* in International Arbitration—Practical Guidance” (2019) 37:4 *ASA Bull* 822; Kathleen Paisley, “It’s All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration” (2018) 41:4 *Fordham Intl LJ* 840.

⁸ EC, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] OJ, L 281/31 [*Data Protection Directive*].

⁹ As a result of ongoing developments in technology, the Government of Canada introduced Bill C-11, or the *Digital Charter Implementation Act, 2020 [Act]*, on November 17, 2020. If adopted, the *Act* would replace the privacy component of the *Personal Information Protection and Electronic Documents*

amendments may affect PIPEDA's application to arbitration, which is not addressed in this Article. Further, this amendment process provides a potential opportunity for the Canadian arbitration community to clarify the application of the Canadian data protection laws to international arbitrations.

The Canadian courts and the Office of the Privacy Commissioner of Canada ("OPC") have stated that *PIPEDA* has quasi-constitutional status.¹⁰ At the same time, like the *GDPR*, *PIPEDA* seeks to balance the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use, or disclose personal information in the course of carrying out their business.¹¹

PIPEDA requires organizations to comply with a set of "Fair Information Principles" which are the foundation of Canadian personal information protection law. They require the following:

- Accountability
- Identifying purposes
- Consent

Act [*PIPEDA*] with the *Consumer Privacy Protection Act* [*CPPA*] and the *Personal Information and Data Protection Tribunal Act* [*PIPD*T].

¹⁰ See *Joint investigation of Clearview AI, Inc by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, PIPEDA Report of Findings #2021-001*, 2 February 2021, at para 61, citing e.g. *Nammo v Transunion of Canada Inc*, 2010 FC 1284 at paras 74—75; *Bertucci v Royal Bank of Canada*, 2016 FC 332 at para 34; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at paras 19, 22; *Cash Converters Canada Inc v Oshawa (City)*, 2007 ONCA 502 at para 29, citing *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, and *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403.

¹¹ *Englander v Telus Communications Inc*, 2004 FCA 387.

- Limiting collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance¹²

Organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances, and only in line with the Fair Information Principles.¹³ Annex 1 of this article provides a brief overview of these principles.

The OPC is responsible for overseeing compliance with *PIPEDA*. It has published a guide entitled “*PIPEDA* and Your Legal Practice – A Privacy Handbook for Lawyers”,¹⁴ which is now more than ten years old but remains a useful resource. The OPC Handbook provides an overview of how these principles could apply in the litigation context, which, although not arbitration-specific, provides useful guidance for arbitration professionals subject to *PIPEDA*.

The OPC takes the view that *PIPEDA* applies to legal professionals to the extent their work constitutes “commercial activity”. As explained more fully below, this is likely to include lawyers’ day-to-day operations and case work that is considered

¹² *PIPEDA*, Schedule 1.

¹³ *PIPEDA*, s 5(3).

¹⁴ *PIPEDA and Your Legal Practice - A Privacy Handbook for Lawyers*, online: Office of the Privacy Commissioner of Canada <www.priv.gc.ca/en/privacy-topics/business-privacy/gd_phl_201106/> [*Handbook for Lawyers*].

to be commercial. The extent to which this definition applies to investor-state cases is unclear, and is beyond the scope of this article.

PIPEDA applies to all to “organizations” that collect, use, or disclose personal information in the course of “commercial activities.”¹⁵ *PIPEDA* defines the term “organization” to include associations, partnerships, persons, and trade unions.¹⁶ Further, the OPC has indicated that professionals engaged in commercial activities, including lawyers, are likely covered by *PIPEDA*. Hence, arbitration professionals would likely be considered to be “organizations” for purposes of the law and *PIPEDA* would be applicable to them to extent the particular activities being undertaken are considered commercial.

PIPEDA defines “commercial activity” as any “transaction, act, or conduct or any regular course of conduct that is of a commercial character.”¹⁷ Under this standard, law firms have been found to be engaged in commercial activities in their day-to-day operations when they perform services for their commercial clients.¹⁸

However, not all personal information that an organization, including an arbitration professional, collects, uses, and discloses is subject to *PIPEDA*. Rather, for *PIPEDA* to apply, it must be collected, used, or disclosed in the course of “commercial activity.”

¹⁵ *PIPEDA*, s 4(1).

¹⁶ *PIPEDA*, s 2(1).

¹⁷ *PIPEDA*, s 2(1).

¹⁸ For example, under this standard, law firms have been found to be engaged in a commercial activity when they undertake credit checks on potential clients, and the obligations with respect to good record keeping and a client’s right of access to their personal information have been found to apply to lawyers unless an exception applies.

This raises the question whether or which activities undertaken by arbitration professionals during arbitration proceeding are commercial activities. The OPC recently considered the application of *PIPEDA* to an insurance company's internal ombudsman office and its decision gives useful insight to the approach that may well be taken to *PIPEDA*'s application to commercial arbitration ("*Insurance Ombudsman Decision*"). Based on the reasoning of that decision, the OPC is likely to take the view that commercial arbitration is covered by *PIPEDA*.

Subsection 2(1) of *PIPEDA* defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

In deciding whether *PIPEDA* applied to the *Insurance Ombudsman Decision*, the OPC referred to the decision of the Federal Court of Canada in *State Farm*.¹⁹ The court applied a narrow interpretation of "commercial activity" and found that personal information collected by an insurer for the purpose of defending a claim against its insured was not subject to *PIPEDA*, even though the information was collected before any claim had been commenced. The case involved an automobile accident between a complainant and a woman insured by State Farm who, in anticipation of potential litigation, hired private investigators to conduct surveillance on the complainant.

In deciding that *PIPEDA* did not apply, the court stated the following:

The primary characterization of the activity or conduct in issue is the dominant factor in assessing the commercial character of that activity or conduct under [the Act], not the

¹⁹ *State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada*, 2010 FC 736 [*State Farm*].

incidental relationship between the one who seeks to carry out the activity or conduct and third parties.²⁰

Applying that test in its *Insurance Ombudsman Decision*, the OPC looked to the dominant purpose for the information being collected or generated in the course of the Ombudsman dispute resolution process. Since the data collection arose out of commercial activity between the complainant and the respondent, the OPC reasoned that *PIPEDA* would apply “on account of the commercial activity between the complainant and the Respondent, the ensuing relationship between the complainant and the Ombudsman falls under the scope of the Act.”²¹ Under the reasoning, commercial arbitration cases brought under arbitration agreements between commercial actors would be considered commercial activities covered by *PIPEDA*.

In deciding that the ombudsman proceeding was covered by *PIPEDA*, the OPC also considered the fact that *PIPEDA* contains an express exemption to the right of access for information gathered in the context of formal dispute resolution procedures. The OPC noted that “the very presence of ... an exemption to provide an individual with access to personal information under the Act indicates that information relating to a formal dispute resolution process is capable of falling under the Act.”²²

The OPC’s reasoning in the *Insurance Ombudsman Decision* is consistent with the approach taken in the Handbook for Lawyers, published five years earlier, which states “For example, the collection, use or disclosure of personal

²⁰ *Ibid* at para 106.

²¹ *An insurance company’s internal ombudsman office is not a “formal dispute resolution process” under PIPEDA*, *PIPEDA Report of Findings #2021-001* (Ottawa: Office of the Privacy Commissioner of Canada, 2021) [*Insurance Ombudsman Decision*].

²² *Ibid*.

information in connection with litigation involving commercial organizations may well be carried out in the course of commercial activities, as distinguished from a personal injury claim involving individual litigants in their personal capacity.”²³ For this reason, the collection, use, or disclosure of information carried out in connection with arbitrations of commercial disputes, and perhaps all arbitrations involving commercial parties, may be covered by *PIPEDA*.

Therefore, arbitration professionals based in Canada should consider whether *PIPEDA* may apply to them and the arbitrations in which they are involved, and what this requires in practice.

The remainder of this article is based on the premise that arbitration professionals will generally be considered to be covered by the *GDPR* or *PIPEDA*, such that the data protection rules apply to them during arbitration proceedings. This creates obligations, but also potential benefits because, if *PIPEDA* applies to one arbitration professional during an arbitration while other participants in the same arbitration are subject to the *GDPR*, this allows the free flow of information among them, effectively equating *PIPEDA* compliance with *GDPR* compliance for all practical purposes. As a result, it is easier to include Canadian arbitration professionals in cases where the *GDPR* applies.

²³ *Handbook for Lawyers*, *supra* note 14.

II. WHEN DO THE DATA PROTECTION LAWS APPLY DURING ARBITRATION PROCEEDINGS?

1. *Coverage of Data Protection Laws*

The GDPR and other EU-based data protection laws apply whenever: “personal data”²⁴ about a “data subject”²⁵ is “processed”²⁶ during activities falling within their jurisdictional scope. These concepts are broadly defined, and cover most information exchanged during an arbitration.

a. Personal Data of Data Subjects

Most of the information exchanged during a typical international arbitration contains personal data. Personal data is defined in the *GDPR* as “any information relating to an identified or identifiable natural person” or “data subject”.²⁷

²⁴ “Personal data” means any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. See *GDPR*, art 4(1).

²⁵ “Data subject” means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. See *GDPR*, art 4(1).

²⁶ “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. See *GDPR*, art 4(2).

²⁷ *GDPR*, art 4(1).

PIPEDA refers to information about an “identifiable individual.”²⁸

Under many laws, including the *GDPR*, it is irrelevant that the personal data is contained in a business-related document, such as work files, work emails, laboratory notebooks, agreements, construction logs, etc. Provided that the data relates to an individual who is identified or identifiable, it is considered to be personal data, and the individual to whom it relates is a data subject with rights.

Only the individuals who are identified or identifiable are referred to as “data subjects”; legal entities cannot be data subjects.²⁹ In the context of arbitration, the data subjects are the individuals mentioned in the evidence—the witnesses, the lawyers, etc.—which in a major arbitration can be hundreds of people, each of whom has rights under the data protection laws that cannot be waived by the parties. The *GDPR* applies stricter rules to sensitive personal data,³⁰ also referred to as “special category data,” and largely prohibits the processing of criminal offence data without license.

b. Processing

EU-based data protection laws apply whenever personal data is “processed”. Processing includes not only active steps

²⁸ *PIPEDA*, s 2(1).

²⁹ See *GDPR*, recital 14.

³⁰ The *GDPR* refers to “special category data”, more commonly referred to as “sensitive data”, which is defined as data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation. The processing of special category data is allowed, among other reasons, where necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity. See *GDPR*, arts 9(1), 9(2)(f).

such as collecting, using, disseminating, and deleting data, but also passive operations such as receiving, holding, organizing, and storing data.³¹ Most activities undertaken in an international arbitration constitute processing.

2. Jurisdictional Scope of Data Protection Laws

The jurisdictional scope of EU-based data protection laws is broad, and they often apply extraterritorially. For example, the *GDPR* applies whenever personal data is processed:

- in the context of the activities of an establishment of a controller or a processor in the EU³² or
- where the processing activities are related to the offering (targeting) of goods or services to individuals *in* the EU (regardless of their residence or citizenship).³³

a. Data Processing in the Context of an EU Establishment

The *GDPR* applies to data processing by arbitration professionals when they have an EU establishment and the data processing takes place in the “context of the activities” of that establishment, wherever in the world the data processing occurs. The concept of “establishment” is defined broadly to include activities undertaken in the EU through “stable arrangements”, regardless of the legal form those arrangements take.³⁴

³¹ See *Ibid*, art 4(2).

³² *GDPR*, art 3(1).

³³ *Ibid*, art 3(2)(a).

³⁴ See “European Data Protection Board Guidelines 3/2018 on the Territorial Scope of the *GDPR* (Article 3), Version 2.1” (12 November 2019), online (pdf): *European Data Protection Board* <edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf> [“Territorial Guidelines”]

Applying these criteria, arbitration professionals based outside the EU, including in Canada, should consider whether they undertake activities in the EU through stable arrangements and, if so, whether the data processing activities at issue are being carried out in the “context” of those activities. If the answer to both questions is affirmative, those data processing activities are likely to be covered by the *GDPR*.³⁵

This determination will not always be straightforward. For example, when arbitrators based in Canada have of counsel or tenancy arrangements with firms or chambers within the EU, such arrangements would likely qualify as stable arrangements, and those arbitrators will then need to consider whether the data processing is being undertaken in the context of the activities of their chambers in the EU. In the case of London-based barristers’ chambers, with the UK’s departure from the EU the question would be whether the Data Protection Act 2018 and the UK *GDPR* applies; but for our purposes, the rules are generally the same (at least for now).

b. Data Processing Related to the Targeting Data Subjects Based in the EU

Even where the processing does not take place in the context of an EU establishment, the *GDPR* also applies “where processing activities are related to the offering of goods or services to such data subjects in the EU”. This is also referred to as “targeting.” This language appears to be geared at the

(“[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect”).

³⁵ *Ibid* (“determining whether processing is being carried out in the context of an establishment of the controller or processor in the Union for the purposes of Article 3(1) should be carried out on a case-by-case basis and based on an analysis in *concreto*” at 7).

targeting of individual consumers but could be applied more broadly.

When acting in a professional capacity, arbitration professionals typically do not target individual consumers, but rather other arbitration professionals and parties (typically companies). It is not clear whether these sorts of contacts trigger the application of the *GDPR*, but the fact that an individual is acting in a professional capacity does not prevent the application of the *GDPR* to him or her.³⁶

Many EU-based data protection laws have similar jurisdictional requirements, but *PIPEDA* is silent on its extraterritorial application, although this is one of the issues under consideration for amendment.³⁷

Under *PIPEDA*, the Federal Court of Canada has held that when a Canadians' personal information is collected, used, or disclosed from outside of the territory of Canada, *PIPEDA* will apply to the processing of personal information by an organization where there exists a "real and substantial connection" to Canada.³⁸ This standard applies to both domestic and foreign entities, and has been interpreted to the effect that

³⁶ *Supra* note 34. The "Territorial Guidelines" do not specifically address whether the *GDPR* applies to targeting outside of individual consumers, however, the guidelines contain numerous examples, all of which relate to the targeting of individual consumers, not in a professional context. This could imply that when data processing activities do not take place in the context of an EU establishment, the *GDPR* only applies when consumers are targeted, but it is not clear.

³⁷ For an excellent overview of the extraterritorial application of *PIPEDA*, see Wendy J Wagner, Christopher Oates & Sarah Boucaud, "Canada's Piece Of The Regulatory Pie: Application Of Canadian Data Privacy Laws To A Local Data Processor With A Global Reach" (14 January 2020), online: *Mondaq* <www.mondaq.com/canada/privacy-protection/883314/canada39s-piece-of-the-regulatory-pie-application-of-canadian-data-privacy-laws-to-a-local-data-processor-with-a-global-reach>.

³⁸ See *Lawson v Accusearch Inc (cob Abika.com)*, 2007 FC 125 at paras 38—43.

a foreign entity collecting personal information about an individual in Canada must comply with *PIPEDA*.

Also of potential importance to arbitration, the OPC recently issued a report in the AggregateIQ Data Services, Ltd. (“AIQ”) investigation finding, which held that an organization based in Canada (which would include arbitration professionals as discussed above) is required to apply Canadian data protection laws to data that is collected abroad and transferred to Canada for processing.³⁹ The report finds that *PIPEDA* applies to data processors and service providers who use and disclose personal information, regardless of the jurisdiction in which that information was collected, stating as follows:

Even where the information was collected in a different jurisdiction, whether that be the United Kingdom or the United States, AIQ is still required to meet its obligations under Canadian law with respect to its handling of that personal information in Canada. [9]

If this reasoning would be applied to international arbitration, these cases stand for the proposition that: *PIPEDA* would apply to arbitrational professionals based outside Canada that process Canadians’ personal information where there exists a “real and substantial connection” to Canada. Further, arbitration professionals based in Canada are subject to *PIPEDA* whenever they process personal data in Canada during an international arbitration, regardless of where the data was collected or whether it relates to a Canadian but this would not necessarily apply where Canadians process data abroad, for example, in the UK or Hong Kong.

³⁹ *Investigation Report P19-03/PIPEDA-035913: AggregateIQ Data Services, Ltd.*, 26 November 2019, online (pdf): *Office of the Information & Privacy Commissioner For British Columbia* <www.oipc.bc.ca/investigation-reports/2363> [AIQ Investigation].

III. WHAT DOES DATA PROTECTION COMPLIANCE REQUIRE FOR ARBITRATION PROFESSIONALS?

What does it mean when the data protection laws apply to you as an arbitration professional? This section will explain what data protection obligations may apply to arbitration professionals in the context of their practice, generally, and during the arbitral process. Again, it is not intended to be specific advice, but simply an overview.

If *PIPEDA*, the *GDPR*, the UK *Data Protection Act*, the UK *GDPR*, or another EU-based data protection law applies to you as an arbitration professional, it will be important for you to consider the impact this has on your practice and any cases in which you are involved. These laws usually will not apply to the case as a whole but rather to specific data processing activities depending on when, where, and by whom they are undertaken.

On a practical level this means that you will be required to comply with the data protection laws alongside the applicable arbitration law, rules, and any rules of evidence such as the IBA Rules on the Taking of Evidence, where they are applied. Furthermore, where the *GDPR* or *PIPEDA* applies, the doctrine of accountability requires those who process personal data subject to those laws to document the approach and measures they have taken towards compliance, which is important to demonstrate good faith efforts to comply should a dispute later arise.

1. *What obligations may apply to arbitration professionals?*

The data protection laws create a set of rules to protect the processing of personal data/information as well as stricter rules that apply to sensitive or special category data. The scope of these obligations depends on the applicable law and the arbitration professional's status under that law.

a. GDPR

Under the *GDPR*, the extent of the obligations depends on whether you are considered to be a data controller, a joint controller, or a data processor, each of which can be either a natural or legal person. Data controllers and joint controllers are primarily responsible for compliance and demonstrating compliance, whereas data processors, who process data on behalf of a controller, have more limited responsibility.

Controller: A data controller determines “the purposes and means of the processing of personal data” (see, e.g. *GDPR* Art. 4(7)). As discussed in the Draft Roadmap, applying this definition, during the course of an arbitration most participants are likely to be considered data controllers because the nature of their function is such that they control the purpose and means of the data they are processing in the context of an arbitration. Both barristers⁴⁰ and solicitors⁴¹ are considered to be data controllers by relevant data protection authorities in the EU and the UK.

⁴⁰ Article 29 Data Protection Working Party, “Opinion 1/2010 on the Concepts of “Controller” and “Processor”” (16 February 2010) (“A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client’s case. The legal ground for making use of the necessary information is the client’s mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as an independent ‘controllers’ when processing data in the course of legally representing their client” at 29) [emphasis added].

⁴¹ The ICO is the UK Information Commissioner’s Office, which applies the UK *DPA 2018* and the UK *GDPR*. The ICO has taken the view that solicitors are data controllers. *Ibid* at 29; ICO, “Data controllers and data processors: what the difference is and what the governance implications are, *Data Protection Act 1998*” (2014) at paras 40—43; Article 29 Data Protection Working Party, “Opinion 1/2010 on the Concepts of “Controller” and “Processor””, (00264/10/EN WP 169, 2010).

Joint Controller: The *GDPR* has introduced the concept of joint controllers who jointly determine the purposes and means of the data processing.⁴² Where the *GDPR* applies, each of the joint controllers is responsible for compliance with the *GDPR* and the joint controllers are jointly and severally liable for any data protection violation. They are required to make arrangements to allocate the risks involved, for example through a data protection protocol. However, the liability of a joint controller is limited to the processing for which that controller determines the purposes and means of the processing and does not extend to the overall chain of processing for which it does not determine the purposes and means, but this line can be difficult to draw in practice.⁴³

In the context of an arbitration proceeding, distinguishing between (i) controllers, who are likely to be acting alongside other controllers with parallel responsibilities, or (ii) joint controllers acting jointly, may be difficult, and caution is warranted in light of recent decisions of the European Court of Justice (“CJEU”) under the Data Protection Directive indicating that the notion of joint controllership is broadly interpreted. This emphasizes the importance of data protection compliance by all those involved in international arbitration proceedings.

Data processors: Data processors have more limited responsibilities under the *GDPR*. However, they must act under the instruction of a data controller in undertaking their tasks and cannot be responsible for deciding the purposes and means of the data processing and furthermore must be retained under a *GDPR*-compliant data processing agreement allowing the data controller to direct the processing and stop it at any time. This

⁴² *GDPR* Art. 26(1).

⁴³ See “Judgment of 29 July 2019”, *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629 at paras 74, 85. See also “Judgment of 5 June 2018”, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388; “Judgment of 10 July 2018”, *Jehovan todistajat*, C-25/17, EU:C:2018:551.

makes it unlikely that counsel, experts, arbitrators or institutions can be considered to be merely data processors during an arbitration because their function requires them to decide the purposes and means of the processing of personal data. However, depending on the context, tribunal secretaries, e-discovery professionals, transcribers, interpreters, and other vendors, may be considered data processors.

b. PIPEDA

PIPEDA does distinguish between data controllers, joint controllers, and data processors. Rather, as described above, *PIPEDA* applies equally to all organizations that collect, use or disclose personal information in the course of commercial activities.⁴⁴

2. What does this mean in practice?

The *GDPR* applies generally to the processing of personal data, special category data, and, in the case of *PIPEDA*, in a commercial context. Special rules apply to certain types of special category data including highly sensitive data like medical records. However, there are no special rules for the processing of personal data depending on the context—the rules are generic and it is up to each person to apply them.

Arbitration is no different. The data protection laws apply to the processing of personal data by arbitration professionals in their general practice, in preparing for cases, and during the arbitral process. But there are no specific regulations applying to arbitration. This means that in any given arbitration there will be multiple data controllers, organizations, and others bound by different data protection laws in relation to the same personal data, each of whom has individual responsibility, liability, and potentially joint liability to ensure the protection of that personal data.

⁴⁴ *PIPEDA*, s 4 (1).

In considering what is required, generally speaking, the data protection laws require the issuance of data privacy notices, adopting appropriate data security measures and data breach procedures, ensuring that personal data processing and transfers are permissible under the law, minimizing personal data processing, putting in place data retention policies, and establishing procedures for addressing data subject complaints.⁴⁵

a. Data Privacy Notices

Arbitration professionals subject to EU-based data protection laws are typically required to notify the data subjects about whom they process personal data of their data processing activities, which are referred to as “policies” under *PIPEDA*, rather than “notices.” These notices or policies should be in plain language and the applicable statutes and regulations will describe what should be covered.⁴⁶

All arbitration professionals should consider whether they are required to publish a general data privacy notice. Furthermore, in specific arbitrations with processing that is covered by the data protection laws like *PIPEDA* and the *GDPR*, the question arises as to how data subjects will be notified and by whom. In the case of a confidential arbitration, providing such notices could compromise the confidentiality of the arbitration.

It is also important to recall that data subjects include everyone who is identified or identifiable from the evidence and the pleadings, regardless of whether they have any relationship

⁴⁵ The Draft ICCA-IBA Roadmap provides a checklist of data protection issues that parties and their counsel may want to consider.

⁴⁶ See e.g. *GDPR*, arts 13—14. The Draft ICCA-IBA Roadmap provides in an annex examples of privacy notices for consideration by institutions, arbitrators, and legal counsel governed by the *GDPR*. This annex may be a starting point for arbitration professionals when deciding what to put in their privacy notices.

to the proceeding, and processing includes essentially everything that is done in arbitration cases. This means that, for many who lack a relationship with the data subject but will be processing their data, there may be no realistic means of providing notice.

In order to avoid overlapping notices, the *GDPR*, for example, provides exemptions from the notice requirements for data controllers who did not originally collect the data from the data subject, many of which will apply in arbitrations to those who did not directly collect data from individuals, like the arbitrators, an administering institution, and counsel.⁴⁷ However, even when those exemptions apply, it is important to determine whether someone has notified the data subject.

Therefore, arbitration professionals should consider whether they are subject to a notification requirement and, if so, to whom, as well as how the notification should be carried out without risking the integrity and confidentiality of the arbitration.

⁴⁷ Under the *GDPR*, when the data controller did not originally collect the personal data, as is often the case in international arbitrations, they are not required to provide notice where:

- The individual data subject already has the required information on the processing of his personal data;
- Providing information on the processing of personal data to the individual would be impossible;
- Providing such information to the individual would involve a disproportionate effort;
- Providing such information to the individual would render impossible or seriously impair the achievement of the objectives of the processing; or
- The data controller is subject to an obligation of professional secrecy regulated by EU or EU Member State law that covers the personal data.

See *GDPR*, art 14 (5), recital 62.

b. Data Security

When data protection laws such as *PIPEDA* and the *GDPR* apply to arbitrational professionals, appropriate data security measures are legally required.⁴⁸ However, those laws do not specify what security measures are required, but only that security measures must be “appropriate”. Deciding what security measures are appropriate requires consideration of the potential risk to the individual data subjects, which is defined in *PIPEDA* by reference to the “sensitivity” of the data.⁴⁹

Arbitration professionals subject to the data protection laws are required to apply appropriate security measures whenever they process personal data. Hence, these rules apply generally and in the context of specific cases.

The legal and arbitration community has published helpful guidance about cybersecurity, including the International Council for Commercial Arbitration (ICCA), the New York City Bar Association (NYC Bar) and the International Institute for Conflict Prevention (CPR): the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration.⁵⁰ The Protocol sets out 14 principles accompanied by explanatory commentary and examples, which provide guidance on establishing reasonable cybersecurity measures. These principles are set forth in Annex 2 of this article. Other guidance includes the International Bar Association Presidential Task Force’s Guidelines on Cyber Security and the ICC’s Note on Information Technology in

⁴⁸ See *GDPR*, art 32.

⁴⁹ *PIPEDA*, s 7.2(1)(a)

⁵⁰ “ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration” (2020), online (pdf): *International Council for Commercial Arbitration* <cdn.arbitration-icca.org/s3fs-public/document/media_document/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf>.

International Arbitration.⁵¹ While these initiatives do not address security requirements in the context of data protection specifically, they are useful resources for applying the appropriateness test in relation to information security and determining how information security may be addressed in international arbitrations.

As described in the Protocol and the Roadmap, applying information security standards in an arbitration will depend on many factors, including the nature of the organizations involved, (including number of employees, their premises and data systems), the individual's role in the arbitration, their existing information security measures, the type of processing being undertaken and whether external service providers have been employed. The degree of security required also depends on the types of data being processed, including how valuable, sensitive, or confidential they are and the damage or distress that may be caused to the data subject if personal or sensitive data were to be compromised.

Note that for data protection purposes, these issues are related to the individual data subject, rather than the parties. In other words, the fact that the data may be commercially sensitive does not impact the extent of security required for data protection compliance, but may be very important for general security obligations. Increasingly in international arbitration practice, these issues are being addressed through the use of

⁵¹ "International Bar Association's Presidential Task Force's Guidelines on Cyber Security" (October 2018), online (pdf): *International Bar Association* <www.ibanet.org/MediaHandler?id=2F9FA5D6-6E9D-413C-AF80-681BAFD300B0&.pdf&context=bWFzdGVyfGFzc2V0c3wxNTA4MzV8YXBwbGljYXRpb24vcGRmfGhlNC9oYWQvODc5NzA1MzM4Njc4Mi8yRjlGQTVENi02RTlELTQxM0MtQUY4MC02ODFCQUZEMzAwQjAucGRmfGNlZWmwNGQwZWw1ZjE1YmUxYTg1YjZjZDZjODVhMzUyN2YxNjg3ZjVlMzYwYzRjNWJkZjc3NzM4NmU2NzU2MTk>; "ICC's Note on Information Technology in International Arbitration", online (pdf): *International Chamber of Commerce* <iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf>.

secure platforms for the exchange of written submissions and evidence.⁵²

PIPEDA, for example, requires:⁵³

- All the personal data an organization collects must be maintained securely, including being protected from personal loss, unauthorized access, and data theft;⁵⁴
- The responsibility for protecting personal data lies with the organization (including arbitration professionals in possession of this data, which is required to designate someone to be accountable for *PIPEDA* compliance;⁵⁵
- Personal data must be protected by physical measures, organization measures, and technological measures, irrespective of the format in which it is held;⁵⁶ and
- Data secrecy must be maintained as, in accordance with the sensitivity of the data, the more sensitive the data, the higher the required protection.⁵⁷

⁵² The Working Group on LegalTech Adoption in International Arbitration has also recently released a protocol for online case management in international arbitration, see “Protocol for Online Case Management in International Arbitration”, online (pdf): *Latham & Watkins LLP* <www.lw.com/thoughtLeadership/protocol-online-case-management-international-arbitration>.

⁵³ For a helpful description of the applicable cybersecurity rules under *PIPEDA*, see Mitch Kocerginski, Lyndsay A Wasser & Carol Lyons, “Cybersecurity – The Legal Landscape in Canada”, *McMillan Cybersecurity Bulletin* (October 2017), online: <mcmillan.ca/insights/publications/cybersecurity-the-legal-landscape-in-canada/>.

⁵⁴ *PIPEDA*, Schedule 1, art 4.7.1.

⁵⁵ *Ibid*, art 4.1.

⁵⁶ *Ibid*, art 4.7.3.

⁵⁷ *Ibid*, art 4.7.

Article 32 of the *GDPR* is more specific, requiring that, when deciding what information security measures are appropriate, consideration must be given to the “state of the art”, implementation costs, data minimization, and the circumstances and risk level of the processing, with a focus on the risks to the data subject. The *GDPR* also provides that “appropriate” technical and organizational measures could include, as appropriate:

- The pseudonymization and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.⁵⁸

Furthermore, under the *GDPR*, account must be taken of the risks that are presented by the processing, in particular from:

- Accidental or unlawful destruction;
- Loss;
- Alteration; or
- Unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.⁵⁹

⁵⁸ *GDPR*, art 32(1).

⁵⁹ *GDPR*, art 32(2).

In the specific context of arbitration proceedings, as set forth in the Roadmap and the Protocol, the data security obligations of all participants are inter-linked, and a breach of security by one will have an impact on all. This means that all those involved in an arbitration should:

- Consider what information security measures they already have in place;
- Employ information security measures appropriate to the size and use of their network and information systems;
- Take into account the state of technological development (although the cost of implementation can also be a factor);
- Employ information security measures appropriate to their business practices, the nature of the personal data processed, and the harm that might result from any data breach;
- Undertake a risk analysis in deciding what information security measures to employ and document the findings; and
- Provide notice to those affected if information security measures in place fail to prevent a data breach.

c. Data Breach Notices

Most EU-based data protection laws, including *PIPEDA* and the *GDPR*, require notifications of data breaches. In addition to these legal reporting requirements, counsel and arbitrators' general duties to protect the integrity of the proceedings or their express ethical obligations may require notification to the parties of a data breach, taking into consideration the risk that notification of a minor data breach may significantly disrupt the process. Given the risks associated with data breaches not only

to data subjects but also to the orderly conduct of the proceedings, questions concerning when notifications should be made should be addressed in advance of any breach.

Organizations subject to *PIPEDA* are required to:

- report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of “significant harm” to individuals;
- notify affected individuals of any such breaches; and
- keep records of all breaches.⁶⁰

Under *PIPEDA*, the definition of “significant harm” includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business, or professional opportunities, financial loss, identity theft, negative effect on credit rating, and damage to or loss of property.⁶¹

The *GDPR* has similar notification requirements, which obligate data controllers to notify the supervisory authorities in case of a data breach that is “likely to result in a risk for the rights and freedoms of the data subject” within 72 hours of their discovery of the breach.⁶² The data subjects must also be notified of the breach if the data controller determines the risk to personal data be to be “high”.⁶³

This is a case-specific determination and, in the EU, for example, the burden to prove the absence of risk in a data

⁶⁰ Office of the Privacy Commissioner of Canada, “What you need to know about mandatory reporting of breaches of security safeguards”, online: <www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.

⁶¹ *PIPEDA*, s 10.1(7).

⁶² *GDPR*, arts 33—34.

⁶³ *Ibid*, art 34.

breach rests on the data controller.⁶⁴ Making this determination in the arbitration context requires consideration of the types of personal data being processed and the harm that could come to the individual data subjects (not the parties) from the incursion. It is therefore important to consider the nature of any personal, sensitive, and criminal offence data being processed and the harm that could befall the individual from its disclosure. It may be, for example, that notification is not required where the only personal data being processed for the arbitration is business email and other commercial correspondence and documentation, but this depends on the context and is highly specific. However, even where notification is not compulsory, a record of the breach must be kept.

If notification is required, *PIPEDA* and the *GDPR* both contain detailed provisions describing when the notification must be done, to whom, and what needs to be included. In the EU, for example, a data controller is considered to become aware of a breach when it has a “reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.”⁶⁵ A breach notification must include the cause, the nature of the breach (if known), and recommendations as to mitigation efforts to reduce the risks of the breach.

d. Lawful Data Processing

In most jurisdictions, including in the EU and Canada, all processing of personal data covered by data protection laws must have a lawful basis. In other word, there must be a lawful reason for the processing.

⁶⁴ *GDPR*, arts 33—34.

⁶⁵ Article 29 Data Protection Working Party, “Guidelines on Personal data breach notification under Regulation 2016/679” (3 October 2017) at 11 (last revised and adopted 6 February 2018).

There is no universal legal basis for lawful processing in the context of arbitration. Rather, the decision as to what data processing is lawful during an arbitration is fact-driven and case-specific. Depending on the circumstances of the case, the lawful bases may be different for different arbitral participants and for different types of personal data (e.g., witness data, data contained in the documentary evidence, sensitive data, criminal data). Lawfulness also requires that the personal data not be processed in a manner that is generally unlawful (for example in breach of confidentiality obligations).

The legal requirements for data processing can generally be met by obtaining the consent of a data subject. Under the *GDPR*, this needs to be informed consent in the case of general personal data processing, and explicit consent in the case of sensitive data, and it can always be withdrawn.⁶⁶ This makes it difficult to obtain valid consent in the arbitration context under the *GDPR*. If consent is withdrawn or refused, further processing must cease, which may complicate or even derail the arbitral process.⁶⁷

Due to the inherent risk that consent may be refused or withdrawn, when the *GDPR* applies, it is generally preferable to rely on other legal bases. This is not to say that consent should never be employed, but rather that it should only be used as a basis for processing when all these considerations are acceptable under the circumstances. Indeed, the EU data

⁶⁶ *GDPR* (“‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”, art 4(11)).

⁶⁷ Article 29 Data Protection Working Party, “Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995” (25 November 2005) at 11.

protection authorities have referred to consent as a “false good solution”.⁶⁸

Under the *GDPR*, as set forth in the Roadmap, the following bases are generally best suited to data processing in the context of international arbitration:⁶⁹

- **Personal data.** The processing of personal data is lawful when it is necessary for the purposes of the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring protection of their personal data. For example, in the arbitration context, the data subject’s rights might override the legitimate interest in processing if the processing could raise significant risks to a data subject’s profession or personal life and the personal data is not likely to be case-determinative.
- **Sensitive (special category) data.** The processing of sensitive (special category) data is lawful when it is “necessary for the establishment, exercise or defence of legal claims,” which is called the “legal claims derogation”.⁷⁰ The legal claims derogation will often be the preferred basis for processing sensitive data. In the arbitration context, it may apply to allow processing where, for example, the processing of sensitive data is likely to have a significant impact on a claimant or respondent’s case. Personal data of children is also given

⁶⁸ EU Working Party, “Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995”, WP 114, 25 November 2005, at 11.

⁶⁹ There are other bases for lawful processing under the *GDPR*, but the ones mentioned are the most likely to apply to arbitration.

⁷⁰ *GDPR*, art 9(2)(f).

special consideration, even where it would not otherwise be considered sensitive or special data.

- **Data Relating to Criminal Convictions and Offences or Related Security Measures.** In addition to requiring a lawful basis for the processing,⁷¹ under Article 10 of the *GDPR*, the processing of personal data relating to criminal convictions and offences, or related security measures, must be carried out under the control of a supervising authority or, if the processing is authorized, by Union or Member State law. This makes it difficult to lawfully process criminal offence data. Arbitrators presiding over cases involving allegations of fraud or corruption or any other matter involving potential criminal activity should be particularly alive to this restriction and take measures to ensure the processing is lawful.

When relying upon legitimate interests as a basis for data processing, the *GDPR* requires a Legitimate Interests Assessment to be undertaken and recorded, which must be updated if events occur that might affect the original assessment.⁷² A Legitimate Interests Assessment is a contemporaneous analysis undertaken to identify the particular interests being relied upon when a data controller invokes “legitimate interests” as the lawful basis for data processing, which may be important to show if issues are raised with a data protection authority.

This is probably the area where *PIPEDA* differs the most from *GDPR* personal data processing. *PIPEDA* is consent-based; consent is required for personal data processing in Canada unless an exception applies. In the words of the OPC, individual

⁷¹ *GDPR*, art 6(1).

⁷² *GDPR*, recital 47.

knowledge and consent is the “cornerstone” of *PIPEDA*.⁷³ Express or implied consent, or a prescribed exception to the consent requirement, must always be present in respect of any collection, use or disclosure of personal information including in the context of dispute resolution. Further, personal information may only be collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances.

The OPC recognizes the challenges of obtaining consent in the context of dispute resolution, and *PIPEDA* contains a number of relevant exceptions that may apply to the consent requirement in an arbitration. The Handbook states as follows with respect to litigation, which would also apply to arbitration:

In many litigation matters, neither express nor implied consent will be applicable. This can be so where affected individuals are not parties to the litigation (*e.g.* where a corporate litigant’s employee or customer personal information is involved). In such cases, lawyers and their clients must determine whether an exception to the knowledge and consent principle listed under section 7 of *PIPEDA* applies.⁷⁴

The following are relevant *PIPEDA* sections that tend to arise in the arbitration context:

Collection:

⁷³ Policy and Research Group of the Office of the Privacy Commissioner of Canada, “Discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act*” (May 2016), online: <www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/>.

⁷⁴ *Supra* note 14.

The collection of personal information without consent is permitted under paragraph 7(1)(b) where it is reasonable to expect that:

- the collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information; and
- the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province, including the common law.

Use:

The use of personal information without consent is permitted under paragraph 7(2)(d) where the information was collected under paragraph 7(1)(b) above;

Disclosure:

The disclosure of personal information without consent is permitted by one of the exceptions listed under subsection 7(3), including the following:

- for the purpose of collecting a debt owed by the individual,
- where required to comply with a subpoena, warrant or order, or to comply with rules of court relating to the production of records, or
- when made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or of a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the

knowledge or consent of the individual would compromise the investigation.⁷⁵

It is for the Canadian arbitration professional to decide whether these exceptions apply to allow the processing of personal information without consent.

e. Lawful Data Transfer

EU-based data protection laws typically contain data transfer restrictions. Under the *GDPR*, whenever personal data is transferred outside the EU to entities or individuals who are not for other reasons already subject to the *GDPR*, transferors are required to make efforts to ensure that the personal data is protected after the transfer. As noted in the Roadmap, this leads to significant scope creep, even beyond the already broad territorial reach of the *GDPR*.

The *GDPR* rules respecting transfers of personal data to third countries apply to arbitration professionals bound by the *GDPR*. When an arbitration professional transfers personal data outside the EU to entities or individuals who are not subject to the *GDPR* or equivalent legislation or to international organizations, there must be a lawful basis for the transfer.⁷⁶

It is worth noting that the *GDPR* treats data transfers to international organizations as transfers outside the EU, even if those organizations are located in the EU. This includes international organizations such as the Permanent Court of Arbitration, the World Bank, and the International Court of Justice, which are established under international law or by an agreement between countries. Accordingly, data transfers to

⁷⁵ *Handbook for Lawyers*, *supra* note 14.

⁷⁶ “Data transfer(s)” as used herein refers to third country data transfers of personal data outside of the EU or to an international organization, keeping in mind that immunities may apply to data transfers to international organizations. The EU adopts a broad concept of transfer and strict requirements for when it is lawful. See *GDPR*, arts 45, 46(1), 49.

these bodies must meet the *GDPR*'s requirements for international data transfers (but may be subject to privileges and immunities).⁷⁷

The *GDPR* allows data transfers to third countries and international organizations where:

- the country has been deemed to provide adequate data protections, including *PIPEDA*;
- the data controller or data processor has put in place “appropriate safeguards” to protect the data through one of the means expressly prescribed by the *GDPR*;⁷⁸
- one of a list of specified derogations apply, including where the processing is “necessary for the establishment, exercise or defence of legal claims”;⁷⁹ or
- there are compelling legitimate interests pursued by the controller which are not overridden by the interests or rights of the data subject and the controller.⁸⁰

Importantly, the EU has decided that “Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act.”⁸¹ In other words, *PIPEDA* has been found to be equivalent

⁷⁷ *GDPR*, art 4(26) defining international organizations; *GDPR*, art 46(1) addressing transfers to international organizations.

⁷⁸ *GDPR*, art 46.

⁷⁹ *GDPR*, recital 52.

⁸⁰ *GDPR*, arts 45—49.

⁸¹ EC, 2002/2/EC: *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, [2002] OJ, L2 at 13—16 [*Canadian Adequacy Decision*].

to the GDPR, so data transfers may be freely made to Canadian arbitration professionals whenever PIPEDA applies.⁸²

The same is not generally true of the United States, and indeed very few countries are considered by the EU to be adequate.⁸³ This provides a significant competitive advantage to Canadian-based arbitration professionals in cases where the GDPR is implicated, because it means that personal data can flow freely from the European Union to arbitration professionals based in Canada provided that they are subject to PIPEDA without having to follow the other requirements for data transfers described above.⁸⁴ These data transfer mechanisms will often require either entering into so-called standard contractual clauses developed by the EU, or limiting data transfers to what is necessary for the establishment, exercise or defence of legal claims, which is not necessary for Canadian arbitration professionals covered by PIPEDA.

Unlike the GDPR, PIPEDA does not provide a mechanism for establishing that a third-party organization has developed an adequate level of protection. Rather, under PIPEDA, transferring organizations remain responsible for personal information transferred to third parties, as the information is considered to remain under the control of the transferring organization.⁸⁵

⁸² *GDPR*, art 45(3). An adequacy decision is an EU decision made by reference to a set of criteria to the effect that a country's data protection laws are adequate. An adequacy decision allows data to be transferred without any further authorization or notice because adequate protections apply as a matter of law, as is the case with *PIPEDA*.

⁸³ *Supra* note 5.

⁸⁴ European Commission, "Questions & Answers on the Japan Adequacy Decision" (23 January 2019), online: *European Commission* <ec.europa.eu/commission/presscorner/detail/en/MEMO_19_422>. The EC has said the "decision on Canada applies only to private entities falling under the scope of the Canadian *Personal Information Protection and Electronic Documents Act*."

⁸⁵ *PIPEDA*, art 4.1.3.

Organizations must employ contractual privacy protection clauses or other means to ensure a comparable level of protection while the information is being processed by the third party. The OPC's Guidelines for Processing Personal Data Across Borders (the "Cross-border Guidelines") clarifies that appropriate means include, but are not limited to, ensuring that the third party:

- has appropriate policies and processes in place;
- has trained its staff to ensure information is properly safeguarded at all times; and
- has effective security measures in place.⁸⁶

Further, *PIPEDA* does not distinguish between domestic and international transfers of information to third parties. It is not required to obtain additional consent for cross border transfers.⁸⁷ Although there is no requirement for additional consent for cross-border transfers under *PIPEDA*, the Cross-border Guidelines state that organizations must provide notice that:

- personal information may be sent to another jurisdiction for processing; and

⁸⁶ *Guidelines for Processing Personal Data Across Borders*, (January 2009), online: *Office of the Privacy Commissioner*, <www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127> [Cross-border Guidelines].

⁸⁷ *Bank ensures openness and comparable protection for personal information transferred to third party*, *PIPEDA Report of Findings #2020-001*, (Ottawa: Office of the Privacy Commissioner, 2020), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/PIPEDA-2020-001/>.

- while the information is in the other jurisdiction, it may be accessed by the courts, law enforcement, and national security authorities of that jurisdiction.⁸⁸

f. Data Subject Rights

Data protection laws, including the *GDPR* and *PIPEDA*, grant data subjects important rights with respect to the processing of their personal data, several of which are likely to apply during the course of an arbitration. Data subject rights is an area where there are significant differences among countries with EU-based data protection regimes, and *PIPEDA* grants fewer express rights to individuals than the *GDPR* does to data subjects.

When the *GDPR* applies, data subjects are granted the following rights:

- the right of access and to obtain a copy⁸⁹ of the personal data being processed (referred to as a “data subject access request”) except that “[t]he right to obtain a copy ... shall not adversely affect the rights and freedoms of others”⁹⁰
- the right to request modification of their data, including the correction of errors and the updating of incomplete information;⁹¹
- the right to withdraw consent if consent was the basis for processing, which highlights why it is risky to rely on consent as a lawful basis;⁹²

⁸⁸ See Cross-border Guidelines, *supra* note 86.

⁸⁹ *GDPR*, art 15(4).

⁹⁰ *GDPR*, art 7(3).

⁹¹ *GDPR*, art 16; in contrast to the *GDPR*, no right of rectification exists under the *CPPA*, *supra* note 9.

⁹² *GDPR*, art 15; *CPPA*, ss 1798.100(d), 1798.110, 1798.115.

- the right to object to processing where the lawful basis relied upon is a legitimate interest, in which case the controller must demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject;⁹³ and
- the right to erasure—also referred to as the right to deletion or the right to be forgotten—which allows a data subject to request, under certain circumstances, that their personal data be erased.⁹⁴

Arbitration professionals subject to the *GDPR* should also keep in mind that national laws may provide derogations from the *GDPR* with respect to data subject rights, which may impact the extent of the data subject rights in arbitration proceedings.

PIPEDA, on the other hand, does not contain an express list of data subject rights in the same manner as the *GDPR*, although this is something being considered for the revised legislation currently under consideration in Canada. However, some of the same rights apply under *PIPEDA*, including, for example, the right of access and the right to withdraw consent.

The right of access is the right most commonly enforced by data subjects. The *GDPR* provides that a data subject has the right to obtain from a data controller confirmation as to whether or not their personal data is being processed and, if it is, the right of access, which should include electronic access, to a broad range of information about that processing, as well as a copy of the data processed, provided that the provision of a copy does not interfere with the rights and freedoms of others.⁹⁵ However, the *GDPR* provides expressly that “the result of those

⁹³ *GDPR*, art 21; *CCPA*, s 1798.120.

⁹⁴ *GDPR*, arts 12, 17; *CCPA*, ss 1798.105, 1798.130(a), 1798.145 (g)(3).

⁹⁵ See *GDPR*, recital 63, art 15(4).

considerations should not be a refusal to provide all information to the data subject".⁹⁶

During the arbitration process, arbitration professionals may receive requests from data subjects seeking to exercise their rights. These requests may come from any individual whose personal data is handled in the arbitration, including but not limited to individual parties, witnesses, experts, or even persons not directly involved in the proceedings but about whom personal data may have been adduced (*e.g.*, an employee of a party who is not personally involved in the proceedings but who was involved in the underlying transaction), and who believes that his or her data is being processed. Data subject requests must be addressed within a prescribed timeframe (30 days under the *GDPR*⁹⁷) and it is therefore important to consider procedures for doing so in advance.

The right of access is difficult to apply during arbitration proceedings because providing a data subject with access to information about them being processed during an arbitration may violate the integrity of the proceedings or breach confidentiality. Arbitrators should be aware that invocations of the right of access may be made in a deliberate attempt to interfere with the proceedings.

The European data protection authorities have expressly taken the position that the right of access applies during dispute resolution proceedings. The *Working Document on Pre-trial Discovery for Cross Border Civil Litigation* states that data subject rights, including the right of access and to amend, may only be restricted:

on a case by case basis for example where it is necessary to protect the rights and freedoms of others. The Working Party is clear that the rights

⁹⁶ *Ibid.*

⁹⁷ *GDPR*, recital 59.

of the data subject continue to exist during the litigation process and there is no general waiver of the right to access or to amend.⁹⁸

Under *PIPEDA*, individuals generally have a broad right to access their own personal information similar to the *GDPR*. However, unlike the *GDPR*, *PIPEDA* helpfully restricts an individual's right of access to personal data processed during a formal dispute resolution procedure, likely including commercial arbitrations. Specifically, an organization is generally not required to provide access to personal information if:

- the information is protected by solicitor-client privilege;
- the information would reveal confidential commercial information;
- providing access could reasonably be expected to threaten the life or security of another individual;
- the information was collected without the individual's knowledge and consent for reasonable purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or
- the information was generated in the course of a formal dispute resolution process.⁹⁹

As discussed above, the OPC decided in the *Insurance Ombudsman Decision* that the ombudsman procedure at issue in

⁹⁸ Article 29 Data Protection Working Party, "Working Document 1/2009 on pre-trial discovery for cross border civil litigation" (11 February 2009) at 12, online (pdf): www.garanteprivacy.it/documents/10160/10704/ARTICOLO+29+-+WP+158+-+cross+border+civil+litigation.pdf/1595b252-efb3-460d-837d-c892b5d3e22a?version=1.2 ["Discovery Guidelines"].

⁹⁹ *Insurance Ombudsman Decision*, *supra* note 21.

that case was a dispute resolution procedure, but did not rise to the level of being “formal”, so that it was *subject to* the right to access. However, the OPC’s reasoning gives insight into why commercial arbitration agreed to between the parties and subject to binding arbitration rules would likely be considered a “formal dispute resolution” and therefore *not* subject to the right to access:

A “formal dispute resolution process” suggests the presence of a framework, either legislated or agreed to by the parties to the dispute, as well as a process that takes place in accordance with recognized rules. This is consistent with an unpublished finding by our Office, which examined the Ombudsman’s Office of a financial institution with a framework almost identical to that of the Ombudsman.¹⁰⁰

Under the OPC’s rationale in that decision, commercial arbitrations based on arbitration agreements entered into between commercial entities under recognized arbitration rules would seem to fall within this standard. As such, information generated in the course of commercial arbitration proceedings may not be subject to the right to access.

As noted by the OPC in that decision, it is important to keep in mind that in making this determination the OPC was “considering whether the process at issue should be exempted from the obligation to allow data subjects access to their data from the process” (thereby restricting their rights. The OPC noted in that regard that:

Paragraph 9(3)(d) constitutes an exemption to an organization’s obligation to provide an individual with access to personal information under the Act. Since the Act has been recognized as quasi-

¹⁰⁰ *Ibid.*

constitutional legislation, the rights accorded under it should be given a liberal and purposive interpretation, and restrictions on those rights should be interpreted narrowly. In this case, any ambiguity concerning the scope of paragraph 9(3)(d) should be resolved in favour of granting access to personal information.¹⁰¹

This would caution in favour of reading the *Insurance Ombudsman Decision* narrowly.

When faced with a data subject access request during an arbitration proceeding, careful consideration should be given to whether an exemption applies (for example under PIPEDA), to the impact that meeting the request might have on others (both those involved in the arbitration and third parties), and to identifying and implementing measures to reduce any potential adverse impact on third parties or the proceedings themselves. For example, personal data relating to third parties may be redacted and access limited to those documents or portions thereof strictly necessary to meet the exact terms of the data subject's request, rather than adopting a blanket (and less onerous) approach. National courts have also suggested that striking a balance between different stakeholders' interests might involve obtaining undertakings to restrict the onward transfer of any information disclosed in response to the data subject access request.¹⁰²

g. Data Minimization

Data minimization is a key component of data protection compliance, both as a requirement in itself and also as part of data security. Data minimization requires the collection and

¹⁰¹ *Ibid.*

¹⁰² *B v General Medical Council* [2018] EWCA Civ 1497.

retention of personal data to be limited to information that is directly relevant and necessary for a specified purpose.

Data minimization is required by *PIPEDA*:

Principle 4 – Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. ... Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.¹⁰³

Data minimization is also a fundamental principle of the *GDPR*:

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.¹⁰⁴

Data minimization is also part of good cyber security hygiene. Given the amount of personal data that is typically processed and transferred in the context of a dispute, data minimization is an important consideration.

As discussed in the Roadmap, data minimization is required in all stages of the arbitral process and requires those involved to ensure that the amount and type of personal data processed is adequate, relevant, and limited to what is necessary for the lawful purpose of the processing (i.e., preparing a case for arbitration, prosecuting, defending against, or deciding a claim, administering the proceedings, or retaining data in relation to the arbitration after completion of the proceedings). As discussed below, this is especially important during the

¹⁰³ *PIPEDA*, Annex 1.

¹⁰⁴ *GDPR*, art 5(1)(c).

document disclosure phase of the arbitration and supports limiting disclosure.

h. Data Retention

Similar to the rules requiring the minimization of personal data being processed generally, EU-based data protection laws contain express limitations on the retention of personal data.

The *GDPR* provides that:

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.¹⁰⁵

PIPEDA imposes a similar requirement:

Personal information shall be retained only as long as necessary for the fulfilment of [the purposes for which it was collected]. ... Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.¹⁰⁶

These principles ensure that personal data is only stored for as long as necessary for the purpose for which it is being processed. As discussed in the Roadmap, in practice, this means that arbitration professionals, like all those covered by the data protection laws should:

- Retain personal data only for as long as reasonably necessary;

¹⁰⁵ *GDPR*, art 5(1)(e).

¹⁰⁶ *PIPEDA*, Annex 1.

- Be able to justify how long they retain personal data, which will depend on the purposes informed to the data subject for holding the data;
- Periodically review the data held, and erase or anonymize it when they no longer need it; and
- Carefully consider any challenges to their retention of data.

IV. WHAT DOES THIS MEAN FOR ARBITRATION PROCEEDINGS?

The nature of the arbitral process is such that significant amounts of personal data (sometimes including sensitive and criminal data) is exchanged and processed, often across borders. Such data exchanges, transfers, and processing are inherent to the international arbitration process. However, they must be lawful under the applicable data protection laws, and procedures must be put in place to ensure compliance with those laws throughout (and beyond) the proceedings.

At the outset of any dispute, long before any request for arbitration is filed, parties and their lawyers will review the facts by going back through the chain of events that led to the dispute. This will involve review of contemporaneous correspondence, usually starting from the contracting stage. Moreover, the possibility of document disclosure during an arbitration may require the parties and others to suspend their usual data destruction policies or to make changes to their usual retention or deletion processes to comply with a “litigation/arbitration hold” in contemplation of legal proceedings. All of these activities constitute the processing of the personal data subject to the data protection laws and must comply with those laws when they apply.

Data minimization is an important part of all EU-based data protection laws and should be practiced throughout the arbitration process. Data minimization obligations are particularly relevant in the selection, production, and disclosure

of documents.¹⁰⁷ The EU data protection authorities have suggested that data minimization is likely to require the following when making disclosures:

- Limiting the data disclosed to what is relevant to the dispute and non-duplicative;
- Identifying the personal data contained in the responsive material;
- Redacting or pseudonymizing unnecessary personal data;
- Considering confidentiality orders; and
- Ensuring proper data protection measures are in place after disclosure

Limiting disclosure to relevant documents is already standard practice in international arbitration, in order to reduce the volume of data disclosed. However, redaction of personal data is not common practice and may require significant additional time and effort. Technology, including artificial intelligence, may assist in both culling the data for relevance and in redacting personal data. However, these measures themselves constitute data processing, triggering data protection obligations, and can be costly and time-consuming.

¹⁰⁷ The European Data Protection Board has stated that “the principle of data minimization ... emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which [it is] processed.” See European Data Protection Board, “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0” (2021) at 13, online (pdf): *Eurioean Data Protection Board* <edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> [Data Transfer Guidance].

It is also important to keep in mind that data protection principles apply during the hearing and to the award. This means in the context of remote hearings, for example, the exchange of information and testimony during the hearing could be considered a data transfer subject to the restrictions imposed on such transfers. Further, any personal data included in the award must comply with the data protection rules, taking into account that the award may become public even in the context of confidential arbitrations (for example during enforcement proceedings).

As a procedural matter, it is important that in cases where an EU-based data protection law, like the *GDPR* or *PIPEDA*, applies to some or all those involved in the proceeding, data protection be considered at the initial procedural hearing or case management conference. This will allow the tribunal, together with the parties and their counsel, to consider the potential impact that data protection may have on the proceedings and to put measures in place to manage these issues and to avoid either party using them to its advantage. This may be complicated in the event that only one of the parties is subject to strict data protection obligations, which may lead to issues of inequality of treatment.

Issues to be considered include:

- Data security
- Potential impact of data protection on the exchange of information during the proceeding, including, for example:
 - Document disclosure
 - Hearing
 - Award
- Any necessary processes for:

- Addressing any data subject requests
- Data breach notification process
- Documenting compliance in a manner that can be shared with regulators if necessary

These issues are discussed in the Roadmap, which includes annexes addressing measures that may be employed during an arbitration. In cases where the impact of data protection is expected to be minimal, this may be limited to the inclusion of general language in the first procedural order or terms of reference that the parties will comply with such data protection measures and that they will ensure that such compliance will not impact the orderly conduct of the proceedings, including document disclosure, the hearing, the award, data subject access requests, data breach procedures, and the documentation of compliance. Language should also be included addressing data security and data breach procedures.

In cases where data protection may significantly impact the proceedings, a data protection protocol should be considered (and may be required) to ensure compliance among controllers and organizations with their parallel and interlinked obligations, as is the case in arbitration. For example, under the *GDPR*, a data protection protocol is required whenever joint controllers process personal data.¹⁰⁸

As described in the Roadmap, a data protection protocol is an agreement on how data protection will be applied in a particular context. Data protection protocols can be usefully employed in arbitrations to manage the compliance obligations of all those responsible for data protection compliance throughout the arbitration.

¹⁰⁸ *GDPR art 26* (“Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation.”).

V. CONCLUDING THOUGHTS

International arbitration proceedings have become a digital process, which allows for significant benefits in terms of time, cost, and other efficiencies. However, while the wide-spread use of technology largely acts as a facilitator of international arbitration, it also introduces constraints on the process, including those stemming from data protection and related security requirements.

It is therefore important that data protection and security be addressed and managed during international arbitration proceedings. In this context, as described above, Canadian arbitration professionals should be aware that:

- The *GDPR* applies to arbitration professionals when they have an EU establishment and the data processing takes place in the “context of the activities” of that establishment wherever the data processing occurs in the world, and the same applies under the UK Data Protection Act and the UK *GDPR*.
- *PIPEDA* applies to arbitration professionals in the context of their commercial activities.
- *PIPEDA* and the *GDPR* may apply to international commercial arbitration proceedings.
- Where *PIPEDA* applies to an arbitration professional, personal data may freely transfer to them from the EU.
- *PIPEDA* is going to change, so it is important to keep apprised of developments.
- A good source of guidance on when and how data protection laws apply to international arbitrations is the Draft ICCA-IBA Roadmap to Data Protection in International Arbitration and its annexes, which will be finalized during 2021.

ANNEX 1

PIPEDA's FAIR INFORMATION PRINCIPLES

Where *PIPEDA* applies, it requires organizations engaged in commercial activities to comply with a set of legal obligations based on ten principles in relation to those commercial activities unless a relevant exception applies. These are:

Principle 1 - Accountability

An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Principle 2 - Identifying Purposes

The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.

Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 - Limiting Collection

The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

Principle 5 - Limiting Use, Disclosure, and Retention

Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Principle 6 - Accuracy

Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Principle 7 - Safeguards

Personal information must be protected by appropriate security relative to the sensitivity of the information.

Principle 8 - Openness

An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Principle 9 - Individual Access

Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information.¹⁰⁹

An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance

An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be

¹⁰⁹ This will not apply to arbitration proceedings when para 9(3)(a) of *PIPEDA* is engaged, which provides that an organization is not required to give access to personal information if the information is protected by solicitor-client privilege or, in civil law, by the professional secrecy of lawyers and notaries and para 9(3)(d) of *PIPEDA* states that an organization is not required to give access to personal information if the information was generated in the course of a formal dispute resolution process.

addressed to the person accountable for the organization's compliance with *PIPEDA*, usually their Chief Privacy Officer.¹¹⁰

Further, any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances.¹¹¹

These principles are similar to those found in the *GDPR* and other EU-based data protection laws.

¹¹⁰ Office of the Privacy Commissioner of Canada, "*PIPEDA* in Brief" (May 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-PIPEDA/PIPEDA_brief/>.

¹¹¹ *Ibid.*

ANNEX 2**ICCA-NYC BAR-CPR CYBERSECURITY PROTOCOL
FOR INTERNATIONAL ARBITRATION (2020)**

(Without Commentary)

Scope and Applicability

Principle 1 The Cybersecurity Protocol provides a recommended framework to guide tribunals, parties, and administering institutions in their consideration of what information security measures are reasonable to apply to a particular arbitration matter.

Principle 2 As a threshold matter, each party, arbitrator, and administering institution should consider the baseline information security practices that are addressed in Schedule A and the impact of their own information security practices on the arbitration. Effective information security in a particular arbitration requires all custodians of arbitration-related information to adopt reasonable information security practices.

Principle 3 Parties, arbitrators, and administering institutions should ensure that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.

Principle 4 The Protocol does not supersede applicable law, arbitration rules, professional or ethical obligations, or other binding obligations.

The Standard

Principle 5 Subject to Principle 4, the information security measures adopted for the arbitration shall be those that are

reasonable in the circumstances of the case as considered in Principles 6-8.

Determining Reasonable Cybersecurity Measures

Principle 6 In determining which specific information security measures are reasonable for a particular arbitration, the parties and the tribunal should consider: (a) the risk profile of the arbitration, taking into account the factors set forth in Schedule B; (b) the existing information security practices, infrastructure, and capabilities of the parties, arbitrators, and any administering institution, and the extent to which those practices address the categories of information security measures referenced in Principle 7; (c) the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution; (d) proportionality relative to the size, value, and risk profile of the dispute; and (e) the efficiency of the arbitral process.

Principle 7 In considering the specific information security measures to be applied in an arbitration, consideration should be given to the following categories:

- (a) asset management;
- (b) access controls;
- (c) encryption;
- (d) communications security;
- (e) physical and environmental security;
- (f) operations security; and
- (g) information security incident management.

Principle 8 In some cases, it may be reasonable to tailor the information security measures applied to the arbitration to the risks present in different aspects of the arbitration, which may include:

(a) information exchanges and transmission of arbitration related information;

(b) storage of arbitration-related information;

(c) travel;

(d) hearings and conferences; and/or

(e) post-arbitration retention and destruction policies.

Process to Establish Reasonable Cybersecurity Measures

Principle 9 Taking into consideration the factors outlined in Principles 6-8 as appropriate, the parties should attempt in the first instance to agree on reasonable information security measures.

Principle 10 Information security should be raised as early as practicable in the arbitration, which ordinarily will not be later than the first case management conference.

Principle 11 Taking into consideration Principles 4-9 as appropriate, the arbitral tribunal has the authority to determine the information security measures applicable to the arbitration.

Principle 12 The arbitral tribunal may modify the measures previously established for the arbitration, at the request of any party or on the tribunal's own initiative, in light of the evolving circumstances of the case.

Principle 13 In the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident, the arbitral tribunal may, in its discretion:

- (a) allocate related costs among the parties; and/or
- (b) impose sanctions on the parties.

Principle 14 The Protocol does not establish any liability or any liability standard for any purpose, including, but not limited to, legal or regulatory purposes, liability in contract, professional malpractice, or negligence.

1 January 2021

NOTE TO PARTIES AND ARBITRAL TRIBUNALS ON THE CONDUCT OF THE ARBITRATION UNDER THE ICC RULES OF ARBITRATION

Table of contents

I - GENERAL INFORMATION	3
A - The ICC International Court of Arbitration and its Secretariat	3
B - Where Requests for Arbitration can be Submitted	3
C - Communications	3
II - PARTIES	4
A - Representation	4
B - Joinder of Additional Parties	4
C - Consolidation	5
D - Third Party Funding	5
III - ARBITRAL TRIBUNAL	5
A - Statement of Acceptance, Availability, Impartiality and Independence	5
B - Assistance by the Secretariat with the Nomination or Appointment of Arbitrators	8
C - Constitution of the Arbitral Tribunal	8
IV - TRANSPARENCY	9
A - Communication of Reasons for the Court's Decisions	9
B - Publication of Information Regarding Arbitral Tribunals, Industry Sector and Law Firms involved	9
C - Publication of Awards, Procedural Orders, Dissenting and/or Concurring Opinions	10
V - CONDUCT OF PARTICIPANTS IN THE ARBITRATION	11
VI - EMERGENCY ARBITRATOR	12
VII - CONDUCT OF THE ARBITRATION	13
A - Advance on Costs	13
B - Expeditious and Efficient Conduct of the Arbitration	14
C - Hearings – Virtual Hearings	15
D - Expeditious Determination of Manifestly Unmeritorious Claims or Defences	16
E - Protection of Personal Data	17
F - Time Limits under the Rules	18
VIII - EXPEDITED PROCEDURE PROVISIONS	19
A - Scope of the Expedited Procedure Provisions	19
B - Determination of the Amount in Dispute for the Purpose of the Application of the Expedited Procedure Provisions	20
C - Scales	20
D - Information to the Parties	21
E - Constitution of the Arbitral Tribunal	21
F - Proceedings before the Arbitral Tribunal	21
G - Award	22
IX - EFFICIENCY IN THE SUBMISSION OF DRAFT AWARDS TO THE COURT	22
A - General Practice	22
B - Practice under the Expedited Procedure Provisions	23

X - CLOSING OF THE PROCEEDINGS AND SCRUTINY OF AWARDS	23
A - Closing of the Proceedings	23
B - Scrutiny Process	23
C - Information to the Parties	24
D - Timing of Scrutiny	24
XI - ICC AWARD CHECKLIST.....	24
XII - TREATY-BASED ARBITRATIONS	25
XIII - SUBMISSIONS BY <i>AMICI CURIAE</i> AND NON-DISPUTING PARTIES.....	25
XIV - ARBITRAL TRIBUNAL'S FEES AND ADMINISTRATIVE EXPENSES.....	25
A - Scales	25
B - Advance on Fees	25
C - Allocation among Arbitral Tribunal Members	25
D - Fixing of Fees	26
E - Replacement.....	26
F - Administrative Expenses	26
G - Declaration to French Tax Authorities.....	27
XV - DECISIONS AS TO THE COSTS OF THE ARBITRATION.....	27
XVI - SIGNATURE OF TERMS OF REFERENCE AND AWARDS – NOTIFICATION OF AWARDS	27
XVII - CORRECTION AND INTERPRETATION OF AWARDS.....	28
XVIII - ADDITIONAL AWARDS.....	29
XIX - INTERNATIONAL SANCTIONS REGULATIONS	30
XX - ADMINISTRATIVE SECRETARIES	30
A - Appointment.....	30
B - Duties	30
C - Disbursements	31
D - Remuneration	31
XXI - ARBITRATOR'S EXPENSES.....	31
A - How to Submit a Request for Expenses	31
B - When to Submit a Request for Expenses	32
C - Travel Expenses	32
D - Per Diem Allowance.....	33
E - General Office Expenses and Courier Charges	33
F - Advance Payments on Expenses.....	33
XXII - ADMINISTRATIVE SERVICES.....	34
A - Deposit of Funds other than the Advance on Costs for Arbitration.....	34
B - Deposits for VAT, Taxes, Charges and Imposts Applicable to Arbitrators' Fees	35
XXIII - VAT PAYABLE ON ICC ADMINISTRATIVE EXPENSES	36
XXIV - ASSISTANCE WITH THE CONDUCT OF THE ARBITRATION	37
A - Conduct of the Arbitration.....	37
B - Hearings and Meetings	38
C - Sealed Offer(s).....	38
XXV - POST-AWARD SERVICES	39
XXVI - INTERNATIONAL CENTRE FOR ADR	40
A - ICC Mediation Rules	40
B - ICC Expert Rules	40
XXVII - DISPATCH OF MATERIALS TO ICC AND CUSTOMS CHARGES.....	40

I - General information

1. This Note is intended to provide parties and arbitral tribunals with practical guidance concerning the conduct of arbitrations under the ICC Rules of Arbitration (“Rules”) as well as the practices of the International Court of Arbitration of the International Chamber of Commerce (“Court”).
2. Unless otherwise indicated, this Note applies to all ICC arbitrations regardless of the version of the Rules pursuant to which they are conducted. The Articles in this Note refer to the 2021 Rules.

A - The ICC International Court of Arbitration and its Secretariat

3. The Court is an administrative body that ensures that ICC arbitrations are conducted in accordance with the Rules. It does not itself resolve disputes (Article 1(2)).
4. The Court is assisted by its Secretariat (Article 1(5)). The Secretariat is led by the Secretary General, the Deputy Secretary General and the Managing Counsel. It is composed of case management teams, each headed by a Counsel.
5. The Secretariat closely monitors each arbitration and assists parties and arbitral tribunals with any questions relating to the conduct of the arbitration. The parties and/or their representatives are encouraged to contact the Secretariat with any questions or comments arising from the Rules and/or this Note.
6. At the end of each arbitration, the parties, their counsel or other representatives (“counsel”) and the arbitrators will be invited to submit an evaluation form to the Secretariat.

B - Where Requests for Arbitration can be Submitted

7. ICC arbitration is commenced upon the Secretariat’s receipt of a Request for Arbitration. Requests for Arbitration may be submitted by email [at this address](#) or at any of the Secretariat’s offices in hard copies (Articles 4(1) of the Rules and 5(3) of Appendix II). Updated information on the list of the Secretariat’s offices where Requests for Arbitration may be submitted is maintained [here](#).
8. Upon receipt of the Request for Arbitration, the Secretary General will assign the case to one of the Secretariat’s case management teams in any of the Secretariat’s offices. The case file may be transferred to an office of the Secretariat other than the office in which the Request for Arbitration was filed.

C - Communications

9. Pursuant to Article 3(1), parties and arbitrators must send copies of all written communications directly to all other parties, arbitrators and the Secretariat.
10. As a general rule, the Request for Arbitration (Article 4), the Answer and any counterclaims (Article 5), and any Request for Joinder (Article 7) must be sent to the Secretariat by email. Hard copies should be submitted only where the party filing the Request, Answer and any counterclaim or any Request for Joinder requests transmission thereof by delivery against receipt, registered post or courier. In all other instances, hard copies should not be sent to the Secretariat, even when the arbitral tribunal has asked to be provided with hard copies.

11. The Secretariat will communicate via email, unless circumstances warrant other means of communication. The parties, counsel and prospective arbitrators must provide the Secretariat with their email addresses.

II - Parties

A - Representation

12. Parties must inform the Secretariat and the arbitral tribunal of the name(s) and contact details of their representative(s). Parties must promptly inform the Secretariat, the arbitral tribunal and the other parties of any changes in their representation.
13. Once the arbitral tribunal has been constituted, the parties should refrain from introducing a new representative if a relationship exists between that representative and one or more of the arbitrators that affects the arbitrator's independence and impartiality.
14. Pursuant to Article 17(2), the arbitral tribunal may, after affording an opportunity to the parties to comment in writing within a suitable period of time, take any measure necessary to safeguard the integrity of the arbitration, including, but not limited to, excluding the newly introduced party representative from the proceedings.
15. In deciding whether to exclude a newly introduced party representative from the proceedings, the arbitral tribunal shall carefully consider all relevant circumstances with the aim of safeguarding the integrity of the arbitration, such as (a) the ability of the party that has introduced the new representative to properly submit its case in the absence of that representative, (b) the timing of the addition of such newly introduced party representative, and (c) the disruption to the arbitration that may result from its continuing participation in case of a successful challenge against one or more of the arbitrators.

B - Joinder of Additional Parties

16. A party wishing to join an additional party shall submit a request for joinder to the Secretariat ("Request for Joinder"). Requests for Joinder are made in the same manner as a Request for Arbitration. Upon being joined, the additional party becomes a party to the arbitration and may raise pleas pursuant to Article 6(3).
17. After the confirmation or appointment of any arbitrator, an additional party may be joined if (i) all parties, including the additional party, so agree (Article 7(1)); or (ii) the arbitral tribunal, once constituted, so decides, provided the additional party accepts the constitution of the arbitral tribunal and agrees to the Terms of Reference, where applicable (Article 7(5)).
18. In deciding on a Request for Joinder under Article 7(5), the arbitral tribunal shall consider all relevant circumstances, such as whether the arbitral tribunal has prima facie jurisdiction over the additional party, the timing of the request, possible conflicts of interest that may arise from the joinder, and the impact of the joinder on the efficient conduct of the arbitration. Any decision to join a consenting additional party is without prejudice to the arbitral tribunal's decision on its jurisdiction regarding that party, in case such jurisdiction is contested.

C - Consolidation

19. Article 10 contemplates three possible scenarios in which the Court may, at the request of a party, consolidate two or more pending arbitrations:
 - a. when all parties agree to the consolidation (Article 10(a));
 - b. when all claims are based on the same arbitration agreement or arbitration agreements, even if the parties in the pending arbitrations are not the same (Article 10(b)). While previous versions of the Rules limited the possibility of consolidation in the presence of different parties to situations where all claims are made under the same arbitration agreement, the 2021 amendment allows consolidations when all claims are brought under the same arbitration agreement or agreements. For example: parties A, B, C and D are parties to a Share Purchase Agreement (SPA) and a Shareholders Agreement (SHA). Parties A and D are parties to arbitration 1, while parties B and C are parties to arbitration 2. In such a scenario, consolidation of arbitrations 1 and 2 may be possible; or
 - c. the parties in the pending arbitrations are the same and the claims are made under different arbitration agreements (Article 10(c)). For example: arbitration 1 is between parties A and B with claims under an SPA arbitration agreement, and arbitration 2 is between the same parties with claims under a SHA arbitration agreement. In that scenario, consolidation may be possible if the disputes in the arbitrations arise from the same legal relationship and the Court finds these arbitration agreements to be compatible.

D - Third Party Funding

20. To assist arbitrators and prospective arbitrators in complying with their duty of disclosure (see section III(A)), each party must, pursuant to Article 11(7), promptly inform the Secretariat, the arbitral tribunal and the other parties of the existence and identity of any non-party that has entered into an arrangement for the funding of claims and defences and under which that non-party has an economic interest in the outcome of the arbitration. For example, the non-party is entitled to receive all or part of the proceeds of the award.
21. Subject to any different determination that may be made by the arbitral tribunal in the circumstances of any given case, Article 11(7) would normally not capture (i) inter-company funding within a group of companies, (ii) fee arrangements between a party and its counsel, or (iii) an indirect interest, such as that of a bank having granted a loan to the party in the ordinary course of its ongoing activities rather than specifically for the funding of the arbitration.

III - Arbitral Tribunal

A - Statement of Acceptance, Availability, Impartiality and Independence

22. All arbitrators, including emergency arbitrators, have the duty to act at all times in an impartial and independent manner (Articles 11 and 22(4)).
23. The Court requires all prospective arbitrators to complete and sign a Statement of Acceptance, Availability, Impartiality and Independence ("Statement") (Article 11(2)).

24. The parties have a legitimate interest in being fully informed of all facts or circumstances that may be relevant in their view to be satisfied that an arbitrator or prospective arbitrator is and remains independent and impartial or, if the parties so wish, to explore the matter further and/or take the initiatives contemplated by the Rules.
25. An arbitrator or prospective arbitrator must disclose in his or her Statement, at the time of his or her appointment and as the arbitration is ongoing, any circumstance that might be of such a nature as to call into question his or her independence in the eyes of any of the parties or give rise to reasonable doubts as to his or her impartiality. Any doubt must be resolved in favour of disclosure.
26. A disclosure does not imply the existence of a conflict. On the contrary, arbitrators who make disclosures consider themselves to be impartial and independent, notwithstanding the disclosed facts, or else they would decline to serve. In the event of an objection or a challenge, it is for the Court to assess whether the matter disclosed is an impediment to service as arbitrator. Although failure to disclose is not in itself a ground for disqualification, it will however be considered by the Court in assessing whether an objection to confirmation or a challenge is well founded.
27. Each arbitrator or prospective arbitrator must assess what circumstances, if any, are such as to call into question his or her independence in the eyes of the parties or give rise to reasonable doubts as to his or her impartiality. In making such assessment, an arbitrator or prospective arbitrator should consider all potentially relevant circumstances, including **but not limited to** the following:
 - The arbitrator or prospective arbitrator or his or her law firm represents or advises, or has represented or advised, one of the parties or one of its affiliates.
 - The arbitrator or prospective arbitrator or his or her law firm acts or has acted against one of the parties or one of its affiliates.
 - The arbitrator or prospective arbitrator or his or her law firm has a business relationship with one of the parties or one of its affiliates, or a personal interest of any nature in the outcome of the dispute.
 - The arbitrator or prospective arbitrator or his or her law firm acts or has acted on behalf of one of the parties or one of its affiliates as director, board member, officer, or otherwise.
 - The arbitrator or prospective arbitrator or his or her law firm is or has been involved in the dispute, or has expressed a view on the dispute in a manner that might affect his or her impartiality.
 - The arbitrator or prospective arbitrator has a professional or close personal relationship with counsel to one of the parties or the counsel's law firm.
 - The arbitrator or prospective arbitrator acts or has acted as arbitrator in a case involving one of the parties or one of its affiliates.
 - The arbitrator or prospective arbitrator acts or has acted as arbitrator in a related case.
 - The arbitrator or prospective arbitrator has in the past been appointed as arbitrator by one of the parties or one of its affiliates, or by counsel to one of the parties or the counsel's law firm.

In assessing whether a disclosure should be made, an arbitrator or prospective arbitrator should consider relationships with non-parties having an interest in the outcome of the arbitration, such as third-party funders as well as relationships with other members of the arbitral tribunal, as well as experts or witnesses in the case.

28. To assist prospective arbitrators, the Secretariat endeavours to identify, at the outset of the case, entities and individuals in the arbitration that may be relevant for purposes of disclosure. Such an indication does not release an arbitrator or prospective arbitrator from his or her duty to disclose with respect to other relevant entities and individuals he or she may be aware of. In case of doubt with respect to such an indication made by the Secretariat, an arbitrator or prospective arbitrator is encouraged to consult the Secretariat.
29. The duty to disclose is of an ongoing nature and therefore applies throughout the duration of the arbitration.
30. Although an advance declaration or waiver in relation to possible conflicts of interest arising from facts and circumstances that may arise in the future may or may not in certain circumstances be taken into account by the Court, such advance declaration or waiver does not discharge an arbitrator from his or her ongoing duty to disclose.
31. When completing his or her Statement and identifying whether he or she should make a disclosure, both at the outset of the arbitration and subsequently, an arbitrator or prospective arbitrator should make reasonable enquiries in his or her records, those of his or her law firm and, as the case may be, in other readily available materials.
32. For the scope of disclosures, an arbitrator is considered to bear the identity of his or her law firm, and a legal entity includes its affiliates. In addressing possible objections to confirmation or challenges, the Court will consider the activities of the arbitrator's law firm and the relationship of the law firm with the arbitrator in each individual case. In each case, arbitrators should consider disclosing relationships with another arbitrator or counsel who is a member of the same barristers' chambers. Arbitrators should also consider disclosing relationships between arbitrators, as well as relationships with any entity having a direct economic interest in the dispute or an obligation to indemnify a party for the award.
33. Arbitrators have a duty to devote to the arbitration the time necessary to conduct the proceedings as diligently, efficiently and expeditiously as possible. Accordingly, prospective arbitrators must indicate in the Statement the number of arbitrations in which they are currently acting, specifying whether they are acting as president, sole arbitrator, co-arbitrator or counsel to a party, as well as any other commitments and their availability over the next 24 months.
34. If one or more parties object to the confirmation of a prospective arbitrator, or in case of a challenge, the Secretariat will invite the other party or parties and the arbitrator or prospective arbitrator to comment.
35. Arbitrators are encouraged to ensure that they have appropriate insurance to cover their liability. In assessing whether they should seek insurance, arbitrators may want to consider the circumstances of the case, including the amount in dispute, the currencies used, the nationalities and locations of the parties, the place of arbitration and the location of hearings.
36. By signing the Statement, prospective arbitrators acknowledge that their name and contact details, as well as their *curriculum vitae*, may be communicated to the members of the Court, the Secretariat at its various offices, and to ICC National Committees and Groups to perform the functions assigned to them under the Rules. By signing the Statement, prospective arbitrators also acknowledge that their names and related information, as well as their award(s), procedural order(s) and dissenting or concurring opinion(s) may be published pursuant to sections IV(B) and (C), to (a) further the legitimate interests of the parties, arbitrators and the public in accessing transparent information about ICC arbitration; (b) assist them in their decision making and in pursuing their legitimate interests; (c) safeguard the parties' fundamental procedural rights through arbitration and (d) ensure the rendering of high

quality awards. The prospective arbitrator may object to the publication if his/her interests and fundamental rights override such legitimate interests.

B - Assistance by the Secretariat with the Nomination or Appointment of Arbitrators

37. Parties nominating a sole arbitrator or a presiding arbitrator for confirmation by the Secretary General or the Court, and co-arbitrators nominating a presiding arbitrator, may jointly seek the Secretariat's assistance by requesting that the Secretariat either propose names of possible candidates or provide non-confidential information on prospective arbitrators. Upon joint request of the parties, the Secretariat may also contact prospective arbitrators in order to check their experience, availability and possible conflicts of interests.
38. The parties may agree that the Court's appointment of a sole arbitrator or a presiding arbitrator will occur in consultation between the parties and the Secretariat. In particular, the parties may agree that any such appointment will occur following a list procedure, whereby the Secretariat will establish a list of candidates and submit it to the parties (for example by allowing the parties to strike a limited number of candidates and rank the others by order of preference) before proceeding with the appointment.

C - Constitution of the Arbitral Tribunal

39. Arbitral tribunals are constituted under the Rules in accordance with the parties' agreement, as recorded in the arbitration agreement or subsequently.
40. Where the parties have not agreed upon the number of arbitrators, the Court will in general appoint a sole arbitrator, save where it appears that the complexity of the dispute or the interests at stake warrant the appointment of three arbitrators. Without prejudice to other relevant circumstances that may lead to the constitution of a three-member arbitral tribunal, the Court will normally decide in favour of a sole arbitrator where the amount in dispute is less than US\$ 10,000,000 and in favour of three arbitrators where the amount in dispute exceeds US\$ 30,000,000.
41. Article 12(6) addresses the constitution of three-member arbitral tribunals in multiparty arbitrations and requires the multiple claimants, jointly, and multiple respondents, jointly, to nominate an arbitrator. Article 12(7) provides that an additional party may jointly nominate an arbitrator with the claimant(s) or respondent(s).
42. In the absence of the aforementioned joint nomination, the Court may appoint an arbitrator on behalf of the parties that failed to jointly nominate pursuant to Article 12(4). Alternatively, the Court may appoint each member of the arbitral tribunal and designate one of them to act as president pursuant to Article 12(8), unless the parties agree to a method for the constitution of the arbitral tribunal. Where it appears that the interests of multiple parties that failed to nominate jointly may not be aligned, the Court applies Article 12(8) with the aim of ensuring that all parties are treated equally in the process for the constitution of the arbitral tribunal.
43. Article 12(9) provides that, in exceptional circumstances, the Court may appoint each member of the arbitral tribunal, notwithstanding any agreement by the parties on the method for constituting the arbitral tribunal, when the provisions of the arbitration agreement are unconscionable and applying them would result in a significant risk of unequal treatment and unfairness that may affect the validity of the award. For example, the Court may apply Article 12(9) when the arbitration agreement provides that one of the parties will have the right to constitute the arbitral tribunal unilaterally, and such unilateral right is not admitted by the law at the place of the arbitration.

44. Pursuant to Article 13(5), when the Court appoints the sole arbitrator or the president of the arbitral tribunal, that arbitrator must be a nationality other than those of the parties. That rule seeks to ensure that the presiding arbitrator or the sole arbitrator is fully neutral and equidistant from the parties, while acknowledging the right of the parties to nominate co-arbitrators sharing their nationality. Where all parties share the same nationality, however, the Court may appoint a presiding arbitrator or a sole arbitrator having the same nationality of the parties, provided that none of the parties objects. That possibility will normally not be used in a context where the parties are the same nationality but the dispute is international in nature (e.g. one of the parties is a Special Purpose Vehicle (SPV) or the local subsidiary of an international group).
45. Article 13(6) acknowledges the specific nature of treaty-based arbitration, where the arbitral tribunal has to apply international law and may have to assess the legitimacy of public policies, regulation and legislation taken in the interest of the public. In such a context, none of the arbitrators may have the same nationality as any party to the arbitration, unless the parties agree otherwise.

IV - Transparency

A - Communication of Reasons for the Court's Decisions

46. Pursuant to Article 5 of Appendix II, upon request of any party, the Court will communicate the reasons for a decision on (i) *prima facie* jurisdiction (Article 6(4)); (ii) consolidation (Article 10); (iii) Article 12(8); (iv) Article 12(9); (v) the challenge of an arbitrator pursuant to Article 14; (vi) whether to replace an arbitrator pursuant to Article 15(2).
47. In exceptional circumstances, however, the Court may decide not to communicate the reasons for any of these decisions.
48. For arbitrations conducted under the Rules in effect prior to the entry into force of the 2017 Rules, a request for communication of reasons must be made by all parties.
49. Any request for the communication of reasons must be made in advance of the decision in respect of which reasons are sought. Such request may be made when the Secretariat invites parties to comment ahead of the Court's decision.

B - Publication of Information Regarding Arbitral Tribunals, Industry Sector and Law Firms Involved

50. Increasing the information available to parties, the business community at large and academia is key to ensuring that arbitration remains a trusted tool to facilitate trade. Transparency provides greater confidence in the arbitration process, and helps protect arbitration against inaccurate or ill-informed criticism. The Court therefore endeavours to make the arbitration process more transparent without compromising the parties' expectations, if any, of confidentiality.
51. Consistent with that policy and unless otherwise agreed by the parties, the Court publishes on the ICC website, for arbitrations registered as of 1 January 2016, the following information: (i) the names of the arbitrators, (ii) their nationality, (iii) their role within an arbitral tribunal, (iv) the method of their appointment, and (v) whether the arbitration is pending or closed. The arbitration reference number and the names of the parties and of their counsel will not be published.

52. For arbitrations registered as of 1 January 2020, the Court publishes on the ICC website the following additional information: (vi) the industry sector involved, (vii) law firms representing the parties in the case. For arbitrations registered as of 1 January 2021, the Court will also, as of 1 July 2021, publish the names of administrative secretaries.
53. This information is published once the Terms of Reference have been transmitted to, or approved by, the Court (or after the case management conference in expedited proceedings) and updated in the event of a change in the arbitral tribunal's composition or party representation (without however mentioning the reason for the change).
54. This information remains on the ICC website after the closure of the arbitration unless the concerned individual requests erasure in accordance with applicable data protection laws and regulations.
55. The parties may jointly request the Court to publish additional information about a particular arbitration in which they are involved.

C - Publication of Awards, Procedural Orders, Dissenting and/or Concurring Opinions

56. Publicising and disseminating information about arbitration has been one of ICC's commitments since its creation and an instrumental factor in facilitating the development of trade worldwide.
57. ICC awards and/or orders, as well as any dissenting and/or concurring opinions made as of 1 January 2019 ("ICC awards and related documents"), may be published according to the following provisions.
58. The Secretariat will inform the parties and arbitrators, during the proceedings and at the time of notification of any final award made as of 1 January 2019, that the final award, as well as any other awards and/or orders, as well as dissenting and/or concurring opinions made in the case, may be published in their entirety, including the names of the parties and of the arbitrators, no less than two years after the date of said notification. The parties may agree to a longer or shorter time period for publication. Prior to publication, the Secretariat will send the documents to be published to the parties and/or their representatives for their information by using the contact details indicated in the award or any other contact details subsequently provided.
59. At any time before publication, any party may object to publication or require that any award and related documents be in all or part anonymised (removal of names and any contextual data that may lead to identification of individuals, parties or disputes) or pseudonymised (replacement of any name by one or more artificial identifiers or pseudonyms), in which case they will not be published or will be anonymised or pseudonymised. If a party requires anonymisation or pseudonymisation, it will be upon the parties to agree on the redactions or accept the redactions proposed by the Secretariat. ICC endeavours its best efforts to ensure the non-identification of parties by publishing anonymised excerpts. At any time, any individual or entity may also convey to the Secretariat that it does not wish, as a general policy, any ICC award and related documents to which it is a party to be published, in which case none of these awards or decisions will be published. However, ICC cannot be aware of all publicly available data, and possible results of combined information from various sources that may lead to potential identification of the case or the dispute.

60. In case of a confidentiality agreement, order or explicit provisions under the law of the place of arbitration covering certain aspects of the arbitration or of the award, publication will be subject to the parties' specific consent.
61. The Secretariat may anonymise or pseudonymise personal data included in the award and/or orders, dissenting and/or concurring opinions as necessary pursuant to the applicable data protection laws and regulations. Arbitral tribunals will be encouraged to include in their award a list of the names of relevant individuals or entities involved in the case.
62. The Secretariat may, in its discretion, exempt ICC awards and related documents from publication.
63. Parties and/or their representatives should consider the relevant applicable laws and establish whether any legal requirements or limitations may prevent the publication of ICC awards and related documents and inform the arbitral tribunal and the Secretariat accordingly. Any information in this regard available to the Secretariat will be communicated to the parties and the arbitral tribunal.
64. Non-confidential ICC awards and related documents may be consulted for research purposes (Articles 1(5) and 1(6) of Appendix II) and selected extracts thereof may be published in anonymised form, no less than two years after the closing of the case.

V - Conduct of Participants in the Arbitration

65. Arbitral tribunals, parties and their representatives are expected to abide by the highest standards of integrity and honesty, to conduct themselves with honour, courtesy and professionalism, and to encourage all other participants in the arbitral proceedings to do the same.
66. Arbitrators shall discharge their duties in accordance with the Rules, be at all times independent and impartial, avoid any behaviour that may create a conflict of interest, a bias or an appearance of bias, and not allow any consideration that is extraneous to the case to influence their decisions.
67. Parties and arbitral tribunals are encouraged, where appropriate, to adopt or otherwise be guided by the IBA Guidelines on Party Representation in International Arbitration.
68. An arbitrator or prospective arbitrator shall not engage in *ex parte* communications with a party or party representative concerning the arbitration. However:
 - a. A prospective arbitrator may communicate with a party or party representative on an *ex parte* basis to determine his or her expertise, experience, skills, availability, acceptance and the existence of potential conflicts of interest.
 - b. To the extent that the parties so agree, arbitrators may communicate with parties or party representatives on an *ex parte* basis for the purpose of the selection of the president of the arbitral tribunal.
 - c. In all such *ex parte* communications, an arbitrator or prospective arbitrator shall refrain from expressing any views on the substance of the dispute.

VI - Emergency Arbitrator

69. Pursuant to Article 29 and Appendix V (“Emergency Arbitrator Provisions”), a party that needs urgent interim or conservatory measures (“Emergency Measures”) which cannot await the constitution of an arbitral tribunal may make an application to the Secretariat.
70. The Emergency Arbitrator Provisions apply only to parties that are signatories to the arbitration agreement that is relied upon for the application or successors to such signatories.
71. The Emergency Arbitrator Provisions do not apply if:
 - a. the arbitration agreement under the Rules was concluded before 1 January 2012;
 - b. the parties have opted out of the Emergency Arbitrator Provisions; or
 - c. the arbitration agreement upon which the arbitration is based arises from a treaty.
72. Parties may agree that the Emergency Arbitrator Provisions apply to arbitration agreements concluded before 1 January 2012.
73. Parties who wish to file an Application for Emergency Measures (“Application”) should inform the Secretariat as soon as possible and preferably before submitting the Application. If the Application precedes the Request for Arbitration, parties should send an email to: emergencyarbitrator@iccwbo.org. If the Application relates to an ongoing arbitration, parties shall contact the ICC case management team to which the arbitration has been assigned.
74. Upon receipt of the Application, the President of the Court will consider whether the Emergency Arbitrator Provisions apply. If the President of the Court considers that they apply, the Secretariat will transmit the Application to the responding party. If the President of the Court considered that they do not apply, the Secretariat will inform the parties that the Emergency Arbitrator proceedings shall not take place. Without prejudice to the parties’ status in the main arbitral proceedings, the President of the Court may consider that the Emergency Arbitrator Provisions apply only with respect to some of the parties. In that case, the Secretariat will inform the parties accordingly and transmit a copy of the Application to all parties.
75. The President of the Court will terminate the Emergency Arbitrator proceedings if the Secretariat has not received a Request for Arbitration within 10 days from the Secretariat’s receipt of the Application, unless the Emergency Arbitrator determines that a longer period of time is necessary (Article 1(6) of Appendix V).
76. The President of the Court shall appoint the Emergency Arbitrator in as short a time as possible, normally within two days from the Secretariat’s receipt of the Application.
77. Emergency Arbitrators are subject to the requirements set forth in section III. A challenge against an Emergency Arbitrator must be made within three days from the challenging party’s receipt of the notification of the Emergency Arbitrator appointment or from the date when that party was informed of the facts and circumstances on which the challenge is made if such date is subsequent to the appointment notification. The Court may decide the challenge, after affording all parties and the Emergency Arbitrator an opportunity to comment in writing, before or after the Emergency Arbitrator Order (“Order”) is rendered.
78. The Emergency Arbitrator’s first task is to establish a procedural timetable as soon as possible, normally within two days from the transmission of the file to the Emergency Arbitrator (Article 5 of Appendix V). In doing so, the Emergency Arbitrator must ensure that the responding party is granted time to respond to the Application.

79. The Order must be made no later than 15 days from the date on which the file was transmitted to the Emergency Arbitrator (Article 6(4) of Appendix V). The President of the Court may extend that time limit pursuant to a reasoned request or on his or her own initiative (Article 6(4) of Appendix V).
80. The Court will not scrutinise the draft Order. The Emergency Arbitrator is however encouraged to seek guidance from the Secretariat, in particular by submitting his/her draft Order for review prior to the expiration of the time limit set out in Article 6(4) of Appendix V. The [Emergency Arbitrator Order Checklist](#) may also provide guidance to the Emergency Arbitrator in drafting the Order.
81. The Order may be signed and notified in electronic form if the Emergency Arbitrator so decides after having consulted the parties.
82. The effects of the Order are set forth in Article 29(2), (3) and (4) of the Rules, and Articles 6(6), (7) and (8) of Appendix V.

VII - Conduct of the Arbitration

A - Advance on Costs

83. Together with the Request for Arbitration, a claimant must pay the filing fee of US\$ 5,000. Such payment is non-refundable and shall be credited to the claimant's portion of the advance on costs (Article 1(1) of Appendix III). Notification of the Request for Arbitration to respondent will be subject to prior payment of the filing fee (Article 4(5)).
84. Upon receipt of the Request for Arbitration, the Secretary General may fix a provisional advance (Article 37(1)). The provisional advance is intended to cover the costs of the arbitration until the Terms of Reference have been established or, when the Expedited Procedure Provisions apply, until the case management conference.
85. Payment of the provisional advance is considered a partial payment by the claimant of the advance on costs subsequently fixed by the Court. The Secretariat will transmit the file to the arbitral tribunal, once constituted, only upon payment of the provisional advance (Article 16).
86. The advance on costs is fixed by the Court and is intended to cover the arbitral tribunal's fees and arbitration-related expenses, as well as the ICC administrative expenses (Article 37 of the Rules and Article 1(4) of Appendix III). The advance on costs includes (i) an amount between the minimum and maximum fee suggested under the scales, (ii) a reasonable amount for tribunal-related expenses and (iii) the amount of administrative expenses under the scales. Whenever the Court fixes or readjusts the advance on costs, a financial table is provided to the parties and arbitrators for information and guidance. The Court fixes the fees of the arbitrators at the end of the arbitration based on factors detailed in section XIV. Such fees may be less than the entire advance on costs.
87. The Court may readjust the advance on costs if the development of the arbitration so requires (Article 37(5)). The arbitral tribunal should inform the Secretariat of any developments in the value and complexity of the arbitration or any other issues it considers relevant. To this end, the Secretariat will also request from the arbitrators a periodical report on their activities, which should include a description of the tasks performed, an estimate of the amount of time spent on each of those tasks, and any other information related to those tasks that the arbitrators may deem relevant. For this purpose, arbitrators should use the ICC form, [Statement of Time](#)

[and Travel for Work Done](#), or if arbitrators use time sheets as part of their normal professional activities, they may provide the Secretariat with such time sheets. Arbitrators are also encouraged to send such reports to the Secretariat on their own initiative after completing a procedural milestone or when requesting advances on fees or the readjustment of the advance on costs. Every arbitrator should provide information regarding his or her time spent, exclusive of the time spent by the administrative secretary, if any. In addition, the arbitral tribunal may report the time spent by the administrative secretary, if it wishes to do so.

88. Whenever the amount in dispute is significant, the Court may initially fix the advance on costs at an amount that will not cover all of the ICC administrative expenses and arbitrator fees and expenses. In such cases, the Secretariat will inform the parties and arbitrators not to assume that the advance covers the costs until the end of the arbitration and that future readjustments of the advance on costs are therefore likely. To take into account the developments in the case, the Court may make further readjustments to the advance on costs as the case progresses.
89. The parties must pay the advance on costs in accordance with paragraphs 2, 3, 4 and 5 of Article 37 and paragraphs 4, 5, 6, 7, 8 and 9 of Article 1 of Appendix III. As a general rule, payments must originate directly from the parties to the case. However, ICC will accept payments made by duly mandated representatives, provided that the legal relationship between the third-party payer and the party in the case is evidenced. Should the legal document not be considered as satisfactory by ICC's banks pursuant to their legal obligations under French law, the payment received by ICC may be cancelled and the lack of relevant information reported to the relevant regulatory authorities. The party making the payment must pay all bank charges and/or taxes applicable to the payment of the advance on costs. However, bank transfers made within the European Economic Area (EEA) are subject to shared banking fees.
90. Where claims are made under Articles 7 and 8, the Court may either (1) fix several advances on costs, or (2) fix one advance on costs and establish the respective portions to be paid by each party (Article 37(4)). The parties may also agree to a different apportionment.
91. The arbitral tribunal should clarify with the parties whether any hearing costs should be covered by the advance on costs or settled directly between the parties and the hearing facility. If hearing costs are to be included in the advance on costs, the arbitral tribunal should provide the Secretariat with an estimate of such costs. Thereafter, the Secretariat may examine whether it is appropriate to invite the Court to readjust the advance on costs.

B - Expeditious and Efficient Conduct of the Arbitration

92. The arbitral tribunal and the parties must conduct the arbitration in an expeditious and cost-effective manner, having regard to the complexity and value of the dispute (Article 22(1)).
93. In order to ensure effective case management, the arbitral tribunal, after consulting the parties, shall adopt the procedural measures that it considers appropriate, provided that they are not contrary to any agreement of the parties (Article 22(2)). Such measures may include one or more of the case management techniques referred to in Appendix IV to the Rules. In particular, the arbitral tribunal may encourage the parties to consider settling all or part of their disputes, either by negotiation or through any form of amicable dispute resolution method, such as mediation under the ICC Mediation Rules.
94. The arbitral tribunal should give due consideration to the ICC Commission on Arbitration and ADR report entitled [Controlling Time and Costs in Arbitration](#).

C - Hearings – Virtual Hearings

95. Pursuant to Article 26(1), a hearing shall be held if any of the parties so requests or, failing such a request, if the arbitral tribunal on its own motion decides to hear the parties.
96. A party's request for a hearing pursuant to Article 26(1) may be satisfied by the organisation of at least one hearing and does not require that each single question in dispute be discussed at a hearing. After consulting the parties, the arbitral tribunal may decide to organise several hearings if doing so results in greater efficiency.
97. The arbitral tribunal may decide, after consulting the parties, to conduct any hearing either by physical attendance or by remote means of communication, such as videoconference ("virtual hearing"), or both.
98. The organisation of a virtual or hybrid hearing may be particularly appropriate for case management conferences (Article 24(4)), as well as for any hearing in Expedited Procedure Provisions (see section VIII), Emergency Arbitrator Provisions (see section VI), or with respect to dispositive motions (see paragraph 109).
99. The arbitral tribunal must take any decision to hold an evidentiary hearing by remote means of communication rather than by physical attendance after careful consideration of all relevant circumstances, including the nature of the hearing, the possible existence of travel constraints, the planned duration of the hearing, the number of participants and of witnesses and experts to be examined, the size and complexity of the case, the need for the parties to properly prepare for the hearing, the costs and the gains of efficiency that may be expected by resorting to virtual means of communication, and whether rescheduling the hearing would entail unwarranted or excessive delays.
100. 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. In making such a determination, arbitral tribunals may take into account their broad procedural authority under Article 22(2), to, after consulting the parties, adopt such procedural measures as they consider appropriate, provided that they are not contrary to any agreement of the parties.
101. Any virtual hearing requires a consultation between the arbitral tribunal and the parties with the aim of implementing measures – often called a cyber-protocol – that are needed in order to comply with any applicable data privacy regulations. Such measures should also deal with the privacy of the hearing and the protection of the confidentiality of electronic communications within the arbitration proceeding and any electronic document platform.
102. In preparation for a virtual hearing, and in order to ensure that parties are treated with equality and that each party is given a full opportunity to present its case, the arbitral tribunal should consider:
 - Different time zones in fixing the hearing dates, start and finish times, breaks and length of each hearing day;
 - Logistics of the location of participants, including, but not limited to, the total number of participants, the number of remote locations, the extent to which any participants will be in the same physical venue, the extent to which members of the arbitral tribunal may be in the same physical venue as one another and/or any other participants, and the availability and control of break out rooms;
 - Use of real-time transcript or another form of recording;

- Use of interpreters, including whether simultaneous or consecutive;
- Procedures for verifying the presence of and identifying all participants, including any technical administrator;
- Procedures for the taking of evidence from fact witnesses and experts to ensure that the integrity of any oral testimonial evidence is preserved;
- Use of demonstratives, including through shared screen views; and
- Use of an electronic hearing bundle hosted on a shared document platform that ensures access by all participants.

103. [A Checklist for a Protocol on Virtual Hearings, and Suggested Clauses for Cyber-Protocols and Procedural Orders Dealing with the Organisation of Virtual Hearings](#) are available on the ICC website.
104. The [ICC Hearing Centre in Paris](#) offers technical support and assistance to arbitral tribunals seeking to better understand the options for virtual hearing and electronic bundle facilities and how to operate those facilities in a manner that best preserves the integrity of the arbitral process, preserves confidentiality and ensures proper data protection. In addition, ICC has signed [Memoranda of Understanding](#) with other hearing centres in most major arbitral seats and is able to coordinate with arbitral tribunals in order to access virtual hearing facilities on offer at those centres and obtain necessary technical support and guidance. Additional information may be obtained by emailing: infohearingcentre@iccwbo.org.
105. Various videoconference platform options are available for virtual hearings. A third-party comparative table of available options can be found [here](#). These range from customised hearing solutions offered by some hearing centres and/or service providers to licenced publicly available platforms to free-to-use public platforms. Customised or licensed, fee-based videoconference platforms may offer greater security, confidentiality and data protection than free use, public platforms.
106. Arbitral tribunals should consult with the parties to ensure that any video sharing platform that is used for virtual hearings is licensed and is set to maximum security settings. ICC has licensed access to the following videoconference platform options: Microsoft Teams, Vidyocloud and Skype for Business. ICC technical support is available remotely to assist arbitral tribunals with using such platforms, joining a meeting (or hearing), operating in-meeting audio and video functions, and operating screen sharing functions. Other platforms that have been used in recent cases include Zoom, Blue Jeans and GoToMeeting.
107. Various documents sharing platforms are available for electronic bundles. Like videoconference platforms, these also range from customised hearing solutions offered by some hearing centres and/or service providers (such as Opus, Transperfect and XBundle) to licensed publicly available platforms to free-to-use public platforms. Customised or licensed, fee-based document sharing platforms may offer greater security, confidentiality and data protection than free-to-use, public platforms.
108. ICC does not endorse or make any representation or warranty with respect to any third-party vendor mentioned in this Note. Parties, their representatives and arbitral tribunals should conduct their own due diligence as to their suitability in any given case.

D - Expeditious Determination of Manifestly Unmeritorious Claims or Defences

109. This section includes guidance as to how an application for the expeditious determination of manifestly unmeritorious claims or defences may be addressed within the broad scope of Article 22.

110. Any party may apply to the arbitral tribunal for the expeditious determination of one or more claims or defences, on grounds that such claims or defences are manifestly devoid of merit or fall manifestly outside the arbitral tribunal's jurisdiction ("application"). The application must be made as promptly as possible after the filing of the relevant claims or defences.
111. The arbitral tribunal has full discretion to decide whether to allow the application to proceed, taking into consideration any circumstances it considers to be relevant, including the stage of the proceedings and the need to ensure time and cost efficiency.
112. If the arbitral tribunal allows the application to proceed, it shall promptly adopt the procedural measures it considers appropriate, after consulting the parties. The responding party or parties shall be given a fair opportunity to answer the application. Further presentation of evidence will only be allowed in exceptional circumstances.
113. The arbitral tribunal shall decide the application as promptly as possible, consistent with the nature of the application, and may state the reasons for its decision in as concise a fashion as possible. The decision may be in the form of an order or award. In either case, the arbitral tribunal may decide on the costs of the application pursuant to Article 38 or reserve this decision to a later stage.
114. The Court will scrutinise any award made on an application for expeditious determination, typically within one week of receipt by the Secretariat.

E - Protection of Personal Data

115. ICC recognises the importance of effective and meaningful personal data protections when it collects and uses such personal data as data controller pursuant to data protection laws and regulations, including 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"). To that effect, ICC has published the [ICC Data Privacy Notice for ICC Dispute Resolution Proceedings](#).
116. In order to comply with the Court's (i) mission to disseminate and improve international knowledge of arbitration and (ii) obligations under the Rules, ICC, the Court and its Secretariat collect and process the personal data of the parties, their representatives, the arbitrators, the administrative secretary, the witnesses, the experts, and any other individuals that may be involved in any capacity in the arbitration. In performing their duties under the Rules, arbitral tribunals also have to collect and process such personal data. For this purpose, such personal data may be transferred by or to the various offices of the Secretariat in and out of the European Union.
117. The parties, their representatives, the arbitrators, the administrative secretary, the witnesses, the experts, and any other individuals who may be involved in any capacity in the arbitration, acknowledge that collecting, transferring and archiving personal data is necessary for the purposes of arbitration proceedings, and that said data may be published in case of a publication of an award, procedural order and dissenting and/or concurring opinion.
118. The parties shall ensure that (i) 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, and (ii) applicable data protection regulations, including the GDPR, are complied with.

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.
120. Parties and arbitrators shall ensure that only personal data that are necessary and accurate for the purposes of the arbitration proceedings are processed. Any individual whose data is collected and processed in the context of an arbitration may at any time request the appropriate data controller to exercise notably his right of access and that inaccurate data be corrected or suppressed, according to the applicable data protection laws and regulations.
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 the information being processed or transferred, including whether it includes personal data or sensitive business, proprietary or confidential information. To that effect, arbitral tribunals and parties are encouraged to consult the [Report on the Use of Information Technology in International Arbitration](#) by the ICC Commission on Arbitration and ADR.
122. 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.
123. Once an arbitration is completed, arbitrators may retain the personal data that were processed during the proceedings for as long as they keep the case file in their archives pursuant to applicable laws. Such duration shall be communicated to the parties and the Secretariat.
124. At the end of each case, the Secretariat shall retain, pursuant to its obligations (Article 1(7) of Appendix II), personal data pertaining to the case. Such data shall be archived. Other personal data that are no longer necessary for ICC to discharge its obligation under the Rules shall be destroyed or erased.
125. The archives of the Court and its Secretariat are also kept for scientific and historical research purposes. Access to archives and their publication either in full, as excerpts redacted or not, or in a summarised form, may be allowed by the President or the Secretary General of the Court in furtherance of ICC's mission to disseminate and improve international knowledge of arbitration.

F - Time Limits under the Rules

126. The Rules contain time limits which arbitrators and parties must endeavour to comply with, including:

- a. **Terms of Reference:** must be established within one month from the transmission of the file to the arbitral tribunal (Article 23(2)). Terms of Reference are not required in arbitrations under the Expedited Procedure Provisions.
- b. **Case management conference:** must be convened (1) when drawing up the Terms of Reference or as soon as possible thereafter (Article 24(1)), or (2) no later than 15 days after the date on which the file was transmitted to the arbitral tribunal in arbitrations under the Expedited Procedure Provisions.
- c. **Procedural timetable:** must be established during or immediately following the case management conference and transmitted to the Court and the parties (Article 24(2)).
- d. **Closing of the proceedings:** must be done as soon as possible after the last hearing on matters to be decided in an award, or the filing of the last authorised submissions concerning such matters (Article 27).
- e. **Date for submission of draft awards:** must be indicated to the Secretariat and the parties when the arbitral tribunal closes the proceedings (Article 27). Draft final awards must be submitted to the Secretariat three months after the last substantive step in the arbitration for three-member arbitral tribunals and two months for sole arbitrators (see paragraph 153).
- f. **Final award:** must be rendered within six months from the date of the last signature added to the Terms of Reference or the date of notification of their approval (Article 31(1)) or otherwise the time limit fixed by the Court based upon the procedural timetable, or six months from the date of the case management conference in arbitrations under the Expedited Procedure Provisions.

VIII - Expedited Procedure Provisions

A - Scope of the Expedited Procedure Provisions

127. By agreeing to the Rules, the parties agree that Article 30 of the Rules and Appendix VI (collectively, the “Expedited Procedure Provisions”) takes precedence over any contrary terms of the arbitration agreement.
128. The Expedited Procedure Provisions apply if:
- a. the arbitration agreement was concluded after 1 March 2017; and
 - b. the amount in dispute does not exceed US\$ 2,000,000 if the arbitration agreement was concluded from 1 March 2017 to 31 December 2020, and US\$ 3,000,000 if the arbitration agreement was concluded on or after 1 January 2021; and
 - c. the parties have not opted out of the Expedited Procedure Provisions in the arbitration agreement or at any time thereafter. Agreements to opt out should express in specific terms the parties’ intention not to subject themselves to the Expedited Procedure Provisions. It is not sufficient, to that effect, that the parties have referred in the arbitration agreement to a three-member arbitral tribunal, or have adopted time limits that depart from those provided by the Expedited Procedure Provisions. It is recommended that parties wishing to opt out of the Expedited Procedure Provisions use the standard clauses contained in the Rules.
129. The Expedited Procedure Provisions also apply, irrespective of the date of conclusion of the arbitration agreement or the amount in dispute, if the parties have agreed to opt in. Such opt in agreements can be concluded in the arbitration agreement or by separate or subsequent agreement. It is recommended that the parties wishing to opt in to the Expedited Procedure Provisions use the standard clauses contained in the Rules.

130. The Court may at any time, upon request of a party or on its own motion after consulting the arbitral tribunal and the parties, decide that the Expedited Procedure Provisions no longer apply (Article 1(4) of Appendix VI). In particular, the Court may use such power if new circumstances arise that make the Application of the Expedited Procedure Provisions no longer appropriate.

B - Determination of the Amount in Dispute for the Purpose of the Application of the Expedited Procedure Provisions

131. For purposes of deciding whether the Expedited Procedure Provisions apply, the amount in dispute includes all quantified claims, counterclaims, cross-claims and claims pursuant to Articles 7 and 8. Claims relating to interest and costs will not be considered to that effect.
132. Pursuant to the Rules (Articles 4(3), 5(5)(b), 7(2), 7(4), 8(2) and 8(3)), the parties shall quantify their claims and, to the maximum extent possible, provide an estimate of the value of any non-monetary claims.
133. For purposes of deciding whether the Expedited Procedure Provisions apply, the Secretariat will consider the quantifications or estimates submitted by the parties.
134. Expedited Procedure Provisions do not apply in cases involving declaratory or non-monetary claims the value of which cannot be estimated, unless it appears that such non-monetary claims merely support a monetary claim or that they do not add significantly to the complexity of the dispute.
135. If an objection is raised as to the applicability of the Expedited Procedure Provisions, the matter will be decided by the Court after giving an opportunity to the other parties to state their views.
136. Any submission by the parties with respect to the applicability of the Expedited Procedure Provisions shall be made in the Request for Arbitration and in the Answer, or within any time limit subsequently given by the Secretariat.
137. Any decision made by the Secretariat or by the Court as to the amount in dispute for purposes of deciding whether the Expedited Procedure Provisions apply does not bind the arbitral tribunal when deciding the substance of the dispute.
138. In assessing costs pursuant to Article 38(5), the arbitral tribunal may take into account whether a party has artificially inflated its claims, thereby preventing the Expedited Procedure Provisions from applying.

C - Scales

139. In all cases conducted under the Expedited Procedure Provisions, the Scales of Administrative Expenses and Arbitrator's Fees for the Expedited Procedure apply as indicated in paragraph 179 and any advance on costs will be fixed on this basis. The arbitrator's fees pursuant to these scales are 20% less than under the general scales.
140. After receipt of the Request for Arbitration on the basis of the Expedited Procedure Provisions and the amount in dispute at that stage, the Secretary General will fix the provisional advance. The provisional advance may be readjusted on the basis of the general scales if the Expedited Procedure Provisions ultimately do not apply.

D - Information to the Parties

141. Pursuant to Article 1(3) of Appendix VI, the Secretariat will inform the parties that the Expedited Procedure Provisions apply (1) upon receipt of the Answer to the Request for Arbitration, (2) upon expiry of the time limit for the Answer, or (3) at any relevant time thereafter.
142. If a Request for Joinder is filed or claims pursuant to Article 8 are made, the Secretariat will inform the parties as to the applicability of the Expedited Procedure Provisions after receiving the Answer to the Request for Joinder or to such claims or upon expiry of the time for such Answer.

E - Constitution of the Arbitral Tribunal

143. According to Article 2 of Appendix VI, the Court may appoint a sole arbitrator notwithstanding any contrary provision of the arbitration agreement.
144. By submitting to arbitration under the Rules, the parties agree that any reference of disputes to three arbitrators in their arbitration agreement is subject to the Court's discretion to appoint a sole arbitrator if the Expedited Procedure Provisions apply.
145. When the Expedited Procedure Provisions apply, the Court will normally appoint a sole arbitrator in order to ensure that the arbitration is conducted in an expeditious and cost-effective manner.
146. The Court may nevertheless appoint three arbitrators if appropriate in the circumstances. In all cases, the Court will invite the parties to comment in writing before taking any decision and shall make every effort to ensure that the award is enforceable at law.
147. If the Court decides that the Expedited Procedure Provisions no longer apply (see paragraph 130), the arbitral tribunal will normally remain in place, unless the Court finds, at the request of the parties or on its own initiative, after giving an opportunity to the parties and the arbitral tribunal to state their views, that circumstances exist which justify replacing and/or reconstituting the arbitral tribunal. If the Court decides to reconstitute the arbitral tribunal and proceed with a three-member arbitral tribunal, the Court may consider appointing the individual who was acting as sole arbitrator as president of the arbitral tribunal.

F - Proceedings before the Arbitral Tribunal

148. In conducting the arbitration under the Expedited Procedure Provisions, the arbitral tribunal shall act fairly and impartially and ensure that each party has a reasonable opportunity to present its case.
149. Under the Expedited Procedure Provisions, the arbitral tribunal has discretion to adopt such procedural measures it considers appropriate to conduct the arbitration in accordance with the time limits established therein. In particular, after giving an opportunity to the parties to state their views, the arbitral tribunal may: (1) decide the case on documents only, with no hearing and no examination of witnesses, (2) decide not to allow requests for the production of documents and/or (3) limit the number, scope and length of submissions.

G - Award

150. The final award shall be made within six months from the date of the case management conference. The Court expects arbitral tribunals acting under the Expedited Procedure Provisions to conduct the procedure in such a way as to comply with this deadline, with no need for extensions. If an extension nonetheless is needed, the arbitral tribunal shall submit a reasoned application to the Court.
151. Any award under the Expedited Procedure Provisions must be reasoned. In such arbitrations, it is particularly appropriate to keep the factual and/or procedural sections of the award to what the arbitral tribunal considers necessary for the understanding of the award, and state the reasons of the award in as concise a fashion as possible.

IX - Efficiency in the Submission of Draft Awards to the Court

A - General Practice

152. The Court expects arbitral tribunals to render awards within six months from the establishment of the Terms of Reference, or within the time limit fixed by the Court for this purpose (Article 31(1)).
153. While the Court has the power to extend such time limits, sole arbitrators are expected to submit draft awards within two months, and three-member arbitral tribunals within three months after the last substantive hearing on matters to be decided in the award, or the filing of the last written submissions concerning such matters (excluding cost submissions), whichever is later (Article 27).
154. Whenever the arbitral tribunal has conducted the arbitration expeditiously, the Court may increase the arbitrators' fees above the amount that it would otherwise consider fixing.
155. Where the draft award is submitted after the time referred to in paragraph 153, the Court may lower the fees as set out below, unless it is satisfied that the delay is attributable to factors beyond the arbitrators' control or to exceptional circumstances, and without prejudice to any other measures that it may take, such as replacing one or more of the arbitrators:
 - If the draft award is submitted for scrutiny up to 7 months after the last substantive hearing or written submissions (excluding cost submissions), whichever is later, the fees that the Court would otherwise consider fixing are reduced by 5% to 10%.
 - If the draft award is submitted for scrutiny up to 10 months after the last substantive hearing or written submissions (excluding cost submissions), whichever is later, the fees that the Court would otherwise consider fixing are reduced by 10% to 20%.
 - If the draft award is submitted for scrutiny more than 10 months after the last substantive hearing or written submissions (excluding cost submissions), whichever is later, the fees that the Court would otherwise consider fixing are reduced by 20% or more.
156. In deciding on the above, the Court may also take into account any delays incurred in the submission of one or more partial awards.

B - Practice under the Expedited Procedure Provisions

157. Under the Expedited Procedure Provisions, the arbitral tribunal must render the final award in six months from the case management conference, with extensions to be granted only in limited and justified circumstances.
158. The Court considers that compliance with such time limit is of the essence under the Expedited Procedure Provisions.
159. In order to effectively comply with such time limit, an arbitral tribunal acting under the Expedited Procedure Provisions is expected to submit its draft award within five months from the case management conference.
160. Whenever the arbitral tribunal has conducted the arbitration expeditiously, the Court may increase the arbitrators' fees above the amount that it would otherwise consider fixing.
161. Where the draft award is submitted after the time referred to in paragraph 159, the Court may lower the fees as set out below, unless it is satisfied that the delay is attributable to factors beyond the arbitrators' control or to exceptional circumstances, and without prejudice to any other measures that it may take, such as replacing one or more of the arbitrators:
 - If the draft award is submitted for scrutiny up to 7 months after the case management conference, the fees that the Court would otherwise fix are reduced by 5% to 10%.
 - If the draft award is submitted for scrutiny up to 10 months after the case management conference, the fees that the Court would otherwise fix are reduced by 10% to 20%.
 - If the draft award is submitted for scrutiny more than 10 months after the case management conference, the fees that the Court would otherwise fix are reduced by 20% or more.

X - Closing of the Proceedings and Scrutiny of Awards

A - Closing of the Proceedings

162. An arbitral tribunal should declare the proceedings closed as soon as possible after the last hearing or the last authorised submission filed in relation to matters to be decided in an award, whether final or otherwise (Article 27). Upon doing so, the arbitral tribunal must inform the Secretariat and the parties of the date by which it expects to submit the draft award for the Court's scrutiny (Article 34).

B - Scrutiny Process

163. The scrutiny process carried out by the Court with the assistance of its Secretariat is a unique and thorough procedure designed to ensure that all awards are of the best possible quality and more likely to be enforceable. Before a draft award is submitted to the Court for scrutiny, it is reviewed first by the Counsel of the team in charge of the arbitration that has followed the proceedings, and then by the Secretary General, the Deputy Secretary General or the Managing Counsel. For certain arbitrations, generally those involving state parties or dissenting opinions, a Court member will draft a report with recommendations on the draft award.

164. All draft awards are scrutinised in Committees, composed of three Court members (Article 4 of Appendix I), in Special Committees (Article 5 of Appendix I) or in Single-member Committees (Article 6 of Appendix I). Draft awards scrutinised during a Special Committee include, but are not limited to, arbitrations involving (i) a state or a state entity, (ii) dissenting opinions by one or more arbitrators and/or (iii) matters in which a Committee Session was unable to reach a unanimous decision or otherwise makes a referral to the Special Committee.

C - Information to the Parties

165. Upon receipt of a draft award, the Secretariat informs the parties and the arbitral tribunal that the draft will be scrutinised at one of the Court's next Sessions.
166. After scrutiny, the Secretariat informs the parties and the arbitral tribunal that the award either was approved or will be further scrutinised at one of the Court's next Sessions.
167. Once a draft award is approved subject to comments, the Secretariat will request the arbitral tribunal to indicate the time needed to finalise the draft award and, to the extent possible, inform the parties of the estimated time of notification of the award. The arbitral tribunal must finalise the award as expeditiously as possible.

D - Timing of Scrutiny

168. Any draft award submitted to a three-member Committee will be scrutinised within three to four weeks of receipt by the Secretariat. Awards submitted to a Special Committee (which are typically held once a month on the last Thursday of the month) will be scrutinised within five or six weeks, depending on when the draft is submitted, or earlier if a Special Committee can be scheduled to expedite scrutiny.
169. If the Expedited Procedure Provisions apply, any draft award submitted to the Court will be scrutinised as soon as possible, and in any event no later than two to three weeks of receipt by the Secretariat. The Court may decide, in exceptional circumstances, that any award made under the Expedited Procedure Provisions will be scrutinised by a Committee consisting of one member of the Court (Article 4(6) of Appendix II).
170. If the scrutiny process is delayed, other than by circumstances that are beyond the Court's control, the Court's administrative expenses will be reduced by up to 20%, depending on the length of the delay.
171. For purposes of assessing whether the draft was submitted timely, the Court considers the first submission of the draft award to the Court for approval, irrespective of whether that draft of the award is approved.

XI - ICC Award Checklist

172. The [ICC Award Checklist](#) is intended to provide arbitrators with guidance for the drafting of awards and is not an exhaustive, mandatory or otherwise binding document. It should not be thought to reflect the opinion of the members of the Court or of its Secretariat, but is intended to facilitate the arbitrators' work. It may not be published or used for any purpose other than the conduct of ICC arbitrations. The Checklist is not exhaustive of issues that may be raised by the Court under Article 34.

XII - Treaty-based Arbitrations

173. In view of the specific nature of treaty-based arbitration, for the sake of transparency and subject to any considerations of confidentiality, prospective arbitrators should provide a *curriculum vitae* including a complete list of the treaty-based cases in which they participated as arbitrator, expert, or counsel.
174. The parties may agree to adopt the UNCITRAL Rules on Transparency in Treaty-based Investor-State Arbitration, either in full or in part, or to be guided by the same in adopting similar rules. In such case, the Secretariat may act as the repository of published information.
175. In treaty-based cases, Articles 13(6) (requirement of nationality, see paragraph 45), and 29(6)(c) (non-availability of the Emergency Arbitrator provisions, see paragraph 71(c)), apply.
176. In treaty-based cases, the President, and/or Vice-Presidents of the Court and Court members with experience in treaty-based arbitration, will scrutinise the draft award.
177. In derogation from section IV(C) (see paragraph 58), and unless a party objects, a treaty-based award will be published within six months from its notification.

XIII - Submissions by *Amici Curiae* and non-disputing parties

178. Pursuant to Article 25(3), the arbitral tribunal may, after consulting the parties, adopt measures to allow oral or written submissions by *amici curiae* and non-disputing parties.

XIV - Arbitral Tribunal's Fees and Administrative Expenses

A - Scales

179. Arbitrators' fees in ICC arbitration are calculated on an ad valorem basis pursuant to Article 4 of Appendix III, which provides two scales: (i) the general scales of administrative expenses and arbitrator's fees, and (ii) the scales applicable to the cases conducted under the Expedited Procedure Provisions. Parties and arbitrators are encouraged to consult the [Cost Calculator](#) on the ICC website and the applicable scales contained in Article 4 of Appendix III.

B - Advance on Fees

180. The Court fixes the arbitrators' fees at the end of the arbitration, although advances on fees may be granted upon request and the completion of certain milestones in the arbitration.

C - Allocation among Arbitral Tribunal Members

181. In arbitrations conducted by a three-member arbitral tribunal, arbitrators may agree on the fee allocation for each arbitrator and inform the Secretariat as early as possible in the proceedings of their agreement. Arbitrators may modify their agreement in the course of the proceedings. Unless the Court is advised in writing that the arbitral tribunal has agreed on a different allocation, the Court will fix the arbitrators' fees so that the president receives between 40% and 50% of the total fees, and each co-arbitrator receives between 25% and 30%, as the case may be, although the Court may decide upon a different allocation based on the circumstances. Unless otherwise agreed, the same allocation applies to any advances on fees granted by the Court.

D - Fixing of Fees

182. The Court fixes arbitrators' fees. Separate fee arrangements between the parties and arbitrators are not permitted.
183. The Court normally fixes arbitrators' fees within the limits specified by the scales or, in exceptional circumstances, in an amount that is higher or lower than that resulting from those limits. An exceptionally high amount in dispute may be considered as such a circumstance in deciding whether to fix the arbitrators' fees below the limits specified in the scales.
184. Pursuant to Article 2 of Appendix III, when fixing the arbitrators' fees, the Court takes into consideration the diligence and efficiency of the arbitrator, the time spent, the rapidity of the proceedings, the complexity of the dispute and the timeliness of the submission of any draft award. To this end, the Secretariat will request from the arbitrators the information specified in paragraph 87.
185. The Court may fix the arbitrators' fees below the average, including at the minimum under the scales, where the amount in dispute is high or very high, or towards the maximum where the amount in dispute is low or very low. The amount of the advance on costs is not an indication of the final amount of the arbitrators' fees.
186. As a matter of guidance only, the Court may proceed as follows when fixing the fees of the arbitrators or granting advances on fees when the advance on costs has been fixed on the basis of the average fee:
- | | | |
|----|--|------------------------------------|
| a. | Case Management Conference
(in Expedited Procedure cases) | 35% of minimum fee |
| b. | Terms of Reference established | 50% of minimum fee |
| c. | A partial award issued / major hearing | Minimum fee |
| d. | Multiple partial awards | Between 50% of average and average |
| e. | Final award issued | Average fee |
187. The Court may depart from this guidance depending on the circumstances of each arbitration, the criteria set forth in Article 2 of Appendix III, and the practice set forth in section IX(A).

E - Replacement

188. When fixing the fees of an arbitrator who has been replaced, the Court takes into consideration the nature of and reasons behind the replacement, the milestones completed in the arbitration, and the work expected to be completed by the successor. The Court may deduct the replaced arbitrator's fees from those of the successor.

F - Administrative Expenses

189. The Court normally fixes the ICC administrative expenses in accordance with the scale. In exceptional circumstances, the Court may fix them in an amount that is higher or lower than that resulting from the application of such scale, provided that they do not normally exceed the maximum amount of the scale.
190. As a matter of guidance only, when fixing the ICC administrative expenses, the Court may proceed as follows:

a.	File transmitted to the arbitral tribunal	25%
b.	Case Management Conference (in Expedited Procedure cases)	35%
c.	Terms of Reference established	50%
d.	Partial award(s) or other major procedural milestones completed	75%
e.	Final award	100%

191. The Court may depart from this guidance, depending on the circumstances of each arbitration. In any event, the figures above do not include abeyance fees, or additional advances to cover Article 36 applications.

G - Declaration to French Tax Authorities

192. Depending on the applicable law, ICC may be required to declare the amount of fees, including advances on fees, paid to any arbitrator during each calendar year, as well as any expenses reimbursed during the same period.

XV - Decisions as to the Costs of the Arbitration

193. Arbitral tribunals may make decisions as to costs, except for those to be fixed by the Court, and order payment thereof at any time during the proceedings (Article 38(3)).
194. In making decisions as to costs, the arbitral tribunal may take into account such circumstances as it considers relevant, including the extent to which each party has conducted the arbitration in an expeditious and cost-effective manner (Article 38(5)). Further information on this topic may be found in the ICC Commission Report [Decisions on Costs in International Arbitration](#).
195. If the parties withdraw their claims or the arbitration terminates before the rendering of a final award, the Court fixes the fees and expenses of the arbitrators and the ICC administrative expenses. If the parties have not agreed upon the allocation of the costs of the arbitration or other relevant issues with respect to costs, the arbitral tribunal shall decide such matters (Article 38(6)). If the arbitral tribunal has not been constituted at the time of the withdrawal, any party may request the Court to proceed with the constitution of the arbitral tribunal so that it may make decisions as to costs.

XVI - Signature of Terms of Reference and Awards – Notification of Awards

196. Subject to any applicable mandatory law requirements, and unless the parties agree otherwise, (1) the Terms of Reference may be signed by each party and member of the arbitral tribunal in counterparts, and (2) such counterparts may be scanned and communicated to the Secretariat pursuant to Article 3 by email or any other means of telecommunication that provides a record of the sending thereof. An original of the signed Terms of Reference must be provided to the Secretariat.
197. Awards signed and dated by the arbitral tribunal are sent to the Secretariat for notification to the parties (Article 35(1)). The award must be signed and dated on or after the date of the Court Session at which the draft award was approved. The date of the award is the date on which the last arbitrator signed.

198. Unless the parties have agreed to electronic notification of the award (see paragraph 199), the arbitral tribunal must provide the Secretariat with the required number of originals (unbound) requested by the Secretariat. The arbitral tribunal must also provide the Secretariat with a PDF of the signed original by email. The Secretariat will send a courtesy copy of the PDF of the award to the parties by email ahead of the notification of originals. The sending of a courtesy copy by email does not trigger any of the time limits under the ICC Rules of Arbitration.
199. Subject to any applicable mandatory law requirements, the parties may agree that (1) any award may be signed by the members of the arbitral tribunal in counterparts, and/or (2) such counterparts may be assembled in a single electronic file and notified to the parties by the Secretariat by email or any other means of telecommunication that provides a record of the sending thereof, pursuant to Article 35.
200. Paragraphs 197 to 199 apply *mutatis mutandis* to additional awards, *addenda* and decisions.

XVII - Correction and Interpretation of Awards

201. If the arbitral tribunal decides to correct the award on its own initiative, pursuant to Article 36(1), it should inform the parties and the Secretariat of its intention to do so and grant a time limit to the parties to comment in writing. The arbitral tribunal should submit the draft *addendum* to the Court for scrutiny within 30 days of the date of the award.
202. Upon receipt of an Article 36(2) application, the Secretariat will assess whether, based on the circumstances of the case, including whether the application appears to fall within the scope of Article 36(2) to request the Court to fix an advance to cover additional fees and expenses of the arbitral tribunal and additional ICC administrative expenses (Article 2(10) of Appendix III). The arbitral tribunal should not address an application until the application is transmitted to the arbitral tribunal by the Secretariat.
203. Even if the Court has not asked for an additional advance upon filing of the application, it can nevertheless take a decision on costs at the time of the scrutiny and make the notification of the *addendum* or the decision contingent upon the payment by one or both parties of the costs so fixed by the Court.
204. Upon receipt of the application from the Secretariat, the arbitral tribunal should grant the other parties a short time limit, normally not exceeding 30 days, for comments. The arbitral tribunal may however grant a shorter time limit to the parties depending on the circumstances of the case, after consideration of all relevant circumstances.
205. Parties should be mindful of the limited scope of Article 36(2), which does not allow to revise or vary determinations that have been finally made in the award.
206. The arbitral tribunal shall submit its draft determination to the Court for scrutiny no later than 30 days following the expiration of the time limit granted for comments. Should the arbitral tribunal require an extension of such time limit, it should inform the Secretariat.
207. The arbitral tribunal's determination can take one of four forms:

- a. **Addendum:** if the arbitral tribunal decides to correct or interpret the award. An Addendum constitutes part of the award.
- b. **Decision:** if the arbitral tribunal decides that the award does not need to be corrected or interpreted and does not take a decision on costs. A Decision does not constitute part of the award.
- c. **Addendum and Decision:** if there are two or more applications and the arbitral tribunal decides to correct or interpret the award on the basis of one or more, but not all applications.
- d. **Decision and addendum on costs:** if the arbitral tribunal decides that the award does not need to be corrected or interpreted, but takes a decision on costs related to the application. An addendum on costs constitutes part of the award.

208. All decisions and *addenda* must state the reasons upon which they are based. They must also include operative conclusions ("dispositif") or a finding either rejecting or granting the application as the case may be. For further guidance about what should be included in a draft decision or *addendum*, see the [ICC Checklist on Correction and Interpretation of Arbitral Awards](#). The Court will scrutinise all draft decisions and *addenda*. Upon approval by the Court, the arbitral tribunal shall sign the decision or *addendum* and send it to the Secretariat for notification to the parties as per paragraphs 197 to 199.

209. In all cases, the arbitral tribunal must first ensure that mandatory rules of law at the place of arbitration do not exclude the correction or interpretation of an award by the arbitral tribunal.

XVIII - Additional Awards

210. Pursuant to Article 36(3), a party may apply for an additional award as to claims which the arbitral tribunal has omitted to decide. A claim that the arbitral tribunal has omitted to decide is a claim that was made in the arbitration and that the arbitral tribunal, based on the parties' submissions, should have decided in the award.

211. Any application for an additional award must be made to the Secretariat within 30 days of the receipt of the award by the applicant party. After the receipt of an application for an additional award, the arbitral tribunal must grant an opportunity to the other parties to comment on the application. Because there may be objections as to the admissibility of the application or the need to make submissions, granting a time-limit to the other parties is required in all cases.

212. Because an application for an additional award refers to claims that were made in the arbitration and that the arbitral tribunal omitted to decide, it is expected that the parties will have already made submissions on said claims in the arbitration, and there should be no need for lengthy additional submissions. Accordingly, Article 36(3) provides that the other parties should be granted a short time-limit, normally not exceeding 30 days, to comment on the application. The arbitral tribunal may however decide, upon consideration of all relevant circumstances, to grant a shorter or longer time-limit to the parties. Similarly, although assessing an application for an additional award would normally not require the taking of additional evidence, the arbitral tribunal may decide to allow the production of additional evidence as appropriate.

213. Paragraphs 197 to 199, 202 and 203 apply *mutatis mutandis*.

214. Where the relevant national law or court practice provide specific circumstances in which an arbitral tribunal may render certain decisions other than corrections or interpretation regarding an award which has already been approved and notified or additional awards, such situations will be treated in the spirit of the Rules and this Note.

XIX - International Sanctions Regulations

215. International sanctions regulations may apply to an arbitration. Parties and arbitrators must consult the [Note to Parties and Arbitral Tribunals on ICC Compliance](#).

XX - Administrative Secretaries

216. This section sets out the policy and practice of the Court regarding the appointment, duties and remuneration of arbitral tribunal administrative secretaries or other assistants (“administrative secretaries”), appointed on or after 1 August 2012.
217. Administrative secretaries can provide a useful service to the parties and arbitral tribunals in ICC arbitration. While principally engaged to assist three-member arbitral tribunals, an administrative secretary may also assist a sole arbitrator. Administrative secretaries can be appointed at any time during an arbitration.

A - Appointment

218. If an arbitral tribunal envisages the appointment of an administrative secretary, it must consider carefully whether in the circumstances of that particular arbitration, such an appointment would be appropriate.
219. Administrative secretaries must satisfy the same independence and impartiality requirements as those which apply to arbitrators under the Rules. ICC staff members are not permitted to serve as administrative secretaries.
220. There is no formal process for the appointment of an administrative secretary. However, before any steps are taken to appoint an administrative secretary, the arbitral tribunal must inform the parties of its intention to do so. For this purpose, the arbitral tribunal must submit to the parties the proposed administrative secretary’s *curriculum vitae*, together with a declaration of independence and impartiality, an undertaking on the part of the administrative secretary to act in accordance with the present Note and an undertaking on the part of the arbitral tribunal to ensure that this obligation on the part of the administrative secretary are met.
221. The arbitral tribunal must make clear to the parties that they may object to such proposal and that an administrative secretary shall not be appointed if a party has raised such an objection.

B - Duties

222. Administrative secretaries act upon the arbitral tribunal’s instructions and under its strict and continuous supervision. At all times, the arbitral tribunal is responsible for the administrative secretary’s conduct during the arbitration.
223. Under no circumstances may the arbitral tribunal delegate its decision-making functions to an administrative secretary or rely on an administrative secretary to perform on its behalf any of the essential duties of an arbitrator. Likewise, the tasks entrusted to an administrative secretary, such as the preparation of written notes or memoranda, will not release the arbitral tribunal from its duty to personally review the file and/or draft itself any arbitral tribunal’s decision.
224. An administrative secretary may, consistently with the above, perform organisational and administrative tasks such as:

- transmitting documents and communications on behalf of the arbitral tribunal;
- organising and maintaining the arbitral tribunal's file and locating documents;
- organising hearings and meetings and liaising with the parties in that respect;
- drafting correspondence to the parties and sending it on behalf of the arbitral tribunal;
- preparing for the arbitral tribunal's review drafts of procedural orders as well as factual portions of an award, such as the summary of the proceedings, the chronology of facts, and the summary of the parties' positions, provided that such procedural orders and portions of the award are subsequently reviewed by the arbitral tribunal itself;
- attending hearings, meetings and deliberations; taking notes or minutes or keeping time;
- conducting legal or similar research; and
- proof-reading and checking citations, dates and cross-references in procedural orders and awards, as well as correcting typographical, grammatical or calculation errors.

225. The administrative secretary may not act, or be required to act, in such a manner as to prevent or discourage direct communications between the arbitrators, between the arbitral tribunal and the parties, or between the arbitral tribunal and the Secretariat.

226. When in doubt about which tasks may be performed by an administrative secretary, the arbitral tribunal or the administrative secretary should consult the Secretariat.

C - Disbursements

227. The arbitral tribunal may seek reimbursement from the parties of the administrative secretary's justified reasonable expenses disbursed for hearings and meetings.

D - Remuneration

228. With the exception of the administrative secretary's justified reasonable expenses, the engagement of an administrative secretary should not pose any additional financial burden on the parties.

229. The arbitral tribunal must pay any remuneration due to the administrative secretary out of the total fees paid to all arbitrators, such that the fees of the administrative secretary will not increase the total costs of the arbitration.

230. The arbitral tribunal may not seek from the parties any form of remuneration for the administrative secretary's activity. Direct arrangements between the arbitral tribunal and the parties on the administrative secretary's fees are strictly prohibited. Because the fees of the arbitral tribunal are established on an *ad valorem* basis, any remuneration to be paid to the administrative secretary is deemed to be included in the arbitral tribunal's fees.

XXI - Arbitrator's Expenses

A - How to Submit a Request for Expenses

231. The Secretariat will reimburse expenses upon receipt of a request. Expense reimbursement claims must be supported by original receipts, in order for the Secretariat to carry out its accounting responsibilities and, from time to time, to provide the parties with comprehensive statements of expenses incurred by arbitrators.

B - When to Submit a Request for Expenses

232. Arbitrators should submit their requests for the reimbursement of expenses and/or the payment of *per diem* allowances, together with any required supporting documentation as specified below, **as soon as possible after expenses are incurred**. This will help ensure that the advance on costs paid by the parties is adequate to cover the costs of the arbitration.
233. All requests for the reimbursement of expenses and/or the payment of *per diem* allowances relating to any period prior to the submission of the draft final award must be provided at the latest when the draft final award is submitted to the Secretariat. Three-member arbitral tribunals should co-ordinate their submission of requests for reimbursement of expenses and/or payment of *per diem* allowances in order to ensure that they reach the Secretariat no later than the draft final award. Requests for the reimbursement of expenses and/or the payment of *per diem* allowances submitted **after the Court has approved the final award will not be taken into account by the Court when fixing the costs of the arbitration and will not be paid**, save in exceptional circumstances as decided by the Secretary General.
234. In the event of the withdrawal of all claims or the termination of the arbitration before the rendering of a final award, all requests for the reimbursement of expenses and/or the payment of *per diem* allowances must be submitted within the time limit granted by the Secretariat. Requests for the reimbursement of expenses and/or the payment of *per diem* allowances submitted after the Court has fixed the costs of arbitration will not be taken into account by the Court and will not be paid.

C - Travel Expenses

235. If required to travel for the purpose of an ICC arbitration, an arbitrator will be reimbursed for the actual travel expenses he or she incurs travelling from and returning to his or her usual place of business as indicated on the *curriculum vitae* filed for the relevant ICC arbitration. Travel expenses will be reimbursed in accordance with paragraphs 236 to 238.
236. A request for reimbursement of travel expenses must be accompanied by the originals of all receipts claimed or other proper substantiation if receipts are unavailable. Travel expenses that are not fully and comprehensively justified will not be reimbursed.
237. The reimbursement of travel expenses is subject to the following strict limits:
- a. Air travel: an airfare equivalent to the applicable standard business-class airfare.
 - b. Rail travel: the applicable first-class train fare.
 - c. Transport to and from airport(s) and/or train station(s): the applicable standard taxi fare.
 - d. Travel by private car: a flat rate for every kilometre driven, plus all necessary actual parking and toll charges incurred. The flat rate is US\$ 0.80 per kilometre.
238. Except for expenses claimed pursuant to paragraph 237(d), travel expenses will, where possible, be reimbursed in the currency in which they were incurred. An arbitrator may alternatively request reimbursement in US dollars provided that the request is accompanied by a statement of the US dollar amount and evidence of the exchange rate (for example, a printout from www.oanda.com). The date for the currency conversion should be the date on which the expense was incurred.

D - Per Diem Allowance

239. In addition to travel expenses, an arbitrator will be paid a flat-rate *per diem* allowance for every day of an ICC arbitration that he or she is required to spend outside his or her usual place of business as indicated on the *curriculum vitae* filed for the relevant ICC arbitration. The arbitrator is not required to submit receipts in order to claim the *per diem* allowance, but simply evidence of the travel for purposes of the arbitration.
240. If the arbitrator is not required to use overnight hotel accommodation, the flat-rate *per diem* allowance is US\$ 400.
241. If the arbitrator is required to use overnight hotel accommodation, the flat-rate *per diem* allowance is US\$ 1,200.
242. The applicable *per diem* allowance is deemed to cover fully all personal living expenses of whatever nature and of whatever actual value (other than travel expenses) incurred by an arbitrator. In particular, the applicable *per diem* allowance is deemed to cover the total cost of, *inter alia*:
- Accommodation
 - Meals
 - Laundry/ironing/dry cleaning and other housekeeping or similar services
 - Inner-city transport
 - Telephone calls, faxes, emails and other means of communication
 - Gratuities
243. For the avoidance of doubt, no *per diem* allowance will be paid in respect of time spent by an arbitrator travelling to or from the relevant destination.
244. Because the *per diem* allowance is deemed to cover all personal living expenses incurred by an arbitrator while outside his or her usual place of business on ICC arbitration business, the Secretariat will not reimburse expenses over and above the applicable *per diem* allowance under any circumstances.

E - General Office Expenses and Courier Charges

245. General office expenses and overheads incurred in the ordinary course of business by an arbitrator or an arbitral tribunal in connection with an ICC arbitration will not be reimbursed. However, an arbitrator or an arbitral tribunal may request to be reimbursed at cost for any courier, photocopying, fax or telephone charges incurred for the purposes of an ICC arbitration, provided such request is accompanied by detailed receipts.

F - Advance Payments on Expenses

246. An arbitrator may request an advance payment of travel expenses and/or the applicable *per diem* allowance. If an advance is granted, the arbitrator must subsequently submit the relevant supporting documentation to the Secretariat, including all receipts and a statement of working days and nights spent outside of his or her usual place of business on ICC arbitration business.

XXII - Administrative Services

A - Deposit of Funds other than the Advance on Costs for Arbitration

247. ICC may provide arbitrators and parties who expressly so request in writing a service allowing funds to be deposited, in the course of an arbitration, into an account administered by ICC for the purpose of paying an advance on VAT due on the arbitrators' fees or an advance to cover fees and expenses of any expert appointed by the arbitral tribunal, or for escrow purposes.
248. When arbitrators and parties avail themselves of this service and ICC consents to provide it, ICC acts as the depositary of the funds. ICC receives funds from one or more parties who have been instructed accordingly by an arbitrator (president or member of an arbitral tribunal on behalf of the other arbitral tribunal members, or sole arbitrator) and makes the payments from the account at the request of the arbitrator.
249. ICC acts as depositary of funds related to:
- a. VAT, taxes, charges and imposts applicable to arbitrators' fees
 - b. Experts
 - c. Escrow accounts
250. This service is available to arbitrators and parties from any country.
251. The deposit accounts are administered solely in US dollars or in Euros, unless otherwise decided.
252. The deposit accounts do not yield interest for the parties or the arbitrators.

Step 1: Request for a Deposit Account

Any arbitrator wishing to use this service must inform the Secretariat in writing and request ICC to act as depositary of funds to be paid by one or more parties as an advance on the VAT due on the arbitrators' fees or an advance to cover fees and expenses of any expert appointed by the arbitral tribunal, or for escrow purposes.

The initiative of requesting the opening of a deposit account, calling deposits, and making payments from the amounts deposited lies solely with the arbitrators.

Arbitrators are responsible for ensuring that payments are made in compliance with applicable laws and banking practices.

Step 2: Estimation of Amounts

The arbitrator determines the funds to be paid by one or more parties into a deposit account.

If, in the course of an arbitration, the amount of the advance on costs is increased pursuant to a decision of the Court, this step may be repeated. Likewise, if, in the course of the arbitration, the amount of the funds deposited to cover the fees and expenses of any expert or the amount of the funds deposited into an escrow account is increased pursuant to a decision of the arbitral tribunal, this step may be repeated.

Step 3: Funds to be Deposited

The arbitrator requests one or more parties to pay the funds and sets a time limit in which to do so.

The Secretariat will provide the party/parties with the relevant banking instructions.

As a general rule, payments in ICC arbitration cases must originate directly from parties to the case. ICC will accept payments made by duly mandated representatives, provided that the legal relationship between the third-party payer and the party in the case is evidenced. Should the legal document not be considered as satisfactory by ICC's banks pursuant to their legal obligations under French law, the payment received by ICC may be cancelled and the lack of relevant information reported to the relevant regulatory authorities. The party making the payment must pay all bank charges and/or taxes applicable to the payment of the advance on costs. However, bank transfers made within the European Economic Area (EEA) are subject to shared banking fees.

Step 4: Acknowledgement of Payments and Administration

The Secretariat confirms to the arbitrator and the parties receipt of the amounts paid by the party/parties.

If the arbitrator receives no confirmation from the Secretariat of receipt of payment by the party or parties, it is up to the arbitrator to renew his or her request for payment and to fix a time limit for this purpose.

ICC administers the funds on behalf of the arbitrator.

Step 5: Payments

The arbitrator requests ICC to make payments from the funds deposited by the parties.

Payments are made by ICC within the limits of the funds deposited.

Step 6: Balance of Account

At the end of the arbitration the Secretariat seeks instructions from the arbitrator with regard to closing the deposit account. On the basis of the information provided by the arbitrator and in accordance with his or her instructions, the Secretariat closes the deposit accounts and returns to the party or parties any amounts remaining from the funds deposited with ICC.

After advising the arbitrator, ICC may close the deposit account if no balance remains. The account will be closed even if a request by the arbitrator for the payment of funds is still outstanding.

B - Deposits for VAT, Taxes, Charges and Imposts Applicable to Arbitrators' Fees

253. Payments made by ICC to arbitrators do not include Value Added Tax (VAT) or other taxes or charges and imposts of the same nature that may be applicable to the arbitrator's fees (Article 2(13) of Appendix III). Parties have a duty to pay such VAT or similar taxes or charges due pursuant to applicable law. The recovery of any such charges or taxes is a matter solely between the arbitrator and the parties. Such parties' duty does not include the payment of any

other taxes, charges and imposts that may be applied to the arbitrator's fees, such as, but not limited to, income or company tax, professional license fees, charges or retentions applied by the arbitrator's bar association, pension or social security regime, as well as banking charges and commissions. In case of doubt, arbitrators should consult the Secretariat.

254. Arbitrators subject to VAT may request in writing to use the service described above allowing them to have the funds corresponding to their estimate of the VAT due on their fees and expenses (hereinafter "Fees") administered by ICC.
255. This service is completely separate from, and has no effect on, the procedure for paying advances as set out in the Rules. Should the parties fail to pay the VAT on the arbitrators' fees, this cannot be invoked by the arbitrators before the Court, for instance as a ground for suspending the arbitration.
256. If the president of an arbitral tribunal requests a VAT advance on behalf of all those members of the arbitral tribunal who are subject to VAT, the president must inform the Secretariat of the breakdown of this advance arbitrator-by-arbitrator.
257. Arbitrators bear sole responsibility for ensuring that the procedure described above complies with the tax laws and regulations applicable to the exercise of their profession as arbitrators, including the payment of their fees. Arbitrators are encouraged to check the basis on which they should calculate the amount of VAT due.
258. ICC acts exclusively as depositary and is not in a position to advise arbitrators on tax law issues.
259. The arbitrator determines the amount of VAT on his or her fees according to the rules that apply at the place where he or she is taxable.
260. Arbitrators may use the [Cost Calculator](#) on the ICC website to estimate the amount of the fees that may be payable. Such amounts, however, are only indicative of the fees that they may ultimately receive, which may be in a higher or lesser amount. Arbitrators should also be mindful that the breakdown of fees between the members of the arbitral tribunal (from 40% to 50% for the president, and 25% to 30% for each co-arbitrator) which is referred to in this Note is given merely as a guide and may be varied by the Court.
261. Any invoice issued by an arbitrator to a party for fees and, as the case may be, VAT applicable to those fees should be for the portion of the fees and the amount of tax payable by that party. No invoice should in principle be issued by an arbitrator to ICC, save in special circumstances to be discussed in advance with the Secretariat.
262. When drawing up his or her invoice, the arbitrator requests ICC to pay the amount corresponding to the VAT on the fees due by the party. This applies at the time of the final award, but also in the event that the Court decides to pay an advance on fees to arbitrators who reside in countries where, under local tax law, VAT becomes payable to the tax authorities when fees are paid in advance.

XXIII - VAT payable on ICC Administrative Expenses

263. ICC administrative expenses do not include French Value-Added Tax ("VAT"; Article 2(14) of Appendix III). As of 1 January 2021 and to the extent that VAT is applicable, ICC administrative expenses will be subject to VAT. Accordingly, ICC administrative expenses may be increased by the corresponding amount at the prevailing rate as further set out in the [Explanatory Note](#)

on VAT Applicable on ICC Administrative Expenses. The applicable rate under French tax law is currently 20%. The Secretariat's requests for payment of the advance on costs will result in the issuance of invoices that will cover all amounts requested (i.e. amounts to cover ICC administrative expenses alongside the advance on arbitrators' fees and expenses).

264. The basic scheme under the Rules with respect to ICC administrative expenses is that the parties are required to pay them (alongside the arbitrators' fees and expenses) through advance payments on costs requested by the Secretariat (see section VII(A)). Where applicable, VAT will be charged on the requested advance payments corresponding to the ICC administrative expenses. Indicatively, VAT will be charged and invoiced on:

- a. The filing fee (Article 4(4)(a) of the Rules and Article 1(1) of Appendix III).
- b. The portion of requested payments corresponding to ICC administrative expenses of:
 - (i) Advances on costs (Article 37 of the Rules and Article 1 of Appendix III);
 - (ii) Additional advances on costs (Article 36(5) of the Rules and Article 2(11) of Appendix III); and
 - (iii) Costs of the Emergency Arbitrator Proceedings (Article 7(1) of Appendix V).
- c. Any abeyance fee (Article 2(7) of Appendix III).

ICC will not charge VAT on the portion of the advance on costs corresponding to the arbitrators' fees and expenses. The invoicing and collection of VAT due by the parties to the arbitrators, where applicable, is a matter solely between the arbitrators and the parties (see paragraph 253).

XXIV - Assistance with the Conduct of the Arbitration

A - Conduct of the Arbitration

265. The Secretariat may assist parties and arbitral tribunals with the conduct of the arbitration, in particular:

- a. **Deposit of documents:** the Secretariat may in certain circumstances act as depositary of documents.
- b. **Conference calls:** the Secretariat may assist arbitral tribunals in organising conference calls with the parties and, when required, participate in such calls.
- c. **Administrative secretaries:** the Secretariat may assist arbitral tribunals in identifying administrative secretaries for appointment pursuant to section XX.
- d. **Model documents:** the Secretariat may provide arbitral tribunals with model documents related to the conduct of the arbitration, in particular terms of reference and procedural timetables.
- e. **Transparency:** pursuant to paragraph 55, the Court may, at the request of parties, publish on its website or otherwise make available to the public information or documents related to an ICC arbitration that is subject to transparency rules or regulations.
- f. **ADR:** the ICC International Centre for ADR provides parties and arbitral tribunals with a number of services relevant to ongoing ICC arbitrations, in particular the proposal and appointment of experts (see section XXVI).
- g. **ICC Commercial Crime Services:** the Secretariat may assist parties and arbitral tribunals in liaising with ICC Commercial Crime Services (for more information visit: www.icc-ccs.org).

B - Hearings and Meetings

266. The Secretariat may assist parties and arbitral tribunals with the organisation of hearings and meetings, in particular:
- a. **ICC Hearing Centre in Paris (France):** the ICC Hearing Centre offers flexible packages and a range of specialised facilities and services for hearings and meetings. Parties and arbitral tribunals may contact the Secretariat for further information or visit the website at www.icchearingcentre.org. By reserving a room at the ICC Hearing Centre for an ICC arbitration, parties and arbitrators accept that their contact details be communicated by the Secretariat to the ICC Hearing Centre for the sole purpose of their booking.
 - b. **Other hearing facilities:** ICC has agreements with other hearing facilities around the globe. Parties and arbitral tribunals may consult the Secretariat for further information.
 - c. **Court reporting and translation:** the Secretariat may provide parties and arbitral tribunals with information regarding court reporting and translation services.
 - d. **Visas and other authorisations:** the Secretariat may issue letters to facilitate the obtaining of visas or other authorisations for individuals participating in a hearing or meeting related to an ICC arbitration.
 - e. **Hotels:** ICC negotiates preferential rates with a number of hotels in Paris and other jurisdictions. Parties and arbitral tribunals may consult the Secretariat for further information.

C - Sealed Offer(s)

267. The Secretariat may assist parties to put information relating to certain unaccepted settlement offers, and related communication (commonly referred to as “Sealed Offer(s)”), before an arbitral tribunal. The Secretariat may also assist with any counter-offer(s) made as Sealed Offer(s) by the offeree.
268. The arbitral tribunal should consider consulting the parties at an early stage (e.g. at the first case management conference pursuant to Article 24) and inviting them to agree on a procedure for the possible use of Sealed Offer(s) in the arbitration. Absent initiative by the arbitral tribunal in this respect, any party is free to raise this issue.
269. The Secretariat will keep any such communication regarding Sealed Offer(s) confidential from the arbitral tribunal until all issues of liability and quantum have been resolved.
270. To obtain the Secretariat’s assistance, the following procedure should be followed:
- a. At any point after the Secretariat has transmitted the Request for Arbitration to the respondent(s), any party to the arbitration may send to the Secretariat a copy of an offer of settlement previously made to any other party in the arbitration, but not accepted, that is marked “without prejudice save as to costs”. The offer should be submitted to the Secretariat in a sealed envelope marked “without prejudice save as to costs”. An accompanying letter should request the Secretariat to treat the sealed envelope as confidential and not to transmit it to the arbitral tribunal until the latter has resolved all issues of liability and quantum and is ready to consider the allocation of costs. The original recipient of the offer should be copied on all communications to the Secretariat related to the Sealed Offer(s).

- b. Following receipt of correspondence pursuant to paragraph (a), the Secretariat will inform:
 - (i) the sending party (copying the other party) that the sealed envelope will be held in confidence, and
 - (ii) the original recipient of the offer (copying the other party) of the circumstances in which the sealed envelope may be submitted to the arbitral tribunal and solicit any comments.
- c. Further correspondence arising from the original offer (including, for example, any counter-offers) which is sent by a party to the Secretariat in a sealed envelope marked “without prejudice save as to costs” will be held by the Secretariat on the same basis as the original offer.
- d. At an appropriate stage in the proceedings, the Secretariat will write to the arbitral tribunal to inform it that the Secretariat is holding correspondence exchanged between the parties that is potentially relevant to its determination of costs under Article 38. The Secretariat will request the arbitral tribunal to: (i) inform the Secretariat in writing whether it accepts to receive the Sealed Offer(s); and in such case to (ii) inform the Secretariat in writing once it has completed its deliberations on all liability and quantum issues and is ready to apportion costs.
- e. If the arbitral tribunal accepts to receive the Sealed Offer(s), it should refrain from closing the proceedings pursuant to Article 27 to the extent necessary to allow the parties to make further submissions on costs.
- f. Once the arbitral tribunal has informed the Secretariat that it is ready to apportion costs under Article 38, the Secretariat will send to the arbitral tribunal all the correspondence marked “without prejudice save as to costs” held by the Secretariat. Once the arbitral tribunal has received this information, it shall open the sealed envelopes and provide copies of any documents contained therein to the parties.
- g. The arbitral tribunal will decide whether any further procedural steps are necessary or whether it can proceed to allocate costs pursuant to Article 38. For the avoidance of doubt, the arbitral tribunal retains discretion to decide what weight, if any, should be given to correspondence marked “without prejudice save as to costs” and received from the Secretariat.
- h. Once the arbitral tribunal has completed its deliberations on costs, it will add its decision as to the allocation of costs to the draft final award, which will be submitted to the ICC Court for scrutiny pursuant to Article 34.

XXV - Post-Award Services

271. In accordance with Article 35, the Secretariat shall assist the parties in complying with whatever formalities may be necessary, in particular:
- a. Certified copies of awards, Terms of Reference, correspondence or any other document issued or approved by the Secretariat or the Court.
 - b. Notarisation by the ICC notary public in Paris of signatures of members of the Secretariat who certify copies of documents.
 - c. Certificates.
 - d. Non-certified copies of documents from the case file, limited in size and number.
 - e. Letters reminding parties of their obligation to comply with the award.
272. As some post-award services take time and preparation, parties should allow sufficient time when requesting such assistance from the Secretariat.

XXVI - International Centre for ADR

A - ICC Mediation Rules

273. Parties are free to settle their dispute amicably prior to or at any time during an arbitration. They may wish to consider conducting an amicable dispute resolution procedure administered by the ICC International Centre for ADR (“Centre”) pursuant to the ICC Mediation Rules, which, in addition to mediation, allow for the use of other amicable settlement procedures. The Centre can also assist the parties in finding a suitable mediator. The appointment of a mediator by the Centre made at the joint request of all the parties in an ongoing ICC arbitration is provided free of charge.
274. Where appropriate, arbitrators may wish to remind the parties about the ICC Mediation Rules.
275. Further information is available from the Centre at +33 1 49 53 29 03 or adr@iccwbo.org.

B - ICC Expert Rules

276. If a party requires the assistance of an expert, the Centre can, upon request, propose experts with a wide range of specialisations. The fee for this service is US\$ 5,000.
277. Likewise, if the arbitral tribunal requires the assistance of an expert, the Centre can, upon request, propose experts. This service is provided free of charge to arbitrators.
278. Further information is available from the Centre at +33 1 49 53 29 03 or adr@iccwbo.org.

XXVII - Dispatch of Materials to ICC and Customs Charges

279. Materials sent to ICC (correspondence, submissions, binders, tapes, CDs, etc.) must be sent exclusively as “Documentation”. No other description should be indicated on the transportation slip or waybill. Generally, documentation is not subject to customs taxes. Other material may be subject to taxes, which vary according to the origin, content and weight of such material. Customs charges, if any, will increase the costs of arbitration.



Commission on Arbitration and ADR
Leading Dispute Resolution Worldwide

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, -oceanos, 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 proceedings 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://jusmundi.com/en/icc-dispute-resolution-library>.

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 interoperability 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** (CIArb, 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-###
Other Applications	<i>Index of Legal Authorities-RLA-0001 to RLA-0023</i>
	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	Ask all attendees to turn on their cameras and verify visually who is in attendance. Review the participants list in the platform. If anyone has connected separately by audio, ensure the audio and video lines are merged by the host. Ensure the host re-names participants as necessary to show full names and roles (e.g. John Doe, Arbitrator and not jdoe).
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	Mute your microphone if you are not speaking. Address any planned early departures or late joining by individual participants to avoid disruption. Only one person may speak at a time. If chat or raise hand features are enabled, remind participants of agreed protocol. No unauthorised recording or screenshots.
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	Re-name yourself as necessary to show full name and role (e.g. John Doe, Claimant's Counsel). Mute your microphone if you are not speaking. Give notice of any planned early departures or late joining. Only one person may speak at a time. No unauthorised recording or screenshots.
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	For the purpose of this checklist, the following terms are defined as follows: > '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	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.
Other services offered by an OCMP	The platform should initially present general information to any visitor and user: > 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). .../...

Other services offered by an OCMP (continued)	> 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.
Terms and conditions of service	The OCMP's terms and conditions may be non-negotiable but must be acceptable to all Users of the platform. 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. <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).
Agreement and Commitment to use the OCMP for the arbitration	<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. <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. <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. <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. <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.)

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. ... / ...

Default rules for organisation of case information, folders and uploaded documents (continued)	<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. <u>Timetable</u>: all deadlines fixed in a procedure, any extension granted and if the expected performance was met. <u>Correspondence</u>: all correspondence uploaded by any User. <u>Submissions</u>: upload should only be made available to parties. <u>Exhibits</u>: upload should only be made available to parties. <u>Procedural orders</u>: upload should only be made available to the arbitral tribunal, and any administrative secretary. <u>Terms of reference and awards</u>: upload should only be made available to the arbitral tribunal, any administrative secretary. <u>Index of all documents</u>: all documents uploaded on the platform in a chronological order. <u>Common bundle</u>: if parties produce a common bundle for a hearing. <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. <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). <u>Referencing of documents</u>: when uploading Communications, the system should allow dropdown menus of standard information to be selected for uploading documents: > date format: yyyy-mm-dd for year-month-day > case reference used by a DRO or proposed by an OCMF > 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 with 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 at www.iccwbo.org and in the [ICC Dispute Resolution 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 170 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](#)



Commission on Arbitration and ADR
Leading Dispute Resolution Worldwide

Effective Management of Arbitration

**A Guide for In-House Counsel and Other
Party Representatives**

International Chamber of Commerce (ICC)
33-43 avenue du Président Wilson
75116 Paris, France
www.iccwbo.org

The views and suggestions contained in this guide originate from the ICC Commission on Arbitration and ADR and the widespread consultations conducted during the drafting of the guide. They should not be thought to represent views and suggestions of the ICC International Court of Arbitration or the ICC International Centre for ADR, nor are they in any way binding on either body.

Copyright © 2014, 2017
International Chamber of Commerce (ICC)

All rights reserved.

ICC holds all copyright and other intellectual property rights in this collective work. No part of this work may be reproduced, distributed, transmitted, translated or adapted in any form or by any means except as permitted by law without the written permission of ICC. Permission can be requested from ICC through copyright.drs@iccwbo.org.

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 ICC, registered in several countries.

Dépôt légal avril 2018

EFFECTIVE MANAGEMENT OF ARBITRATION

A Guide for In-House Counsel and Other Party Representatives

The purpose of this guide is to provide in-house counsel and other party representatives, such as managers and government officials, with a practical toolkit for making decisions on how to conduct an arbitration in a time- and cost-effective manner, having regard to the complexity and value of the dispute. The guide can also assist outside counsel in working with party representatives to that effect.

Reflecting the ICC's continuing efforts to provide arbitration users with means to ensure that arbitral proceedings are conducted effectively, the guide focuses on time and cost issues in the management of arbitration. While strategic considerations are of great importance in any arbitration and will have a significant impact on its management, they tend to be case-specific and are beyond the scope of this guide.

While the guide was conceived with the ICC Rules of Arbitration in mind, most of its contents, as well as the dynamic generated by it, can be used in any arbitration. The guide can be useful for both large and small cases.

EFFECTIVE MANAGEMENT OF ARBITRATION
TABLE OF CONTENTS

INTRODUCTION	03
SETTLEMENT CONSIDERATIONS	09
CASE MANAGEMENT CONFERENCE	13
TOPICSHEETS	15
1. Request for Arbitration	17
2. Answer and Counterclaims	21
3. Multiparty Arbitration	25
4. Early Determination of Issues	27
5. Rounds of Written Submissions	31
6. Document Production	33
7. Need for Fact Witnesses	37
8. Fact Witness Statements	41
9. Expert Witnesses (pre-hearing issues)	45
10. Hearing on the Merits (including witness issues)	51
11. Post-Hearing Briefs	59

INTRODUCTION

Arbitration is a dispute resolution mechanism that provides diverse users worldwide with a neutral forum, a uniform system of enforcement and the procedural flexibility that allows parties to tailor-make a procedure to suit their needs in each case. With a joint commitment to efficient management by parties, outside counsel and arbitral tribunals, it can achieve a time- and cost-effective resolution of a dispute. Without that commitment, the opposite can be true: the very flexibility of arbitration can lead to increased time and cost.

As arbitration has become more complex and the scrutiny of dispute resolution mechanisms has intensified, users have expressed the concern that arbitration is often too long and too expensive. One user has queried why a bridge can be built in one or two years but an arbitration to determine responsibility for delays and defects can take as long as three to four years. In light of the concerns of users, the ICC decided to address time- and cost-efficiency in arbitration head-on.

As a first step, in 2007, the ICC Commission on Arbitration (as it was then known) published its report on controlling time and costs in arbitration. Prior research covering a wide range of ICC cases had showed that on average:

- 82% of the costs of an arbitration were party costs, including lawyers' fees and expenses, expenses related to witness and expert evidence, and other costs incurred by the parties for the arbitration;
- 16% of the costs covered arbitrators' fees and expenses; and
- 2% of the costs covered ICC administrative expenses.

It followed that, to minimize costs, special emphasis needed to be placed on reducing the costs connected with the parties' presentation of their cases. The report developed a series of suggested concrete measures for each phase of the arbitration that can be used to reduce time and cost.

EFFECTIVE MANAGEMENT OF ARBITRATION

INTRODUCTION

Then, in 2009, the Commission began its revision of the ICC Rules of Arbitration. The revised Rules came into force on 1 January 2012.* One of the guiding principles for the revision was to improve the time- and cost-efficiency of arbitration. Among the provisions directed to that end is the requirement of an early case management conference during which the parties and the tribunal can establish an appropriate, time- and cost-effective procedure for the arbitration. The suggestions in the 2007 report, many of which are now included as an appendix to the Rules, may be used for that purpose.

The present guide is a continuation of that effort and is designed to help party representatives implement the new provisions and make appropriate decisions for effective case management. The guide will also assist outside counsel in working with party representatives to ensure well-planned and well-managed proceedings.

As noted above, arbitration rules permit flexibility and do not specify precisely how an arbitration is to be conducted. For example, there is nothing in the ICC Rules of Arbitration about the number of rounds of briefs, document production, the examination of witnesses, oral argument, post-hearing memoranda or bifurcation. The open-ended nature of the Rules enables the parties and the arbitral tribunal to tailor-make an effective procedure that suits the needs and particularities of each case. However, when studying the matter, the Commission came to the conclusion that too often the parties and tribunals do not tailor-make the procedure at an early stage, but rather apply boilerplate solutions or simply decide procedural matters piecemeal as the case progresses. This was found to increase time and cost in many arbitrations. Under the new case management provisions in Articles 22–24 of the Rules, which are specifically designed to address that problem, the process of tailor-making the procedure has now become a formal requirement.

* Those Rules have since been further revised to include, among other things, an expedited procedure for lower-value cases. Effective as of 1 March 2017, the newly revised Rules can be downloaded from the ICC website (www.iccwbo.org). In this guide, references to the Rules have been updated, where necessary.

Tailor-making the procedure so that the arbitration will be faster and cheaper is not inherently difficult to accomplish. The parties can agree upon faster and cheaper procedures and, failing their agreement, the arbitral tribunal has the power to determine such procedures after consultation with the parties. This will normally be done at the first case management conference. What is more challenging is determining the appropriate level of process and resources to match the value and complexity of the case. It is faster and cheaper to have one round of briefs rather than three, or to hold a three-day rather than a three-week hearing, but an extended opportunity to be heard will necessarily be given up. It is less expensive and less burdensome to present a witness by videoconference, but perhaps also less persuasive. The goal of each party is to present its case in a manner that is most likely to persuade the arbitral tribunal to find in its favour. The time and cost that a party should be willing to devote to that end will vary according to the importance, complexity and value of the dispute. For each phase of the arbitration, cost/risk/benefit decisions have to be made.

Appropriate time and cost decisions can be made when party representatives have a collaborative relationship with outside counsel and actively participate in the making of those decisions. Each party best knows its own internal processes, the value of the underlying transaction and what is ultimately at stake. It is the party's case, the party's risk and the party's money, so the party itself is in the best position to decide what level of risk to accept and what strategic decisions to make. Outside counsel can assist in reaching such decisions on the basis of an informed evaluation of the pros and cons of the available alternatives. In addition, arbitral tribunals play an important role by bringing their experience to bear in devising cost-effective procedures and encouraging all of the parties to assist in conducting the arbitration in an expeditious and cost-effective manner, as contemplated by Article 22(1) of the Rules.

CASE MANAGEMENT CONSIDERATIONS

As a general matter, party representatives should consider the following when managing an arbitration:

Early case assessment. Much time and cost can be saved by not litigating matters with low chances of success, or that are not worth the cost/time/distraction to its personnel. This should be analysed before an arbitration has begun; however, case assessment should also continue during the arbitration.

Maintaining realistic schedules. Setting up of a realistic schedule for the entire arbitration as early as possible and sticking to that schedule, unless there are serious reasons for not doing so, are essential to controlled and predictable proceedings. Parties will be able more accurately to foresee the date of the award and make appropriate financial plans. The arbitral tribunal also has an important role in establishing and maintaining a realistic schedule.

Establishing a tailor-made and cost-effective procedure. Using this guide, party representatives along with outside counsel can determine optimum procedures from the party's perspective. The question then is how to implement those procedures. First, one party may consult with the other party with a view to reaching agreement on the applicable procedures. Any such agreement must be applied pursuant to Article 19 of the Rules. If the parties cannot agree on one or more of the procedures, each can present its position to the arbitral tribunal prior to or during the case management conference. The arbitral tribunal will decide after hearing the parties.

Awareness of settlement procedures. Settlement procedures such as mediation, neutral evaluation and direct settlement discussions can occur at any time before or during an arbitration. As an arbitration progresses, views on the case and parties' needs may change, affecting the desirability and nature of a potential settlement. New facts may come to light, a partial award may be rendered, management changes may occur, and new perspectives in relations between the parties may emerge. The parties should continually reassess their case and determine whether, at any given point in time, there is an opportunity for a meaningful settlement.

STRUCTURE OF THE GUIDE

This guide is composed of three main parts, each of which is designed to assist in making effective time and cost decisions for an arbitration: first, a discussion of settlement considerations; second, a discussion of the case management conference; and third, a series of eleven topic sheets.

Each topic sheet deals independently with a specific step in the arbitration process where cost/risk/benefit decisions need to be made. The topic sheets are not intended to cover every aspect of an arbitration; rather, they are designed to provide a methodology for decision-making. They may also serve as a tool to assist in making appropriate decisions on each topic. The following topics are covered:

- Request for arbitration
- Answer and counterclaims
- Multiparty arbitration
- Early determination of issues
- Rounds of written submissions
- Document production
- Need for fact witnesses
- Fact witness statements
- Expert witnesses
- Hearing on the merits
- Post-hearing briefs

Each topic sheet is designed to serve as an executive summary and follows a standard format consisting of a series of separate sections. The first section presents the topic and identifies the issue(s); the second section sets out the options available to the parties for that topic; the third section discusses the pros and cons of the different options; the fourth section analyses the different choices from a cost/risk/benefit perspective; and the fifth section lists useful questions that will help to focus on the key decisions that need to be made. The list of questions could, for example, serve as a basis for discussion between party representatives and outside counsel regarding the choices that need to be made for that particular phase of the arbitration. Where useful, a final section contains other general points to consider.

EFFECTIVE MANAGEMENT OF ARBITRATION

The topic sheets are not prescriptive and do not provide any definitive answers but rather contain suggestions that can be used to stimulate discussion and decision-making. It is the hope of the Commission that these topic sheets will help in taking the appropriate cost/risk/benefit decisions that need to be made in order to conduct an expeditious and cost-effective arbitration, having regard to the complexity and value of the dispute.

SETTLEMENT CONSIDERATIONS

A negotiated settlement of the dispute can save a great deal of time and cost, and parties would be well advised to maintain focus on the availability of settlement opportunities before and throughout an arbitration. The case management techniques listed in Appendix IV (h) to the ICC Rules of Arbitration indicate that the arbitral tribunal may inform the parties that they are free to settle all or part of the dispute at any time and, where agreed with the parties, may take steps to facilitate a settlement, subject to enforceability considerations under applicable law.

WHETHER OR NOT TO SETTLE

This is a complex question that will depend on each individual case. It is necessary to weigh the chances of success in an arbitration against a series of factors including the costs, burden and distraction caused by the proceedings and the time required to obtain the result. The choice may be affected by matters of principle or the need to eliminate financial or other uncertainties. Additional considerations include:

Preservation of relationships. Parties to an arbitration may have an ongoing relationship which they wish to preserve. Settlement may support that relationship better than litigating the dispute.

Difficulties of enforcement. If a claimant anticipates difficulties in enforcing an arbitral award against a particular respondent, it should factor that difficulty into its assessment of the strength of its case. When enforcement is uncertain, a settlement for a lower amount may be appropriate.

Reasons not to settle. Various factors may militate against settlement. For example, a claimant may wish to obtain a precedent or guidance from a tribunal for use in future cases or may consider that a given settlement offer does not match the chances of success in an arbitration. A respondent may prefer not to settle in order to discourage other potential claimants from seeking a settlement or because it is concerned that a settlement may be interpreted as an admission of liability.

EFFECTIVE MANAGEMENT OF ARBITRATION SETTLEMENT CONSIDERATIONS

Importance of confidentiality. A settlement may be preferable to an arbitration that is not confidential. ICC arbitration proceedings will not be confidential unless the parties have so agreed, the tribunal has so ordered or applicable law so requires.

METHODS OF SETTLEMENT

If the parties have decided to explore settlement, various methods are available to them. They may seek a settlement on their own, with the assistance of counsel or with the assistance of a mediator pursuant to the ICC Mediation Rules. Recourse to the Mediation Rules may be based on an agreement between the parties or a unilateral request by one party subsequently accepted by the other. While providing for mediation, the ICC Mediation Rules also allow the parties to choose any other settlement method that may be better suited to their dispute. Settlement methods that can be used under the ICC Mediation Rules include:

Mediation. The neutral acts as a facilitator to help the parties arrive at a negotiated settlement of their dispute. The neutral is not requested to provide any opinion on the merits of the dispute.

Neutral evaluation. The neutral provides a non-binding opinion or evaluation on any of a wide variety of matters including issues of fact or law, technical questions or the interpretation of a contract.

Mini-trial. A panel consisting of the neutral and an authorized executive of each party hears presentations by the parties, after which either the panel or the neutral can mediate the dispute or express an opinion on the merits.

A combination of methods, such as mediation with a neutral evaluation on a particular issue.

The report of an expert, selected pursuant to the ICC Rules for the Administration of Expert Proceedings to make findings on a disputed matter, may help to facilitate settlement. However, unlike a neutral evaluation and unless the parties agree otherwise, the expert's report will be admissible in judicial or arbitral proceedings if no settlement is reached.

CASE MANAGEMENT TECHNIQUES

The parties and their counsel should keep in mind that even where settlement is not feasible before or at the outset of an arbitration, the arbitration can be managed in such a way as to facilitate settlement throughout the proceedings. Appendix IV to the ICC Rules of Arbitration highlights several case management techniques that can be used to that end:

Bifurcation. In appropriate cases, a partial award on jurisdiction or liability may facilitate settlement. For example, if the arbitral tribunal decides that it has jurisdiction, the parties will know that the arbitration will go forward. This could prompt them to discuss settlement. Similarly, if the tribunal finds a party to be liable, the parties may prefer to settle the issue of damages rather than incur the time and expense of completing the arbitration.

Early consideration of controlling issues. In some cases there are issues of law, fact or a mixture of fact and law, which necessarily affect the determination of the claims in the arbitration, yet can be resolved independently at relatively little expense. Examples include the determination of the applicable law, statute of limitations, the interpretation of a particular contractual provision, the determination of a key fact or technical issue or the measure of damages. The parties may find it easier to arrive at a settlement after such issues have been resolved by the tribunal.

Engagement of the arbitral tribunal. Where the parties agree and the applicable law permits, the arbitral tribunal can actively facilitate settlement either by encouraging the parties to pursue one of the settlement methods described above, or through discussions with the parties.

CREATIVITY AND OPEN-MINDEDNESS

Arbitrations often take on a life of their own once the parties have developed their positions and incurred costs. Parties and their counsel should keep in mind that a settlement can occur at any time during an arbitration and that the ICC Rules of Arbitration encourage the parties to explore this possibility. When exercising their will and their creativity in seeking a settlement, parties often arrive at solutions that are unavailable through arbitration.

CASE MANAGEMENT CONFERENCE

The case management conference provides the mechanism for determining the manner in which the arbitration will be conducted. If it is not possible to determine the entire procedure at the first case management conference, the remaining issues may be decided at a subsequent conference. The decisions made at the case management conference can be modified during the course of the arbitration by agreement of all of the parties or, failing such agreement, by a decision of the arbitral tribunal.

Article 24(1) of the ICC Rules of Arbitration requires the arbitral tribunal to convene an early case management conference to consult the parties on the conduct of the arbitration. Thereafter, pursuant to Article 22(2) of the Rules, the arbitral tribunal may adopt procedural measures for the conduct of the arbitration, provided that they are not contrary to any agreement of the parties. Article 22(1) requires the arbitral 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.

Issues to be decided include: the number of rounds of briefs; the extent of document production, if any; the early determination of issues; fact and expert witnesses; and the conduct of the hearing, if any. The topic sheets contained in this guide are designed to assist the parties, along with their counsel and the arbitral tribunal, in making appropriate choices for the conduct of the arbitration.

In practice, after receiving the case file, the arbitral tribunal may invite the parties to make case management proposals. If it does not do so, the parties can seek to agree between themselves upon the conduct of the proceedings. If they arrive at an agreement, it must be followed, subject to any proposals of the arbitral tribunal that are accepted by all of the parties. If the parties do not reach an agreement, the arbitral tribunal, after listening to the parties, will adopt procedural measures that it deems to be appropriate for the case at hand.

EFFECTIVE MANAGEMENT OF ARBITRATION CASE MANAGEMENT CONFERENCE

While Article 22(1) of the Rules refers to expeditious and cost-effective proceedings, it also makes clear that speed and low cost are not ends in themselves. The complexity and value of the dispute must be taken into account. A cost-effective and expeditious arbitration will be one in which the time and cost devoted to resolving the dispute is appropriate in light of what is at stake. In each case, it is necessary to make a cost/benefit analysis in order to see whether a particular procedural measure is cost-justified.

The objectives of the parties will play a crucial role in making such choices. Some examples of how parties' goals may translate into case management strategy are set forth below:

- When an important matter of principle is at stake, it may be worth the time and expense needed for a thorough examination of the facts and a full articulation of all legal arguments. A party with this objective may be willing to incur the expense of more extensive document production, multiple rounds of written submissions, a larger number of fact and expert witnesses, and the like.
- When neither an important principle nor great sums are at stake, parties may wish the arbitration to be as inexpensive and rapid as possible. Here, in contrast, parties may seek to limit document production, limit the number of witnesses, shorten hearings or minimize submissions.
- When parties wish to settle the case, for example in order to maintain their relationship or mitigate the risk of loss, they may use the case management conference to seek bifurcation of the proceedings or an early determination of controlling issues, the resolution of which might facilitate settlement. The parties may also agree to undertake settlement procedures either before or during the remaining phases of the arbitration.

TOPIC SHEETS

- 1.** Request for Arbitration
- 2.** Answer and Counterclaims
- 3.** Multiparty Arbitration
- 4.** Early Determination of Issues
- 5.** Rounds of Written Submissions
- 6.** Document Production
- 7.** Need for Fact Witnesses
- 8.** Fact Witness Statements
- 9.** Expert Witnesses (pre-hearing issues)
- 10.** Hearing on the Merits (including witness issues)
- 11.** Post-Hearing Briefs

1. REQUEST FOR ARBITRATION

PRESENTATION

An ICC arbitration is commenced by the filing of a Request for Arbitration with the Secretariat of the ICC International Court of Arbitration (Article 4 of the ICC Rules of Arbitration). In all cases, the Request must contain the information required by Article 4(3) of the Rules. That provision is intended to elicit sufficient information to enable the respondent to respond to the claimant's claims, as required by Article 5(1) of the Rules, and for the International Court of Arbitration to fulfil its functions under the Rules with respect to the constitution of the arbitral tribunal and the setting in motion of the arbitration.

Issue: Should the Request contain only the minimum requirements of the Rules or provide a more elaborate statement of the case?

OPTIONS

A. File a short Request that satisfies the Rules without providing any more content or evidence than is strictly required by the Rules.

B. File a comprehensive Request that constitutes a full statement of the case, including exhibits.

The above options represent two ends of a spectrum. However, there is also the option of filing a Request that provides a level of content and evidence anywhere between those two ends.

PROS AND CONS

A shorter and less comprehensive Request can be prepared more economically and more quickly than a more comprehensive document.

On the other hand, a more comprehensive Request may avoid the need for multiple rounds of subsequent submissions and thereby help to expedite the arbitration. In addition, providing more information may increase the impact of the Request on the respondent. Additional detail may also enable the parties and the

EFFECTIVE MANAGEMENT OF ARBITRATION

1. REQUEST FOR ARBITRATION

arbitral tribunal to focus on the key issues in the case as early as possible and thereby facilitate the drawing up of the Terms of Reference and the conduct of the case management conference.

COST/BENEFIT ANALYSIS

In all circumstances, the claimant should seriously consider conducting an early assessment of the nature, strengths and weaknesses of its case before filing a Request. This will allow it to determine, in the first instance, whether the claims are sufficiently strong to warrant bringing the arbitration or whether it would be better to seek a settlement of the dispute. If it decides to proceed with the arbitration, the early case assessment will help to ensure that the Request does not contain errors and that the claimant's claims are correctly described and set forth in the most effective manner. While this assessment requires some time and expenditure, it typically results in a saving of both over the arbitration as a whole.

If the claimant decides to proceed with the arbitration, it must determine whether to file a shorter or longer Request. The decision on how comprehensive the Request should be will be heavily influenced by the circumstances of the case and strategic considerations. Some time and cost may be saved by drafting a shorter Request although this may be a temporary saving if the claimant is ultimately required to supplement such a Request with additional detailed information. When the Request and the Answer respectively constitute a full statement of the case and a full statement of defence, time and cost can be saved by avoiding one or more further rounds of submissions. However, in complex cases this may not be possible, and the Request and Answer may be ultimately superseded by subsequent written submissions.

If a primary purpose for filing a Request is to elicit settlement discussions, consideration should be given to whether this is best accomplished with a shorter or a longer Request. A shorter Request may be preferable if the respondent is unlikely to discuss settlement unless an arbitration has been commenced and the substantive aspects of the claim would be best dealt with in the

settlement discussions. A longer Request may be preferable if the goal is to show the respondent in writing the strengths of the claimant's case before commencing settlement discussions.

QUESTIONS TO ASK

1. What is the desired result of filing the Request (e.g. triggering settlement discussions or having the dispute resolved by arbitration)?
2. Are there any valid reasons for not conducting an early case assessment?
3. Are there any real cost savings in filing a shorter Request? Would they be outweighed by the benefits of filing a longer Request for any of the reasons described above?
4. Are there any other strategic or legal considerations that may affect the timing of the filing of the Request and consequently whether it should be shorter or longer?

OTHER POINTS TO CONSIDER

In certain cases, questions of timing may militate in favour of a shorter Request. For example, a Request may need to be filed quickly to avoid being barred by a statute of limitations. A Request may also have to be filed within ten days of receipt by the Secretariat of an application for emergency measures pursuant to Article 1 of the Emergency Arbitrator Rules (Appendix V to the Rules).

Pursuant to Article 23(4) of the Rules, after the Terms of Reference have been established, no new claims may be made without the authorization of the arbitral tribunal. It is therefore prudent for the claimant to make all of its claims prior to the signing of the Terms of Reference.

Article 5(6) of the Rules provides that the claimant shall submit a reply to any counterclaim raised by the respondent pursuant to Article 5(5) of the Rules. The topic sheet relating to the Answer and counterclaims offers guidance on this matter.

2. ANSWER AND COUNTERCLAIMS

PRESENTATION

The respondent is required to file an Answer to the Request for Arbitration with the Secretariat (Article 5 of the ICC Rules of Arbitration). In all cases, the Answer must contain the information required by Article 5(1) of the Rules. The Answer may contain a counterclaim pursuant to Article 5(5) of the Rules.

Issue: How detailed or extensive should the Answer and any counterclaim be, above and beyond what is required by the Rules?

OPTIONS

A. File a short Answer that satisfies the Rules without providing any more content or evidence than is strictly required by the Rules.

B. File a comprehensive Answer that constitutes a full statement of defence, including evidentiary exhibits.

The above options represent two ends of a spectrum. However, there is also the option of filing an Answer that provides a level of content and evidence anywhere between those two ends.

In deciding on the appropriate length of the Answer, the respondent should consider whether or not to match the length and level of detail chosen by the claimant. Specifically, the respondent may choose between the following options:

a) File an Answer that reflects the approach taken by the claimant (e.g. a shorter or a longer document).

b) File an Answer in a form that is different from the form of the Request filed by the claimant.

C. Assert a counterclaim, irrespective of the length and content of the Answer. The raising of a counterclaim is subject to considerations similar to those described in the topic sheet on the Request for Arbitration.

PROS AND CONS

The pros and cons of filing a shorter or a longer Answer may vary depending on the form of the Request filed by the claimant. If the claimant has filed a shorter Request and the respondent reciprocates with an equally short Answer, the arbitration should be able to proceed more expeditiously to the Terms of Reference and the case management conference, in part because the respondent is less likely to need an extension of time for filing the Answer pursuant to Article 5(2) of the Rules. On the other hand, if the claimant files a longer and more detailed Request, then the respondent may be required to seek an extension of time in order to respond with a detailed Answer.

A shorter and less comprehensive Answer can be prepared more economically and more quickly than a more comprehensive document.

If the claimant has filed a comprehensive Request and the respondent decides to file a comprehensive Answer, this may avoid the need for multiple rounds of subsequent submissions and thereby expedite the arbitration.

In addition, providing more information may increase the impact of the Answer. Additional detail may also increase the ability of the parties and the arbitral tribunal to focus on the key issues in the case as early as possible and thereby facilitate the drawing up of the Terms of Reference and the conduct of the case management conference.

COST/BENEFIT ANALYSIS

To the extent possible in the time available, the respondent should conduct an early assessment of the nature, strengths and weaknesses of its case before filing an Answer. This will allow it to determine, in the first instance, whether the case should be defended or whether settlement should be pursued. If the respondent decides to defend the arbitration, and possibly assert counterclaims, the early case assessment will help to ensure that the Answer does not contain errors and that the respondent's defence and/or counterclaims are correctly described and set forth in the most effective manner. While this assessment

requires some time and expenditure, it typically results in a saving of both over the arbitration as a whole.

An additional consideration for the respondent is the limited amount of time available under the Rules for making an early case assessment and filing its Answer. If the respondent has prior knowledge of the dispute, then it may be able to undertake an early case assessment before receiving the Request for Arbitration. If, on the other hand, the receipt of the Request for Arbitration is the respondent's first real opportunity to assess the claimant's claims, the time available to it under the Rules for this purpose will be limited.

Depending on the circumstances described above, the respondent must decide whether to file a shorter or a longer Answer. The decision on how comprehensive the Answer should be will be heavily influenced by the circumstances of the case, strategic considerations and the limited time available for submitting the Answer under the Rules. Some time and cost may be saved by drafting a shorter Answer although this may be a temporary saving if the respondent is ultimately required to supplement such an Answer with additional detailed information.

If the claimant has filed a full statement of the case in its Request and if in the time available it is possible to file a full statement of defence in the Answer, time and cost can be saved by avoiding one or more rounds of further submissions. However, this may not be possible in complex cases.

Consideration should be given to whether filing a shorter or a longer Answer might facilitate settlement discussions. A shorter Answer may be preferable if the substantive aspects of the settlement would best be dealt with in negotiations and there is a reasonable prospect of a settlement. A longer Answer may be preferable if the goal is to show the claimant in writing the strengths of the respondent's defence and any counterclaims for purposes of settlement discussions.

QUESTIONS TO ASK

1. Are there any real cost savings or any other advantages in filing a shorter Answer? Would they be outweighed by the benefits of filing a longer Answer for any of the reasons described above?
2. Is there sufficient time to conduct an early assessment of the defence and file the Answer within the 30 days specified in the Rules, or is it necessary to request an extension of time for filing the Answer pursuant to Article 5(2)?
3. Are there any serious counterclaims that can and should be raised in the arbitration? Should they comply with only the minimum requirements set out in the Rules or be more detailed and accompanied by evidentiary exhibits?

OTHER POINTS TO CONSIDER

Pursuant to Article 23(4) of the Rules, after the Terms of Reference have been established, no new claims may be made, without the authorization of the arbitral tribunal. It is therefore prudent for any counterclaims to be made by the respondent prior to the signing of the Terms of Reference.

If the respondent wishes to join an additional party pursuant to Article 7(1) of the Rules, it must be careful to do so within the time limits specified in that Article.

If there are serious objections to jurisdiction, the respondent may consider keeping the Answer short with respect to the merits.

3. MULTIPARTY ARBITRATION

PRESENTATION

Under the ICC Rules of Arbitration, an arbitration having more than two parties may occur when all of the parties have so agreed. Multiparty arbitrations may result from various procedural choices:

- A claimant may commence an arbitration pursuant to Article 4 of the Rules against two or more respondents.
- Two or more claimants may commence an arbitration pursuant to Article 4 of the Rules against one or more respondents.
- Before the confirmation or appointment of any arbitrator, any party may join another party to the arbitration pursuant to Article 7 of the Rules.
- Upon any party's request, two or more pending arbitrations may be consolidated into a single arbitration by the Court, subject to the requirements of Article 10 of the Rules.

Issue: When is it beneficial to choose a multiparty arbitration?

OPTIONS

- A. A single arbitration that includes all relevant parties when they have all so agreed.
- B. Two or more separate arbitrations.

PROS AND CONS

A single multiparty arbitration, when possible, results in more comprehensive proceedings and avoids duplication. It also avoids the risk of conflicting decisions in separate arbitrations.

On the other hand, a single multiparty arbitration may result in more complex proceedings, which could increase the length and cost of the arbitration. For example, a party with a small role in the dispute may not wish to participate in a multiparty arbitration and could

refuse to do so in the absence of a binding arbitration agreement. Further, in an arbitration where there is to be a three-member arbitral tribunal, choosing to have more than two parties in the arbitration may deprive the parties of their ability to choose a co-arbitrator, because the ICC International Court of Arbitration may decide to appoint the entire tribunal pursuant to Article 12(8) of the Rules.

COST/BENEFIT ANALYSIS

Consideration should be given to whether a single multiparty arbitration, as opposed to two or more separate arbitrations, would save time and money. While a single arbitration will usually be more cost-efficient, there could be situations in which separate arbitrations may still be the more efficient option for one or more parties.

If a single multiparty arbitration is the more time- and cost-efficient option, the parties should consider whether the time and cost benefits outweigh any of the potential disadvantages, such as the risk of losing the opportunity to choose a co-arbitrator because the International Court of Arbitration may find it necessary to appoint the arbitral tribunal pursuant to Article 12(8) of the Rules.

Another important factor to consider in deciding whether a single multiparty arbitration would be beneficial is the contractual role of each party and the specific interests flowing from that role. Arbitration of your dispute with one party may weaken your position with respect to another party. Where, for example, parties share potential liability with respect to their contractual counterparty, it may be tactically imprudent for them to have their internal disputes heard in the arbitration with the contractual counterparty, since their allegations against each other may support the counterparty's case against them.

4. EARLY DETERMINATION OF ISSUES

PRESENTATION

Issue: In what circumstances would it be beneficial to break out certain issues for early determination by the arbitral tribunal in a partial award?

Various kinds of issues lend themselves to such treatment:

First, there may be threshold issues that could be dispositive of the entire arbitration. Such issues might include:

- whether the tribunal has jurisdiction over the dispute;
- whether the dispute is barred by an applicable statute of limitations;
- whether there is liability;
- whether the dispute is arbitrable;
- whether the parties have capacity to sue or be sued.

For example, were a tribunal to decide that it lacks jurisdiction over the entire dispute, that would result in a final award dismissing all claims made in the arbitration. If the tribunal decides that it has jurisdiction, that decision would result in a partial award and the arbitration would continue, unless the tribunal's decision leads to a settlement. The same pattern would apply, *mutatis mutandis*, to the other examples given above.

Second, there may be discrete issues which could be usefully broken out and decided in a partial award, even though their resolution would not be dispositive of the entire arbitration. The early resolution of a particular issue may narrow or simplify the issues to be decided in the remainder of the arbitration or may facilitate settlement. Such issues may include:

- a decision on the meaning of a contractual provision;
- a decision on the applicable law;
- a decision on certain key facts in dispute;

EFFECTIVE MANAGEMENT OF ARBITRATION

4. EARLY DETERMINATION OF ISSUES

- a decision on an issue that may significantly affect a party's exposure to one or more claims, such as determination of the types of recoverable damages.

For example, a decision on applicable law may save the parties from having to incur time and cost pleading their case on the basis of alternative applicable laws. The same analysis applies to the other examples above.

OPTIONS

- A. Do not break out any issues for early determination.
- B. Break out one or more issues for early determination by means of an award.

PROS AND CONS

The early determination of one or more issues in a partial award may resolve the entire dispute, simplify the remainder of the arbitration or facilitate settlement. However, if the award does not achieve one of those objectives, the early determination procedure may result in added time and cost. In addition, breaking out a discrete issue rather than having it decided along with the other issues may affect the way the tribunal decides one or more of the issues.

COST/BENEFIT ANALYSIS

Breaking out issues that could be dispositive of the entire arbitration

A cost/benefit analysis of this question is complicated by the fact that the decision has to be made in the face of important unknowns. When deciding whether or not to break out an issue, the parties cannot know what the arbitral tribunal's decision will be. For example, in a case involving issues of liability and damages, if the issue of liability is broken out and the tribunal decides that there is no liability, a great deal of time and cost will be saved since there will be no need to exchange briefs and hold hearings on damages. On the other hand, if the tribunal finds that there is liability, unless such finding encourages the parties to settle the case, there will have to be a damages phase, and the breaking out of the issue of liability may then actually add to the overall time and cost of the proceedings.

Given these unknowns, the cost/benefit analysis must turn on an appreciation of probabilities and an estimate of potential cost. In deciding whether to break out an issue, it may be useful to estimate likely outcomes as well as time and cost in answer to certain specific questions:

- What is the likelihood that the tribunal's decision will be dispositive of the entire arbitration?
- If the tribunal's decision will not be dispositive of the entire arbitration, what is the likelihood that the tribunal's early determination of the issue may result in a settlement of the case?
- What is the added time and cost likely to result from early determination of the issue in comparison with the likely overall cost, i.e. how much more time and cost would there be if the arbitration were conducted in two parts rather than one?

The answers to these questions can help in deciding whether or not to break out an issue for early determination. The following factors would tend to favour the breaking out of an issue for early determination:

- the likelihood of a dispositive determination is high;
- the likelihood of a settlement, even if there is no dispositive determination, is high;
- the remaining phases are likely to be long and expensive;
- the additional cost caused by early determination is low.

A decision on whether to break out an issue can be made by weighing these factors in relation to each other.

Breaking out issues in a partial award not dispositive of the entire arbitration

A similar type of cost/benefit analysis would apply here, although the relevant questions are slightly different:

- What is the likelihood that the tribunal's early determination of a particular issue will significantly narrow or simplify the other issues to be decided in the remainder of the arbitration?

EFFECTIVE MANAGEMENT OF ARBITRATION

4. EARLY DETERMINATION OF ISSUES

- What is the likelihood that early determination of a particular issue may result in a settlement of the case?
- What is the additional time and cost likely to result from early determination of a particular issue?

Once again, weighing the answers to those questions against each other can help in deciding whether it is beneficial to break out a particular issue for early determination.

QUESTIONS TO ASK

1. Does the case contain any threshold or discrete issues that could be determined in a separate award?
2. Would the early determination of those issues by the arbitral tribunal be beneficial, in light of the cost/benefit analysis discussed above?
3. Would early determination (a) potentially resolve the entire dispute, (b) facilitate settlement or (c) simplify the rest of the arbitration?

OTHER POINTS TO CONSIDER

Article 38(5) of the Rules permits the arbitral tribunal, when allocating the costs of the arbitration, to take into account the extent to which each party has conducted the arbitration in an expeditious and cost-effective manner. The arbitral tribunal might allocate some amount of costs against a party that loses in the early determination of a potentially dispositive issue if that party is considered to have acted in bad faith or otherwise not to have acted in an expeditious and cost-effective manner.

There may be logistical reasons for breaking out one or more issues for early determination, such as the availability of witnesses, hearing facilities, counsel or arbitrators. In addition, it may allow a complex case to be conducted in a more orderly manner.

There may be compelling reasons for deciding certain issues early in an arbitration, e.g. whether claims made under different arbitration agreements may be heard together in a single arbitration. The breaking out of an issue for decision in a partial award could be agreed upon by the parties or determined by the arbitral tribunal in the absence of an agreement by the parties.

5. ROUNDS OF WRITTEN SUBMISSIONS

PRESENTATION

An ICC arbitration is commenced by the filing of a Request for Arbitration (Article 4 of the ICC Rules of Arbitration). Thereafter, the respondent files an Answer (Article 5). If the Answer contains a counterclaim, the claimant files a reply (Article 5). The Terms of Reference for the arbitration are then established (Article 23).

Issue: How many subsequent rounds of written submissions are appropriate in a particular arbitration?

OPTIONS

- A. No further written submissions are necessary, since the Request and the Answer sufficiently state the case.
- B. One subsequent round of written submissions.
- C. Two or more subsequent rounds of written submissions.
- D. Post-hearing briefs (assuming there is a hearing).

PROS AND CONS

Additional rounds of written submissions enable the parties to articulate their positions more extensively and respond to the developing arguments on each side.

However, additional rounds of briefs may lead to unnecessary repetition, excessive detail or dilatory tactics.

COST/BENEFIT ANALYSIS

Each round of written submissions increases the length and cost of the arbitration. It is therefore essential to determine whether, in a particular case, the benefits of an additional round are worth the extra time and cost.

Additional submissions may be particularly useful in certain cases, e.g. where there are complicated issues of fact or law or issues of strategic importance for a party. In such cases, it is very common to have two rounds of pre-hearing written submissions after the initial submissions.

QUESTIONS TO ASK

1. Does the case justify the extra time and cost caused by additional written submissions?

And, in particular,

2. Are additional rounds of submissions genuinely useful or necessary for a party to make its case to the arbitral tribunal, and if so, why?

3. What is the estimated cost of such additional rounds?

4. Is the benefit worth the cost, and if so, why?

OTHER POINTS TO CONSIDER

Consider limiting the number of pages of written submissions.

Consider limiting the scope of such submissions, e.g. to issues raised by the other side in its immediately preceding submission.

Consider having the arbitral tribunal indicate issues on which it wishes the parties to focus in any further round of submissions.

Consider whether any subsequent rounds of submissions should be simultaneous or sequential. For example, it may be efficient for post-hearing briefs to be filed simultaneously.

Consider whether post-hearing briefs are genuinely useful or necessary, or whether one round of pre-hearing briefs and one round of post-hearing briefs are sufficient.

The foregoing suggestions could be put into effect either through an agreement between the parties or in an order from the arbitral tribunal upon a party's request.

6. DOCUMENT PRODUCTION

PRESENTATION

Document production can involve substantial time and cost. Obviously, every party may unilaterally submit documents to support its case. Document production refers to the extent to which one party may demand that another party produce documents.

The ICC Rules of Arbitration contain no specific provisions governing document production. Article 19 of the Rules allows the parties to agree upon the procedures to be applied and empowers the tribunal to decide in the absence of an agreement of the parties. Article 22(4) requires the arbitral tribunal to ensure that each party has a reasonable opportunity to present its case. Article 25(1) provides that the arbitral tribunal shall establish the facts of the case by all appropriate means and Article 25(5) allows it to summon any party to provide additional evidence.

In short, the Rules leave the question of whether and how much document production will occur to the parties and the arbitrators, provided that the parties are treated fairly and impartially and that each party has a reasonable opportunity to present its case. When document production is to occur, the manner in which the process is executed and the degree of production can have a significant impact on time and cost.

In-house counsel or other party representatives, working with outside counsel, should consider whether and to what extent document production is genuinely useful and cost-beneficial. When document production is to occur, time and cost can be significantly reduced by establishing an efficient document production procedure.

Issue: Is document production desirable and, if so, how much document production should there be?

OPTIONS

Options range from no document production at all to full document production.

EFFECTIVE MANAGEMENT OF ARBITRATION

6. DOCUMENT PRODUCTION

A. No document production.

- The parties may decide to seek no documents from each other and to rely solely on the documents each of them possesses.
- The parties are always free to submit their own documents.
- The parties are also free to request the arbitral tribunal to order the production of specific documents.

B. Production limited to specific documents or narrow categories of documents, which are relevant and material to deciding an issue in the arbitration.

Consider using:

- the IBA Rules on the Taking of Evidence in International Arbitration (“IBA Rules”) as a standard;
- the suggestions in the report of the ICC Commission on Arbitration and ADR entitled “Controlling Time and Costs in Arbitration”;
- the report of the ICC Commission on Arbitration and ADR entitled “Managing E-Document Production”.

C. Broad document production as used in some common law jurisdictions.

- The parties may agree upon broad requests for documents.
- In rare cases, the parties may agree to common law style “discovery” including depositions and/or interrogatories.

When document production is to occur, the parties may agree upon the ground rules for requesting documents from and producing documents to each other.

If the parties cannot agree on whether to have document production or on the extent of document production or the ground rules for such production, the tribunal will decide.

PROS AND CONS

Document production can be very expensive and time-consuming and the broader the document production the more expensive and time-consuming it

tends to be. It requires time and expenditure from the party that searches for and produces documents as well as from the party that must study and analyse the documents that are produced.

On the other hand, if one of the parties has sole possession of documents needed by the other party, document production may be essential. Moreover, document production can provide the parties and the tribunal with a more complete understanding of the case. Given that parties are unlikely to submit documents spontaneously when they are detrimental to their own case, document production puts them under an obligation to do so.

COST/BENEFIT ANALYSIS

In view of the time and cost required for document production, a cost/benefit analysis is necessary in order to decide whether to seek document production at all and, if so, to determine the desired extent of such production. The parties should explore whether they can effectively meet their burden of proof with the documents that are already in their possession and whether the other side is likely to have documents that are genuinely useful for the first party to make its case.

Each party should then estimate the extra time and cost caused by document production and weigh this against the likelihood that document production will genuinely assist it in making its case. For example, if document production is estimated to cost USD 500,000 and it is considered that there is at best a 10% chance that it will yield valuable results, the question arises as to whether that 10% chance is worth the expense of USD 500,000. This is a decision that can best be made jointly by the party, typically represented by in-house counsel, and outside counsel. Many factors may come into play, such as the amount in dispute, whether there are policy issues, whether there is concern about precedent and whether the benefit of obtaining documents from the other side may be outweighed by the detriment of being required to produce documents oneself.

QUESTIONS TO ASK

1. Are any requests for document production genuinely useful or necessary for a party to make its case or can the party rely effectively on the documents in its possession?
2. What extent of document production is genuinely useful and necessary?
3. When should document production occur?
4. What is the estimated cost of searching for and producing documents, as well as the cost of reviewing and analysing documents that have been produced?
5. Is the benefit of document production worth the cost, and if so, why?

OTHER POINTS TO CONSIDER

Consider whether it is appropriate to deal with document production in the arbitration clause, for example by agreeing that there will be no document production (e.g. in contracts where it is relatively certain that document production will not assist in resolving potential disputes); by agreeing to limited document production in accordance with the IBA Rules; or by agreeing to broad document production or “discovery”.

Consider whether document production should occur once or more than once. Consider whether it should occur prior to or after written submissions.

Consider whether it is appropriate to limit documents transmitted to the arbitral tribunal to a manageable quantity.

Take into account any costs of translation when estimating the cost of document production.

Consider the ground rules to be adopted for implementing document production, including the use of a Redfern Schedule and the setting of the shortest reasonable time frames for production.

Special considerations may be needed if the parties agree upon or the tribunal orders the production of electronic documents. In such cases, the report of the ICC Commission on Arbitration and ADR entitled “Managing E-Document Production” can be used to assist in choosing the most efficient methods of e-document production.

7. NEED FOR FACT WITNESSES

PRESENTATION

Article 25(1) of the ICC Rules of Arbitration requires the arbitral tribunal to establish the facts of the case by all appropriate means. This can include the hearing of fact witnesses. Article 25(3) of the Rules specifically allows the arbitral tribunal to decide to hear witnesses. However, Article 25(6) allows the arbitral tribunal to decide the case solely on documents, unless a party requests a hearing. This would permit an arbitration with no hearing and no fact witnesses.

Issue: Is there a genuine need for fact witnesses?

OPTIONS

A. No fact witnesses at all.

B. One or more fact witnesses.

- Identify the issues on which fact witness testimony is necessary.
- Identify the appropriate fact witnesses for the issues.

PROS AND CONS

Fact witnesses can be essential to proving a case. However, they significantly increase the length and cost of an arbitration, since there will typically be one or more written witness statements for each witness and the oral testimony of each witness may be required at a hearing.

COST/BENEFIT ANALYSIS

Fact witnesses may be genuinely necessary in order to prove disputed facts or to present a broader picture of the circumstances surrounding the dispute. In determining whether fact witnesses are needed, the following issues can be considered:

- Are there any disputed facts? It may appear from the pleadings that there are disputed facts, but it may turn out after discussion between the parties that those facts are not really disputed. In addition, a party may agree not to contest certain disputed facts in order to save time and cost when the dispute over those facts is not sufficiently important.
- If there are disputed facts, are they relevant and material for deciding an issue in the dispute? There is no need to incur the extra time and cost involved in having a fact witness testify on disputed facts that will not affect the determination of an issue in the dispute.
- If there are disputed facts that are relevant and material, can they be proved by documents alone or do they genuinely need to be proved through fact witnesses?
- Is it useful to call fact witnesses to make a general presentation on the circumstances of the dispute?

When a party has decided to use fact witnesses, time and cost can be reduced by avoiding having many witnesses testify as to the same facts and by carefully focusing the scope of the testimony of each witness.

QUESTIONS TO ASK

1. Is there a genuine need for fact witnesses at all?
2. If so, who should they be? What should be the scope of their testimony? How many fact witnesses are genuinely necessary to establish a particular fact or present the circumstances of the case?

OTHER POINTS TO CONSIDER

Consider using videoconferencing for oral witness testimony to save time and cost.

Consider what is the most effective way of examining the fact witnesses at a hearing: e.g. direct examination and cross-examination; opening presentation by the witness followed by cross-examination; use of the witness's written statement as a substitute for direct examination and proceeding straightaway with cross-examination; questioning of fact witnesses by the tribunal only or by the tribunal followed by questions from counsel.

Determine whether it is preferable for a given witness to testify in the language of the arbitration or in his or her native language. When a witness is testifying in a language other than the language of the arbitration, appropriate translation will often need to be arranged, which will increase time and cost.

8. FACT WITNESS STATEMENTS

PRESENTATION

Issues arising when a party has decided to present fact witness evidence: Should witness statements be submitted? What should their scope be? When should they be submitted?

OPTIONS

Form

- A. No written witness statements.
- B. Brief summary of the scope of witness evidence (witness summary).
- C. Full witness statements.

Scope of full witness statements

- A. Lengthy and comprehensive statement.
- B. Short statement limited to key factual issues in dispute.

Number and timing

- A. One or more rounds of witness statements.
- B. Witness statements submitted with written submissions.
- C. Witness statements submitted following the exchange of written submissions.
- D. Witness statements submitted simultaneously or sequentially.

PROS AND CONS

Form

Written witness statements increase the length and cost of the pre-hearing phase, but can reduce the length and cost of the hearing by replacing direct examination and allowing for a more focused cross-examination. The absence of witness statements, or the submission of witness summaries only, will reduce pre-hearing costs but can increase the length and cost of the hearing.

EFFECTIVE MANAGEMENT OF ARBITRATION

8. FACT WITNESS STATEMENTS

Scope

Comprehensive witness statements can be a valuable part of case presentation, allowing witnesses to tell the story of the dispute and place documentary evidence in its context. However, lengthy witness statements will increase time and cost as well as the scope of cross-examination.

Number and timing

More than one round of witness statements provides witnesses with the opportunity to rebut the evidence of other witnesses, but will increase time and cost prior to the hearing.

Submitting witness statements with the written submissions provides direct proof of the facts at the time they are alleged. It also allows the parties to identify and progressively narrow down the factual issues, which may make for shorter, more targeted submissions later.

Submitting witness statements only after the exchange of written submissions may allow the parties to narrow down the factual issues in dispute before preparing and submitting witness statements, which may consequently be more focused on the disputed issues.

COST/BENEFIT ANALYSIS

While witness statements can provide valuable evidence in support of a party's position, they can add significantly to time and cost. The importance of the evidence to be presented must therefore be weighed against the time and expense required to present it. For example, if alternative sources of evidence are available (e.g. contemporaneous documentary evidence), there may be no cost justification for providing a witness statement on those facts. Similarly, if a witness is submitting a statement on a given fact, the submission of another witness statement evidencing the same fact may not be cost-justified, particularly if the fact is of little importance.

Full witness statements require more work and are therefore more expensive to prepare than witness summaries. However, they may subsequently save time and cost during a hearing by obviating the need for lengthy direct examination of the witness at the hearing.

The case management techniques set out in Appendix IV to the Rules include limiting the length and scope of written witness evidence so as to avoid repetition and focus on key issues. In line with Appendix IV, parties may wish to consider how to structure their fact witness evidence as efficiently as possible.

QUESTIONS TO ASK

1. In light of the other sources of evidence available, is the preparation of a given witness statement justified in terms of time and cost?
2. Is a witness statement required to prove a disputed question of fact or provide necessary background information? Is more than one witness statement necessary to accomplish this? Is there a good reason not to limit the witness statement to the key factual issues in dispute?
3. Should the witness evidence be presented in the form of full witness statements or witness summaries?
4. Is it necessary to have more than one round of witness statements?
5. Should the witness statements be filed concurrently with, or only after, the parties' written submissions?

9. EXPERT WITNESSES (PRE-HEARING ISSUES)

PRESENTATION

Article 25(3) of the ICC Rules of Arbitration contemplates the possibility of experts appointed by the parties, while Article 25(4) provides that, after consulting the parties, the arbitral tribunal may appoint one or more experts, define their terms of reference, and receive their reports.

Issues: Is there a genuine need to appoint experts? Should they be appointed by the parties, the tribunal, or both? How should they be selected? How should the written expert reports be produced?

OPTIONS

Whether and how to appoint experts

- A. No experts at all.
- B. Party-appointed expert(s) only.
- C. Tribunal-appointed expert(s) only.
- D. Both party-appointed and tribunal-appointed experts.

How to select party-appointed experts

- A. Selection of an expert by the parties or their counsel.
- B. Selection of an expert proposed by the ICC International Centre for ADR at a party's request.

How to select tribunal-appointed experts

- A. Selection by the tribunal alone after obtaining the parties' comments on the expert to be appointed, including with respect to the expert's independence and impartiality. This option includes the tribunal's selection of an expert proposed by the ICC International Centre for ADR at the tribunal's request.
- B. Selection by the tribunal of an expert agreed by the parties or from a list of experts jointly submitted by the parties.

Production of written reports

A. Separate reports by each party-appointed expert.

- These reports can be produced with the parties' briefs or after the parties have produced their fact witness statements.
- These reports can be produced either simultaneously or sequentially.

B. Instead of, or subsequent to, the production of separate reports, the party-appointed experts meet to determine points of agreement and disagreement and produce reports laying out their respective positions on the points of disagreement.

C. Preparation by the tribunal of terms of reference for tribunal-appointed experts after submitting a draft to the parties for comment. Thereafter, the expert produces a written report based upon the terms of reference.

PROS AND CONS

Certain technical issues may need to be presented through expert opinions. In some cases, expert opinions can be decisive for a case. However, expert witnesses significantly increase the length and cost of an arbitration.

If there are to be experts, the pros and cons of party-appointed experts and/or tribunal-appointed experts must be considered. In particular cases, a tribunal-appointed expert may be the most persuasive expert for arbitrators from certain legal cultures, but reliance on a tribunal-appointed expert deprives the parties of some degree of control. Whether a tribunal-appointed expert should be requested is an important matter of strategy to be considered on a case-by-case basis.

Recourse to a tribunal-appointed expert alone, with no party-appointed experts, will no doubt be the least expensive option. However, there may be cases where a tribunal-appointed expert's views cannot be adequately questioned or tested by the parties without the assistance of party-appointed experts. Recourse to both will increase time and cost.

COST/BENEFIT ANALYSIS

Whether and how to appoint experts

Whether or not to appoint experts can be a complex question requiring consideration of a number of factors, including the nature of the issues, the legal and cultural background of the tribunal, the availability of experts, case strategy and the impact on time and cost. A key consideration will be whether the cost and time associated with expert witnesses is justified by a genuine need in the case at hand.

How to select party-appointed experts

A. Selection of an expert by the parties or their counsel

In order to present evidence on issues requiring expertise, the parties or their counsel may select an outside expert to produce an expert report. Alternatively, evidence on such issues can be presented by the parties' in-house technical experts. The in-house experts may be very knowledgeable in their field and have hands-on knowledge of the specific technical matters at issue. Yet, there is a risk that the tribunal could perceive them as being partial. Outside experts are more expensive and more time-consuming but, depending on their qualifications and professional demeanour, could be viewed as more impartial.

B. Selection of an expert proposed by the ICC International Centre for ADR at a party's request.

The ICC International Centre for ADR offers parties and tribunals a service of finding experts from a wide range of sectors and countries. This may speed up the process of identifying experts and minimize the cost. In addition, the fact that a party-appointed expert has been identified by the ICC International Centre for ADR can reflect well upon the expert's qualifications, independence and impartiality.

How to select tribunal-appointed experts

A. Selection by the tribunal alone after obtaining the parties' comments on the expert to be appointed, including with respect to the expert's independence and impartiality. This option includes the selection by the tribunal of an expert proposed by the ICC International Centre for ADR at the tribunal's request.

The selection of an expert by the arbitral tribunal alone may be more expeditious and may avoid disputes between the parties over the suitability of their respective proposals. Moreover, the appointment of one expert will reduce time and cost. However, this method excludes the parties from the selection process and creates a risk that the chosen expert may fall short of the parties' expectations. From the parties' perspective, a further disadvantage is that the content of the expert's opinion may remain unknown to them until produced before the arbitral tribunal.

B. Selection by the tribunal of an expert agreed by the parties or from a list of experts jointly submitted by the parties.

This is a more time-consuming process than the appointment of an expert by the tribunal alone, but has the advantage of restricting selection to an expert acceptable to the parties and the tribunal. Moreover, the appointment of a single expert will reduce time and cost. However, a potential disadvantage from the parties' perspective will again be that the content of the expert's opinion remains unknown to the parties until produced before the arbitral tribunal.

Production of written reports

A. Separate reports by each party-appointed expert.

- These reports can be produced with the parties' briefs or after the parties have produced their fact witness statements.

The submission of expert evidence with a party's briefs has the advantage of enabling a more comprehensive understanding of that party's case. It may help to focus the content of any subsequent briefs on the actual rather than the assumed areas in which expert evidence may be submitted. The disadvantage is that the expert evidence may not take account of any evidence introduced by the other party in subsequent witness statements, expert reports or subsequent briefs and may either be incomplete or create a need for supplemental expert evidence.

- These reports can be produced either simultaneously or sequentially.

In cases where the points of disagreement are sufficiently clear, simultaneous filings will generally be faster than sequential filings because there will be fewer rounds. However, when the points of disagreement are not sufficiently clear, simultaneous filings may result in expert reports that do not correspond or respond to each other, which could actually increase time and cost.

The ultimate choice will also depend upon tactical or strategic considerations that go beyond issues of time and cost.

B. Instead of, or subsequent to, the production of separate reports, the party-appointed experts meet to determine points of agreement and disagreement and produce reports laying out their respective positions on the points of disagreement.

The production of written expert reports can be time-consuming and expensive. Reducing the scope of those reports will reduce time and cost. If the party-appointed experts are given the opportunity to meet and clearly identify the points over which they disagree, their reports can be shortened and focus on the points of disagreement.

C. Preparation by the tribunal of terms of reference for tribunal-appointed experts after submitting a draft to the parties for comment. Thereafter, the expert produces a written report based on the terms of reference.

It is important to ensure that the tribunal-appointed expert focuses and provides an opinion on the specific issues in dispute within the relevant area of expertise. The terms of reference are designed to serve this purpose. By being allowed to comment on and provide input into the terms of reference, the parties will have a degree of control over the process.

QUESTIONS TO ASK

1. Is there a genuine need to appoint experts or can the case be effectively made without expert evidence?
2. Should there be party-appointed experts, tribunal-appointed experts or both?
3. What is the appropriate method for selecting party-appointed experts or tribunal-appointed experts, as the case may be?
4. If there are to be party-appointed experts, how many experts are genuinely necessary?
5. When and in what form should expert reports be produced?
6. Should reports be submitted simultaneously or sequentially?
7. Should party-appointed experts be required to meet in order to determine points of agreement and disagreement?
8. If such a meeting is held, should counsel be present at the meeting?

OTHER POINTS TO CONSIDER

Consider avoiding more than one party-appointed expert per topic on each side.

Consider whether it is genuinely necessary to have an expert witness on issues of law. A great deal of time and cost can be saved if legal issues are argued by outside counsel in their briefs and at the hearing.

10. HEARING ON THE MERITS (INCLUDING WITNESS ISSUES)

PRESENTATION

Pursuant to Article 25(2) of the ICC Rules of Arbitration, a hearing must be held if requested by any party. In addition, pursuant to Articles 25(2) and 25(3), the arbitral tribunal may hear the parties, witnesses, experts or any other person, if it so decides of its own motion.

Hearings are expensive to hold and the longer they are, the more costly they become.

Issues: Is it genuinely necessary to hold a hearing at all? If so, is there a need for more than one hearing? What is the appropriate length for the hearing and how should it be organized?

OPTIONS

A. Hold no hearing and have the case decided solely on the documents submitted by the parties.

B. Hold one or more hearings, as appropriate.

When a hearing is to be held, a certain number of choices need to be made, including:

- appropriate location;
- dates;
- attendees;
- appropriate duration;
- allocation of time between the parties;
- whether there are to be opening and/or closing statements and their duration;
- whether there should be direct examination, cross-examination and/or witness conferencing for fact and expert witnesses;
- whether the hearing should be transcribed and if so, whether daily transcripts and/or live transcripts (i.e. real-time transcripts available electronically to participants during the hearing) should be made;

EFFECTIVE MANAGEMENT OF ARBITRATION

10. HEARING ON THE MERITS

- when interpreting is needed, whether it should be consecutive or simultaneous;
- whether to use videoconferencing for all or part of the hearing.

PROS AND CONS

Oral hearings are often considered as a key opportunity for the parties to present their case and for the arbitrators to understand it and assess the evidence.

On the other hand, oral hearings are typically one of the most expensive and time-consuming phases of the arbitral process. Costs are generated by a number of factors, including the extensive preparation that is usually necessary and the number of people attending the hearing. In addition, the arbitration is often delayed by the difficulty of finding a mutually convenient time in the calendars of all relevant participants.

Cost and time can nevertheless be reduced by making appropriate choices with respect to the organization of the hearing.

COST/BENEFIT ANALYSIS

In deciding whether to request or agree upon a hearing, the parties should take various factors into consideration. Hearings tend to be most useful when there are disputed issues of fact to be addressed by fact and expert witnesses. Parties may consider proceeding without a hearing, for example, when:

- the case turns exclusively on questions of contract interpretation that do not require witness testimony;
- the case turns exclusively on a question of law;
- no respondent is participating;
- the value of the dispute is low;
- there is a need for a quick decision.

It should be determined whether the potential benefits of a hearing justify the associated time and cost. The choices made with respect to the organization of the hearing may reduce time and cost and may affect the decision on whether or not to hold a hearing at all.

Appropriate location

Pursuant to Article 18(2) of the Rules, hearings may be conducted at any location and not necessarily at the place of the arbitration. The cost of the hearing can be reduced if a location likely to be advantageous in terms of cost is chosen.

Dates

To avoid delay, the dates for the hearing should be set at the earliest reasonable opportunity and recorded in everyone's calendars. Ideally, the hearing dates should be fixed during the first case management conference.

Attendees

Attendees should be limited to those genuinely necessary for the conduct of the hearing.

Time and cost can be reduced if an informed and knowledgeable party representative with decision-making authority participates in the preparation of and attends the hearing. Such a person will be in a position to make cost/benefit decisions in consultation with outside counsel. For companies, the party representative is often an in-house counsel. For states or state entities, an individual with decision-making authority can be appointed.

Appropriate duration

Under the Rules, there is no prescribed length for hearings. In practice, parties often request hearings that are longer than necessary. However, the longer the hearing, the greater the cost. The length of the hearing should be carefully chosen so as to allow no more time than is necessary for adequately presenting the case.

Use and duration of opening/closing statements

An opening statement is an opportunity to make a summary and synthesis of the case and can help focus the arbitral tribunal's attention on the key issues. The longer the statement, the greater the cost. When the case has already been fully developed in briefs with supporting documents and witness statements, it may not be necessary to repeat these matters in an opening statement.

A closing statement is an opportunity to make a summary and a synthesis of what happened at the hearing. However, if the parties are not given sufficient time to prepare a closing statement, it may be of little use. Furthermore, it may not be necessary to have both a closing statement and a post-hearing brief, as they are likely to repeat each other and unnecessarily increase time and cost.

Direct examination, cross-examination, witness conferencing

In some legal systems, the questioning of witnesses is largely conducted by the arbitral tribunal, with counsel for each side being invited to ask follow-up questions. Under this approach there is no direct examination or cross-examination.

In other legal systems, and increasingly in international arbitration, the questioning of witnesses is largely conducted by counsel through direct examination and cross-examination, with the arbitral tribunal having the right to interject questions or ask questions at the end of the witness's testimony.

The first approach will often result in a shorter and less expensive hearing. The second approach will often allow a more comprehensive examination of the witnesses. Since the first approach leaves the arbitral tribunal largely in control, there is little scope for the parties to make cost/benefit decisions. While the overall duration and cost of the second approach will often be greater, a number of choices can be made to reduce the time and cost, as follows:

Direct examination

Direct examination is the questioning of a witness by the party presenting that witness. In international arbitration, witnesses often submit written witness statements setting forth their evidence. When such statements have been submitted, direct examination may be dispensed with entirely or kept short (e.g. 10 or 15 minutes). This will reduce the length and cost of the hearing.

Cross-examination

Cross-examination is the questioning of a witness presented by the opposing party. If each side is given an

overall allocation of time at the hearing, a party is free to determine how much time to use for each witness so long as the total time is not exceeded. Alternatively, time and cost can be reduced by setting time limits on the cross-examination of witnesses.

Consideration should also be given to the appropriate scope of cross-examination. Limiting its scope to matters covered in a witness's statement or in direct examination, if any, may reduce the length and cost of the hearing.

If it is not necessary to cross-examine certain witnesses who have provided statements for the other side, time and cost can be saved by not doing so. However, in that case, it may be necessary to obtain agreement from the other side or an order from the tribunal stipulating that the decision not to cross-examine a witness does not constitute an admission of the truth of that witness's written statement.

Witness conferencing

Witness conferencing can function as an alternative or an addition to cross-examination. In witness conferencing, two or more witnesses dealing with the same area of evidence are questioned together either by the arbitral tribunal first and then by counsel, or vice versa. The witnesses are also given the opportunity to debate with each other.

Witness conferencing (in particular of expert witnesses) can save time and cost insofar as it helps to focus on, clarify and resolve areas of evidential disagreement.

If the witness conferencing is directed by the arbitral tribunal, the arbitrators will need to prepare carefully beforehand in order to be able to fulfil their inquisitorial role effectively. It may deprive the parties of some control over the presentation of the case.

If the witness conferencing is directed by counsel, they retain greater control over the process and debate can still occur between the witnesses. In addition, the tribunal will have the opportunity to ask its own questions. However, some of the benefits of witness conferencing may be lost as the process is likely to be longer, more expensive and less focused.

Nature of transcripts, if needed

Transcripts are expensive, especially daily transcripts and live transcripts (i.e. real-time transcripts available electronically to participants during the hearing). A cost/benefit decision should be made on what is genuinely necessary. A transcript enables the parties and the tribunal to have a complete and accurate record of the evidence adduced at the hearing. It can be very helpful to the parties when preparing post-hearing briefs, if any, and to the tribunal when preparing the award. In very low value or simple cases, it may be possible to save the expense of a transcript at no great loss. In complex cases with many witnesses, the additional cost of daily transcripts and live transcripts may well be justified. They will facilitate effective cross-examination and be useful when preparing further witness questioning.

Consecutive or simultaneous interpreting, if needed

A choice must be made between simultaneous and consecutive interpreting.

Consecutive interpreting requires fewer interpreters and equipment, but is more than twice as long as simultaneous interpreting, which makes it more costly due notably to the extra time lawyers and experts will have to spend at the hearing. While it may be easier to control the accuracy of consecutive interpreting, that benefit must be weighed against the considerable time and cost it may add to the hearing.

Use of videoconferencing for all or part of the hearing

While it is generally preferable to hold hearings in the physical presence of the arbitrators, the parties and the witnesses, the significant time commitment and travel expenditure this may require from certain witnesses can be avoided by using videoconferencing.

QUESTIONS TO ASK

1. Is an oral hearing necessary for the fair determination of the issues in dispute so as to justify the extra time and cost it involves?
2. Is it necessary to test a written witness statement by cross-examining the witnesses at a hearing?

3. Is there a more convenient location for the hearing than the place of arbitration?
4. What is the earliest time at which dates for the hearing can be set?
5. Who genuinely needs to attend the hearing?
6. Should fact witnesses and/or expert witnesses be allowed to attend the hearing while other witnesses are giving testimony?
7. Taking into account the nature of the issues in dispute, the value of the dispute and the number of witnesses, what is the total number of days genuinely necessary for the hearing? Is the proposed length of the hearing justified in terms of cost?
8. How should the total time of the hearing be allocated between the parties?
9. Should there be an opening statement and if so, how long should it be? Is it genuinely necessary to have both a closing statement and a post-hearing brief? If there is to be a closing statement, how long should it be and how much time should be allocated for its preparation?
10. Does every witness need to be cross-examined?
11. Which areas of evidence require examination and what is the most efficient method of examination (cross-examination or witness conferencing)?
12. Should the hearing be transcribed and if so, should there be daily transcripts and/or live transcripts?
13. If interpreting is needed, should it be consecutive or simultaneous?
14. Should videoconferencing be used for all or part of the hearing?

11. POST-HEARING BRIEFS

PRESENTATION

Parties in an arbitration have the opportunity to present their legal arguments and the relevant facts in pre-hearing submissions and during the hearing itself. The issue here is whether it is necessary or useful for the parties to submit post-hearing briefs.

Post-hearing briefs may be used to draw the arbitral tribunal's attention to relevant facts that have emerged at the hearing and place them in the context of the parties' claims and defences. They may be drafted in a manner that assists the arbitral tribunal with drafting the arbitral award. In some cases, the arbitral tribunal may identify key issues to be addressed by the parties in their post-hearing briefs.

If closing statements are made at the end of a hearing, post-hearing briefs may be unnecessary. Conversely, if there are post-hearing briefs, closing statements may be unnecessary.

Issue: Should there be post-hearing briefs and/or closing statements?

OPTIONS

- A. Proceed directly from the hearing to an award with no closing statements or post-hearing briefs.
- B. Provide for closing statements immediately after the hearing or at some agreed time thereafter, but no post-hearing briefs.
- C. Provide for post-hearing briefs but no closing statements.
- D. Provide for both closing statements and post-hearing briefs.
- E. Post-hearing briefs, if any, can be submitted simultaneously or sequentially, and there can be more than one round of post-hearing briefs.

PROS AND CONS

The submission of post-hearing briefs can serve a number of useful purposes, as mentioned above. In a

long and complex hearing, it may be useful for each party to sum up what they consider to have been demonstrated at the hearing. Post-hearing briefs can include valuable references to the hearing transcript and present a short final synthesis of the evidence and facts of the case, which can be of great value to the arbitral tribunal when drafting the award.

On the other hand, post-hearing briefs add to the cost of the arbitration and may delay the rendering of the award. In addition, they may be of little use if they merely repeat facts and arguments already well understood by the arbitral tribunal.

COST/BENEFIT ANALYSIS

The additional time and expense required for post-hearing briefs need to be balanced against the likelihood that they will genuinely serve one of the purposes indicated above. For example, post-hearing briefs will be especially useful where there are numerous witnesses, complicated or disputed facts, or extensive cross-examination. In all cases, the time and cost associated with post-hearing briefs should be weighed against their likely impact on the arbitral tribunal's decision.

The time and expense required for post-hearing briefs can often be reduced if measures are agreed to keep them relatively short and concise, e.g. limiting the number of pages.

QUESTIONS TO ASK

1. Does the case justify the extra time and expense required for post-hearing briefs, closing statements, or both?

And, in particular,

2. Are post-hearing briefs genuinely useful or necessary for a party to make its case to the arbitral tribunal, and if so, why?

3. What is the estimated cost of preparing the post-hearing briefs?

4. Is the benefit worth the cost, and if so, why?

OTHER POINTS TO CONSIDER

Consider limiting the scope, length and timing of any post-hearing briefs.

Consider having post-hearing briefs filed simultaneously to save time.

In some cases, it may be genuinely necessary to allow each party a short period of time in which to reply briefly to the other party's post-hearing brief.

In some cases, simultaneous post-hearing briefs may have the undesirable consequence of creating a need for further rounds of submissions. Care should therefore be taken to define properly the parameters of post-hearing briefs.

Post-hearing briefs may include submissions on costs, which are normally not discussed at the hearing. This can also save time.

ICC COMMISSION ON ARBITRATION AND ADR

The ICC Commission on Arbitration and ADR is the ICC's rule-making and research body for dispute resolution services and constitutes a unique think tank on international dispute resolution. The Commission drafts and revises the various ICC rules for dispute resolution, including arbitration, mediation, dispute boards, and the proposal and appointment of experts and neutrals and administration of expert proceedings. It also produces reports and guidelines on legal, procedural and practical aspects of dispute resolution. In its research capacity, it proposes new policies aimed at ensuring efficient and cost-effective dispute resolution, and provides useful resources for the conduct of dispute resolution. The Commission's products are published regularly in print and online.

The Commission brings together experts in the field of international dispute resolution from all over the globe and from numerous jurisdictions. It currently has over 850 members from some 100 countries. The Commission holds two plenary sessions each year, at which proposed rules and other products are discussed, debated and voted upon. Between these sessions, the Commission's work is often carried out in smaller task forces.

The Commission aims to:

- Promote on a worldwide scale the settlement of international disputes by means of arbitration, mediation, expertise, dispute boards and other forms of dispute resolution.*
- Provide guidance on a range of topics of current relevance to the world of international dispute resolution, with a view to improving dispute resolution services.*
- Create a link among arbitrators, counsel and users to enable ICC dispute resolution to respond effectively to users' needs.*

ICC Commission on Arbitration and ADR

www.iccwbo.org/commission-arbitration-ADR

commission.arbitrationADR@iccwbo.org

T +33 (0)149 53 30 43

It's The Result That Matters

By Usher Winslett



The purpose of arbitration is elegantly summarized in the introduction to the CPR Non-Administered Arbitration Rules: “The primary objective of arbitration is to arrive at a just and enforceable result, based on a private procedure that is fair, expeditious, economical, and less burdensome and adversarial than litigation.” While most arbitrators would take no issue with this statement, if asked to summarize an arbitrator’s primary obligation, they would reflexively respond, “to render an enforceable award.” But note that the word “award” appears nowhere in the CPR’s mission statement. Indeed, CPR conspicuously avoids using the phrase “enforceable *award*.” By using “enforceable *result*” instead, it puts priorities in the right place. The end result of the arbitration need not be a final award, but it must be fair, expeditious, economical – and, of course, enforceable.

While issuing an enforceable award is certainly an essential goal, it vastly diminishes the arbitrator’s role to call it the *primary* objective. After all, no final award is issued in the overwhelming majority of cases. And the parties are generally better served when their disputes can be resolved without the need for a final award. So, an arbitrator’s foremost, overarching responsibility is to provide parties with the most efficient and economical way to resolve their disputes – which may include, but involves much more than, rendering an enforceable award.

To varying degrees, all arbitral institutions encourage the possibility of a result other than a final award and have incorporated explicit requirements for efficiency and economy in their arbitration rules:

- Article 26 of the DIS (German Institution of Arbitration) Rules provides: “Unless any party objects thereto, the arbitral tribunal shall, at every stage of the arbitration, seek to encourage an amicable settlement of the dispute or of individual disputed issues.” And Article 27 states: “The arbitral tribunal and the parties shall conduct the proceedings in a time- and cost-efficient manner. . . .”
- Article 17 of the UNCITRAL Arbitration Rules provides: “The arbitral tribunal. . . shall conduct the proceedings so as . . . to provide a fair and efficient process for resolving the parties’ dispute.”
- Article 22(1) of the ICC Arbitration Rules states: “The arbitral tribunal and the parties shall make every effort to conduct the arbitration in an expeditious and cost-effective manner”
- The introduction to the ICDR International Dispute Resolution Procedures states: “The ICDR Procedures reflect best international practices that are designed to deliver efficient, economic, and fair proceedings.”

So, when parties agree to have their cases arbitrated under these various rules, they have specifically demanded an efficient, economical dispute resolution process, regardless of whether the tribunal will ever issue a final award. Arbitrators and arbitral institutions need to go beyond lip service to economical and efficient dispute resolution and adjust – or perhaps overhaul – their procedures to make sure those goals are the primary focus.

Don't get me wrong, I am not suggesting that an arbitrator should actively take a mediator's role or that the tribunal should strongarm parties into settling. Rather, arbitrators and arbitral institutions need to modify arbitration procedures to put economy and efficiency first – providing opportunities for the parties to engage in productive settlement discussions throughout the process and incentivizing tribunals to foster early dispute resolution.

How do we do that? The key elements include:

- Maximize client (decision-maker) involvement from the beginning.
- Schedule an “early arbitration review” (with decision-makers present), which may set the stage for settlement discussions.
- Build a settlement discussion window into the schedule.
- Give arbitrators the tools and incentives to promote early dispute resolution.

From my experience as a litigator, mediator, and arbitrator, early settlements typically occur when decision-makers personally weigh costs and benefits, so their involvement is essential.

No mediator I know would consider conducting a mediation without the ultimate decision-makers in the room. There is a good reason for that. The decision-makers need to understand the case not only from their lawyers' perspective but from the other side's perspective and a neutral perspective. The decision-makers also need to get a glimpse of the process. Once they see the sausage being made, they will likely lose their taste for it.

Arbitration rules permit – or even encourage – client participation. For example, Article 24(4) of the ICC Rules allows the tribunal to “request the attendance at any case management conference of the parties in person or through an internal representative.” Nonetheless, arbitrators rarely use this essential tool.

Before beginning my point-by-point description of the procedures I am proposing, I should note that everything I am suggesting should be done with the recognition that ar-

bitration is a party-driven process. And arbitrators should not force or coerce the parties into procedures they do not want. But, that said, these procedures are within the letter and spirit of all major arbitration rules, and offering them to the parties is not just an option – it is an obligation.

Initial Case Management Conference – With Client Participation

Step One: The tribunal should strongly encourage client representatives (preferably the ultimate decision-makers) to participate in the initial case management conference. This will allow the clients to better understand the case and the procedure from the outset. It will give the tribunal the opportunity to convey the option of mediation or non-mediated settlement discussions directly to the parties. And if nothing else, the decision-makers will have a front-row seat to the discussions on how the arbitration will play out. In my experience, when clients are exposed to the minutia of arbitration procedures, they see not only the monetary expense but also the productivity cost – and case fatigue can begin to set in quickly.

At the initial case management conference, the tribunal should encourage the parties to incorporate into the schedule an early arbitration review, followed by a mediation window (or settlement discussion pause) – each discussed below.

Early Arbitration Review – With Client Participation

Before the initial case management conference, the parties will have provided the tribunal, and each other, with their pleadings or the equivalent. Soon after that conference, the parties should produce and provide to the tribunal the documents they plan to rely on at the hearing. Once the tribunal reads the pleadings and the reliance documents, it should have a good initial understanding of the case.

At this point, the tribunal should hold an early arbitration review, giving each party the opportunity to summarize its case and answer questions from the tribunal. This step is like what has become known as a Kaplan Opening, but with a few significant differences. Most importantly, I recommend client participation. I also propose holding the early arbitration review a bit earlier than a standard Kaplan Opening, which is sometimes referred to as a “mid-arbitration review.” In addition, I suggest that the tribunal structure the early arbitration review with a focus on setting the stage for – but not forcing – productive settlement discussions. And finally, unlike Kaplan's proposal, I suggest that the early arbitration review be followed by a pre-scheduled settlement discussion break, such as a mediation window (discussed below).

The tribunal should actively participate in the early arbitration review. The more questions the better. Tribunal questions are, of course, essential to educating the arbitrators, but

they will also focus the advocates' attention on the issues the arbitrators care about and could assist the parties in assessing their likelihood of success.

This procedure will yield multiple benefits: First, as I noted above, it should set the stage for productive settlement discussions. The lawyers, the tribunal, and most importantly, the clients will leave the early arbitration review with a much better understanding of the case. The lawyers and clients will also have a window into the tribunal's early views, based on their questions. And the clients will have another look at the internal workings of the sausage factory. All of this should encourage the parties to take a hard look at settlement.

Even if the early arbitration review does not result in productive settlement discussions, it provides multiple other benefits that should lead to a more efficient and economical dispute resolution. In sum, it will ensure that the tribunal is fully up to speed at an early stage, which will lead to more efficient and better decision-making as the case proceeds. And, through the arbitrators' questions, it will focus the lawyers' attention on the issues that are most important to the tribunal, providing a roadmap for a more streamlined case presentation.

Settlement Discussion Window

One of the biggest impediments to settlement is fear of perceived weakness. Neither side wants to broach the subject out of concern that the mere mention of the idea may damage its negotiating position. Arbitrators can – and should – provide a way for parties to avoid such a standoff. This can be achieved easily by the tribunal raising the idea of a settlement discussion window at the initial case management conference. If the tribunal treats a settlement discussion window as standard operating procedure, then neither side will need to worry about appearing weak by agreeing to it. And once the settlement discussion window is memorialized in the tribunal's procedural order, it will be automatic, so neither side will be inclined toward tactical hesitation.

Ideally, the settlement discussion window should immediately follow the early arbitration review. At that point in the proceedings, each side will have just heard a summary of the other side's case and the tribunal's questions to both sides. Assuming the decision-makers from each side participated in the early arbitration review, they will be well informed and should be able to rationally analyze the costs and benefits of settling versus arbitrating.

I am using the term "settlement discussion window" instead of "mediation window" because I believe the tribunal should try to incorporate a time for the parties discussing settlement into the schedule even in cases where the parties may not want to incur the cost of retaining a mediator. Nonetheless, the most productive settlement discussions

usually involve a mediator, so I suggest encouraging a "mediation window" and using a "settlement discussion window" as a fallback.

Assuming the parties elect to use a mediator, the next question is who will serve in that capacity? The parties may try to recruit the arbitrator or a member of the tribunal, assuming they can save time and money by using someone who is already familiar with the case. I suggest foreclosing that option at the outset. It is too fraught and, if the case does not settle, could result in a challenge to the award.

In sum, I recommend raising the idea of a settlement discussion window (or mediation window) at the initial case management conference, treating it as standard operating procedure, coupling it with the early arbitration review, and incorporating both into the tribunal's first procedural order.

Give Arbitrators the Tools and Incentives To Promote Early Dispute Resolution

The arbitration rules and guidelines of major arbitration institutions provide for a mediation option and expressly encourage arbitrators to shepherd the parties toward settlement. Nonetheless, arbitrators rarely incorporate the steps necessary to encourage settlement into their procedures, so we need significant structural changes in terms of both education and incentives.

Arbitration institutions must implement policies to ensure that arbitrators use all available tools to set the stage for productive settlement discussions. The institutions should educate arbitrators on their overarching obligation to resolve disputes in the most efficient and economical way. They need to provide arbitrators with procedural order templates that include things like early arbitration reviews and settlement discussion windows. And perhaps most important, they should modify their fee structures to incentivize – or at least minimize disincentivizing – early dispute resolution.

Although arbitrators routinely put their own interests behind those of the parties, the arbitration institutions, and the arbitral process, it is still an undeniable fact that the compensation structures of most arbitration institutions create a financial disincentive for early dispute resolution. And we need to at least consider the possibility that those existing structures may be hindering adoption of early dispute resolution methods.

I am not suggesting that arbitrators are consciously prolonging arbitrations to benefit themselves. But I am suggesting that arbitration institutions, like any efficiently run business, should align their financial incentives with their goals. And since their primary goal should be efficient, economical dispute resolution, it would benefit both the parties and the

arbitrators to financially incentivize that result to the extent possible and practical.

In a system that is largely billed by the hour, it is difficult to incentivize efficiency, and I do not have a silver bullet solution, but a non-hourly compensation system like the one used by the ICC could hold the answer if properly applied. The current ICC Rules include enough flexibility to incentivize efficient early dispute resolution. Article 2(2) of Appendix III to the ICC Rules provides that “[i]n setting the arbitrator’s fees, the [ICC] Court [of Arbitration] shall take into consideration the diligence and efficiency of the arbitrator, the time spent, the rapidity of the proceedings, [and] the complexity of the dispute,” among other things. Unfortunately, even with that flexibility, the ICC rarely compensates arbitrators in a way that puts an appropriate value on a quick, efficient resolution.

Another possibility would be for arbitration institutions to follow the lead of law firms – which routinely front-end load their compensation. When taking on a new case, many law firms will require a recoupable-but-non-refundable retainer payment. The retainer payment addresses the fact that the firm incurs significant transaction costs when initiating a new representation. Among other things, the firm must clear conflicts, and the attorneys who will be working on the new matter must allocate time on their schedules. As a result of both, the firm might lose work from other clients, so it is only fair that a chunk of the firm’s compensation is paid up front. Moreover, if the matter is resolved quickly, everybody

wins: the client avoids the cost of a prolonged dispute, and the lawyers are compensated above their hourly rate.

All the above is also true for arbitrators, but the fee structures of most arbitration institutions include nothing akin to the front-end loading of a recoupable-but-non-refundable retainer payment for arbitrators.

Different institutions may choose different procedures, but the bottom line is that arbitration institutions need to revamp their rules – including their compensation structures – to put the proper focus on efficiency and economy.

Conclusion

To summarize, encouraging client involvement, holding an early arbitration review, scheduling a settlement discussion window, and incentivizing arbitrators to promote settlement are key to arriving at a just and enforceable *result*. But tribunals must also use all available cost-saving tools, like bifurcation, dispositive motions, streamlined procedures (like having the chair alone oversee all issues that arise between the initial case management conference and the evidentiary hearing), and emerging technologies. Bottom line: economy and efficiency should be the overarching consideration in every decision the tribunal makes. If arbitrators focus solely on their mandate to issue an enforceable award, they run the risk of overlooking the broader goals of arbitration. By adhering to the principles already enshrined in institutional rules and employing the procedures discussed here, arbitrators can conduct proceedings in a way that will serve the parties’ fundamental aims. After all, it’s the result that matters.

Usher Winslett has been an ADR professional since 1996, handling more than 140 international and domestic disputes as an arbitrator or mediator of commercial, intellectual property, employment, insurance, and entertainment claims. He is based in New York and South Carolina but works internationally and remotely.

- [Guide on Effective Conflict Management \(2023\)](#)
- [Report on Facilitating Settlement in International Arbitration \(2023\)](#)
- [ICC releases Guide for Disability Inclusion in International Arbitration and ADR \(2023\)](#)

ICCA

INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION



ICCA–IBA Joint Task Force on Data Protection in International Arbitration

ROADMAP TO DATA PROTECTION
IN INTERNATIONAL ARBITRATION

with the assistance of the
Permanent Court of Arbitration
Peace Palace, The Hague



The ICCA Reports No. 7

INTERNATIONAL COUNCIL FOR
COMMERCIAL ARBITRATION

ICCA–IBA JOINT TASK FORCE
ON DATA PROTECTION IN
INTERNATIONAL ARBITRATION

ROADMAP TO DATA PROTECTION IN
INTERNATIONAL ARBITRATION

THE ICCA REPORTS NO. 7

2022

ICCA is pleased to present the ICCA Reports series in the hope that these occasional papers, prepared by ICCA interest groups and project groups, will stimulate discussion and debate.

INTERNATIONAL COUNCIL FOR
COMMERCIAL ARBITRATION

ICCA–IBA JOINT TASK FORCE
ON DATA PROTECTION IN
INTERNATIONAL ARBITRATION

ROADMAP TO DATA PROTECTION IN
INTERNATIONAL ARBITRATION

THE ICCA REPORTS NO. 7

2022

with the assistance of the
Permanent Court of Arbitration
Peace Palace, The Hague



www.arbitration-icca.org

Published by the International Council for Commercial Arbitration
www.arbitration-icca.org

ISBN 978-94-92405-34-0

All rights reserved.

© 2022 International Council for Commercial Arbitration and
the International Bar Association

The International Council for Commercial Arbitration (ICCA) and the International Bar Association (IBA) wish to encourage the use of this Report for the promotion of arbitration. Accordingly, it is permitted to reproduce or copy this Report, provided that the Report is reproduced accurately, without alteration and in a non-misleading context, and the authorship and copyright of ICCA and the IBA are clearly acknowledged.

For further information, please contact us at bureau@arbitration-icca.org.

All views expressed in this Report are those of the Task Force and not ICCA, the IBA or their governing bodies or members. This Report is the result of the collective efforts of the Task Force, the views expressed are not attributable to any particular Task Force member and all Task Force members served in their individual capacity.

About ICCA

ICCA is a worldwide nongovernmental organisation (NGO) devoted to the use and improving the processes of arbitration, conciliation and other forms of resolving international disputes. Its activities include convening biennial international arbitration congresses; sponsoring authoritative dispute resolution publications (including the ICCA Yearbook Commercial Arbitration, International Handbook on Commercial Arbitration and ICCA Congress Series); and promoting the harmonisation of arbitration and conciliation rules, laws and standards. ICCA has official status as an NGO recognised by the United Nations. See www.arbitration-icca.org.

About the IBA

The IBA is the foremost organisation for international legal practitioners, bar associations and law societies. Established in 1947, shortly after the creation of the United Nations, the IBA was born out of the conviction that an organisation made up of the world's bar associations could contribute to global stability and peace through the administration of justice. The present membership is comprised of more than 80,000 individual international lawyers from most of the world's leading law firms and some 190 bar associations and law societies spanning more than 170 countries.

The IBA Arbitration Committee focuses on the laws, practice and procedures relating to the arbitration of transnational disputes. It currently has over 3,000 members. Through its publications and conferences, the Committee seeks to share information about international arbitration, promote its use and improve its effectiveness. The Committee maintains standing subcommittees and, as appropriate, establishes task forces to address specific issues.

ACKNOWLEDGEMENTS OF THE CO-CHAIRS

In view of the complexity and importance of the ICCA-IBA Roadmap to Data Protection in International Arbitration (“Roadmap”), it is impossible to acknowledge all those who contributed to the project. Yet, the Roadmap would not have seen the light of day without the invaluable contributions of the following individuals and organisations.

First, the members and rapporteurs of the ICCA-IBA Joint Task Force on Data Protection in International Arbitration (“Task Force”) have devoted countless hours, attending task force meetings, drafting and reviewing the Roadmap and the Annexes, and hosting and participating in events to ensure we had adequate feedback from the arbitration community, as well as the many other administrative tasks involved in a project of this size. Thank you for all you have contributed, for your good cheer and constructive attitude throughout the process. A special word of thanks goes to Emily Hay of Hanotiau & van den Berg, for her generosity and hard work, without which this Roadmap simply would not have been possible.

We would also like to extend our heartfelt thanks and appreciation to ICCA President Lucy Reed, past-Presidents Gabrielle Kaufmann-Kohler (Lévy Kaufmann-Kohler) and Donald Donovan, the ICCA Governing Board, Lise Bosman (Executive Director), Lisa Bingham (Deputy Executive Director), and the members of the ICCA Bureau, whose support throughout the process has been invaluable.

We would also like to sincerely thank the Arbitration Committee of the International Bar Association, and especially its present and past co-chairs, Eduardo Silva Romero, Gaetan Verhoosel, Philippe Pinsolle, Julie Bédard, Samaa Haridi and Valeria Galindez for their support and contributions throughout the project. Special thanks goes to Xavier Favre-Bulle for the thoughtful and constructive input he has provided on the successive drafts.

We are also grateful to the representatives of all the arbitration institutions and international organizations who kindly devoted their time to discussing the Roadmap with the Task Force and commenting on drafts, including the AAA-ICDR, HKIAC, ICC, LCIA, SCC, SIAC, DIS, and VIAC as well as ICSID, the PCA and the WIPO. We know your time is valuable, and we appreciate your help enormously.

We would also like to give our thanks and appreciation to Tatiana Campello (Demarest) and Rodrigo Azevedo (Silveiro), and Aaron Kamath (Nishith Desai) and Payel Chatterjee (Adani Enterprises), who, although not being Task Force members, generously gave their time to address the data protection laws of Brazil and India for the Roadmap.

THE ICCA REPORTS

Likewise, we are grateful to members of the arbitration community who took the time to provide their comments on the public draft of the Roadmap, and whose input was extremely valuable.

Lastly, we would like to thank the law firms of Ambos Law, Derains & Gharavi and Hanotiau & van den Berg for their generous support throughout the process.

The bottom line is that this was a collective effort, going well beyond the Task Force itself. We greatly enjoyed the exchanges and remain forever grateful for all your contributions to the ICCA-IBA Roadmap to Data Protection in International Arbitration.

Kathleen Paisley
Melanie Van Leeuwen
Co-chairs

MEMBERS OF THE ICCA–IBA JOINT TASK FORCE ON DATA PROTECTION IN INTERNATIONAL ARBITRATION

Co-Chairs

Kathleen Paisley, Ambos Lawyers

Melanie van Leeuwen, Derains & Gharavi

Members

Lawrence Akka QC, 20 Essex Street

Rosa Barcelo, McDermott Will & Emery

Niuscha Bassiri, Hanotiau & van den Berg

Markus Burianski, White & Case

Hugh Carlson, Three Crowns

Daniel Cooper, Covington & Burling LLP

Javier Fernandez-Samaniego, Samaniego Law

Hilary Heilbron QC, Brick Court Chambers

Robert Maddox, Debevoise & Plimpton LLP

Charlie Morgan, Herbert Smith Freehills LLP

Philippe Pinsolle, Quinn Emanuel Urquhart & Sullivan LLP

Jacques de Werra, University of Geneva

Rapporteurs

Emily Hay, Hanotiau & van den Berg

Brianna Gorence, Freshfields Bruckhaus Deringer

Table of Contents

ACKNOWLEDGEMENTS OF THE CO-CHAIRS	vii
MEMBERS OF THE ICCA–IBA JOINT TASK FORCE	ix
INTRODUCTION	1
A. Data Protection and Arbitration	1
B. Intended Scope and Purpose of the Roadmap	3
I. GENERAL DATA PROTECTION PRINCIPLES RELEVANT TO INTERNATIONAL ARBITRATION	7
A. Material Scope of Data Protection Laws	8
1. Personal Data	9
2. Data Subject	9
3. Processing	9
B. Jurisdictional Scope of Data Protection Laws	10
C. Roles under Data Protection Laws	11
1. Data Controllers	12
2. Joint Controllers	13
3. Data Processors	14
D. Lawful Basis for Processing	15
E. Data Transfer Rules	17
F. Data Protection Principles Applicable in Arbitration	19
1. Fair and Lawful Processing	20
2. Proportionality	21
3. Data Minimisation	22
4. Purpose Limitation	24
5. Data Subject Rights	25
6. Data Accuracy	27
7. Data Security and Data Breach	27
8. Transparency	29
9. Accountability	30
II. DATA PROTECTION COMPLIANCE IN INTERNATIONAL ARBITRATION PROCEEDINGS	32
A. Preparing for the Arbitration	32
1. Applicable Data Protection Laws	34
2. Roles of Arbitral Participants	35
3. Use of Service Providers	35
4. Data Collection and Review	36

THE ICCA REPORTS

B. During the Arbitration	37
1. Filing the Request for Arbitration	37
2. Appointment of Arbitrators	39
3. Documenting Data Protection Compliance	40
4. When Data Protection Issues Arise During the Proceedings	57
5. Remote Hearings	62
6. Arbitral Awards and Other Decisions	63
C. After the Arbitration	64
CONCLUSION	66
ANNEXES	67
ANNEX 1 – Glossary	68
ANNEX 2 – Data Protection Practice Tips	75
ANNEX 3 – Checklist: Data Protection Considerations	78
ANNEX 4 – Checklist: Online Case Management Platform	85
ANNEX 5 – Checklist: Legitimate Interests Assessment	88
ANNEX 6 – Sample Standard Contractual Clauses for Controller-Controller Transfers under the GDPR	90
ANNEX 7 – Sample Provisions for Data Protection Directions	112
ANNEX 8 – Sample Data Protection Protocol under the GDPR	118
ANNEX 9 – Sample Privacy Notices	126
ANNEX 9A – Data Privacy Notice for Arbitral Institutions	127
ANNEX 9B – Data Privacy Notice for Arbitrators	134
ANNEX 9C – Data Privacy Notice for Legal Counsel	141
ANNEX 10 – List of Sources by Category	149
ANNEX 11 – Compendium of Selected Data Protection Laws	154

INTRODUCTION

This ICCA-IBA Roadmap to Data Protection in International Arbitration (“**Roadmap**”) has been developed by the ICCA-IBA Joint Task Force on Data Protection in International Arbitration as a tool to assist arbitration professionals in applying data protection and privacy laws during international arbitration proceedings.

A. DATA PROTECTION AND ARBITRATION

The European Union’s (“EU”)¹ General Data Protection Regulation² (“**GDPR**”) and similar laws in other jurisdictions³ apply as a matter of law to the collection, retention, processing and security policies of personal data, including during arbitration proceedings. As non-compliance may trigger civil and/or criminal liability (for example, under the GDPR potential fines for non-compliance may rise to 4% of global gross revenue

-
1. “European Union” or “EU” designates the current twenty-seven EU Member States: Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the Netherlands. It bears noting that the Roadmap throughout uses the term “EU”, while in fact the scope of application of the GDPR extends to the whole European Economic Area (“EEA”). The EEA encompasses the 27 EU Member States and three additional states: Iceland, Liechtenstein and Norway. On 31 January 2020, the United Kingdom withdrew from the EU. The UK General Data Protection Regulation (“UK-GDPR”) mirrors the GDPR and has been deemed by the EU to be adequate and the UK is an adequacy country. Therefore, at the time of writing, although the UK is no longer a member of the EU, the provisions described herein generally apply in the UK as a matter of application of the UK-GDPR.
 2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4.5.2016.
 3. To assist in deciding the scope of potential legal responsibilities, [Annex 11](#) contains a table including a non-exhaustive list of references to national and regional data protection laws of important arbitration jurisdictions, including those where the EU has issued adequacy decisions. Moreover, in the EU, it is important to keep in mind that, even when the GDPR applies, the national laws of the relevant EU country also need to be considered. Although the GDPR is a European Regulation that should be consistently applied throughout the EU without the need for national implementing legislation, the GDPR itself allows EU Member States discretion (described as a “margin of manoeuvre”) and the possibility to implement derogations in several areas potentially relevant to arbitration (*e.g.*, GDPR Recital 10). [Annex 11](#) also includes a list of the data protection laws of the EU Member States.

or EUR 20 million, whichever is higher⁴), it is important for arbitration professionals to consider what data they process, as well as where, why, by what means, with which information security measures and for how long they do so.

Data protection laws and regulations are generally of mandatory application. They prescribe the legal rules applicable whenever personal data is processed, including when, where and how personal data may be processed. However, such laws and regulations do not address how they should be applied in specific contexts, such as in arbitration. Moreover, although data protection authorities have provided guidance as to the way data protection rules should be given effect in certain industries, such guidance is not yet available for international arbitration. It is also not possible to draw conclusions from how such laws apply to courts, because, at least in the EU, courts are generally not subject to the jurisdiction of the data protection authorities. It is therefore necessary for arbitration professionals to consider how these laws apply to them generally and in their cases specifically.

In the absence of specific guidance, it is important to think through the steps of the arbitral process and document the data protection and procedural measures adopted in the different phases of an arbitration within the framework of whatever data protection law(s) apply. To assist in that process, this Roadmap identifies the data protection issues that may arise in the context of international arbitration proceedings, as well as solutions that may be adopted to address them.

Data protection obligations apply to the processing of personal data by individuals and legal entities that fall within the material and jurisdictional scope of the relevant data protection law. Therefore, it is not the processing of personal data for the arbitration as such that is subject to the data protection laws. Rather, the individuals and entities that are involved in the arbitration are subject to the data protection laws. Each of them may fall under the scope of a different data protection law, or none at all, which means that in any arbitration proceedings, different data protection rules may apply to different participants. Some of those involved may have certain data protection obligations and others may not.

4. Under the Lei Geral de Proteção de Dados (Brazilian General Data Protection Act) (Statute 13709/18) (“Brazil Act” or “LGPD”), the fines may be up to 2% of gross revenue in Brazil or BRL 50 million. The Brazil Act unified 40 pre-existing laws to regulate processing of the personal data of individuals. The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. (“California Act” or “CCPA”) similarly provides for monetary penalties: depending on where the violation occurred, the penalty may be up to USD 2,500 for each violation or USD 7,500 for each international violation. In addition, and unlike the GDPR and the Brazil Act, the California Act does not provide a maximum amount of penalty.

It is important to appreciate that if even one participant in an arbitration is subject to data protection obligations, this may have an impact on the conduct of the arbitration as a whole. This is because the participant's compliance with its data protection obligations may have a spill over effect on the arbitration and require others to process the personal data for the arbitration in a particular way.

B. INTENDED SCOPE AND PURPOSE OF THE ROADMAP

The Roadmap's intended scope and purpose consists of the features set forth in this Section.⁵

Types of Proceedings. The type of arbitration (for example, commercial or investor-State) typically does not determine whether data protection laws apply.⁶ Rather, the application of data protection laws is determined by whether the data processing during the arbitration by a specific participant falls within the material and jurisdictional scope of a relevant law.

Arbitral Participants. The Roadmap is only addressed to **Arbitral Participants**, which is defined in the Roadmap as, and limited to, the parties, their legal counsel, the arbitrators and arbitral institutions. However, while it is not explicitly addressed to them, the guidance provided herein is also relevant to those working for or with Arbitral Participants during an arbitration, such as tribunal secretaries, experts and service providers (*e.g.*, e-discovery experts, information technology professionals, transcribers, translation services, online case management platform providers, remote hearing platform providers, etc.). Therefore, Arbitral Participants who are assisted by others during the arbitral process should consider how data protection laws affect those relationships, taking into consideration that:

-
5. While data protection laws apply in a similar manner to professionals and entities involved in mediation and forms of alternative dispute resolution, they are not expressly addressed in this Roadmap. Moreover, in many jurisdictions, including those of the EU, special rules apply to courts, including self-regulation and certain exemptions, which are also not addressed in this Roadmap.
 6. In the case of arbitrations administered by an international organisation, determining whether any relevant privileges and immunities will impact the application of data protection laws turns on the breadth and scope of the relevant privileges and immunities, as well as the language of the relevant data protection law, both in terms of whether data protection laws would come within their scope, and, if so, which Arbitral Participants would be covered by them. This is an institution-specific and arbitration-specific enquiry, which is beyond the scope of this Roadmap.

- where an Arbitral Participant is a legal entity,⁷ employees of that entity are not considered separately for compliance purposes, rather their actions are attributed to that entity;
- where arbitration-related information containing personal data is shared with a third party,⁸ this is considered to be processing, which requires compliance with data processing rules and transfer restrictions; and
- where an Arbitral Participant uses a third party to undertake data processing activities on its behalf (such as a data analytics company), both parties are responsible for compliance with the data protection laws during that processing.⁹

General Data Protection Principles. The Roadmap addresses data protection compliance in international arbitration with reference to general data protection principles, rather than the law of a particular jurisdiction (unless otherwise indicated by way of illustration). However, the examples provided in the Roadmap are often based on the GDPR because it is one of the most comprehensive and onerous data protection regulations, and is becoming a global reference. The GDPR and its predecessor legislation, the Data Protection Directive,¹⁰ have been widely drawn upon by jurisdictions across the globe for their data protection laws, which are referred to in the Roadmap as “EU-style” data protection laws.

Roadmap Organisation. The Roadmap is divided into two sections:

- [Section I](#) describes the primary data protection principles potentially applicable to international arbitration; and

7. The entity may qualify as a data controller. A “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (GDPR Art. 4(7)).

8. A “third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (GDPR Art. 4(10)).

9. GDPR Data Controllers and Data Processors, <https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/>.

10. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281/31, 24.10.1995 (“Data Protection Directive”).

- [Section II](#) addresses how the data protection principles may apply during the different stages of an international arbitration, and how they may affect the Arbitral Participants during the arbitral process.

Roadmap Annexes. In order to provide practical guidance to practitioners, the Roadmap is accompanied by a set of Annexes that provide greater detail, practical information, checklists, sample language, and references aimed at enabling Arbitral Participants to apply data protection principles in the context of an arbitration, and a glossary of data protection terms, which are also defined in the footnotes. These Annexes are organised as follows:

- [Annex 1](#) contains a glossary of data protection terms;
- [Annex 2](#) contains practice tips for applying data protection principles in specific cases;
- [Annex 3](#) provides a more detailed checklist addressing how to operationalise these tips;
- [Annex 4](#) provides a checklist on the use of an Online Case Management Platform;
- [Annex 5](#) contains a non-exhaustive list of considerations that should be applied in performing a Legitimate Interests Assessment;
- [Annex 6](#) provides a sample set of “standard contractual clauses” for controller-controller transfers under the GDPR;
- [Annex 7](#) contains some non-exhaustive sample provisions for data protection directions for the first procedural order or the terms of reference;
- [Annex 8](#) contains a sample data protection protocol, taking into account the GDPR;
- [Annex 9](#) provides sample data privacy notices for (A) arbitral institutions (other than international organisations),¹¹ (B) arbitrators, and (C) legal counsel;
- [Annex 10](#) provides a list of sources per category, used in the drafting of this Roadmap; and
- [Annex 11](#) contains a compendium of selected data protection laws.

Goal. The aim of the Roadmap is to enable Arbitral Participants to identify and effectively address data protection issues in the context of arbitral proceedings. There are sensible solutions to the data protection challenges that arise in arbitrations, and Arbitral Participants should become familiar with the issues and become accustomed to dealing with them.

11. See [fn. 6](#).

No Legal Advice. Data protection laws impose mandatory legal obligations on those coming within their scope. Importantly, while providing guidance, nothing in the Roadmap or Annexes can be taken as legal advice. The Roadmap provides information and resources to foster a better understanding of the data protection rules that may apply during an arbitration, and the Arbitral Participants' potential obligations thereunder. However, assessing data protection obligations is a fact-driven and case-specific undertaking.

The Roadmap and its Annexes will necessarily be a living document. Over time, data protection authorities and courts may clarify how data protection laws should be applied to international arbitration, whilst recognising the balance that must be struck given the important role arbitration plays in the administration of justice and the enforcement of legal rights and obligations on the international plane.

I. GENERAL DATA PROTECTION PRINCIPLES RELEVANT TO INTERNATIONAL ARBITRATION

The purpose of this Section of the Roadmap is to provide a general understanding of the data protection principles embodied in most EU-style data protection laws as they may apply to international arbitration. The EU, Brazil,¹² Canada,¹³ India,¹⁴ and the State of California¹⁵ are used as examples to give context. However, similar principles apply under many other EU-style data protection regimes. For the avoidance of doubt, references to specific legislation or to a jurisdiction serve as an indication only.

General Obligations. Arbitral Participants have general obligations under the data protection laws that apply to their data processing activities regardless of their involvement in a specific arbitration.¹⁶ The extent of these obligations will depend on the applicable law and the Arbitral Participant's status under that law as a data controller, joint controller or a data processor. Arbitral Participants will generally be data controllers, and joint controllers under certain circumstances. For data controllers and joint controllers (who are jointly responsible), these obligations typically include ensuring and demonstrating compliance, ensuring the lawfulness of their personal data processing and transfers, minimising the personal data they process, issuing GDPR-compliant data privacy notices, and adopting appropriate data security measures, data breach procedures, data retention policies, and procedures for addressing data subject complaints.¹⁷

12. *See* Brazil Act.

13. Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"), SC 2000, c 5, <http://canlii.ca/t/541b8> retrieved on 20 September 2020, which applies to organisations that collect, use or disclose personal information in the course of commercial activities in Canada.

14. India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011 ("India Act"), which addresses data protection in certain contexts and for certain types of data. India has also proposed a comprehensive data protection law, which has yet to be adopted.

15. *See* California Act.

16. In the case of arbitrations administered by an international organisation, *see* [fn. 6](#).

17. *See, e.g., Annex 3*, which provides a checklist of data protection issues that Arbitral Participants may want to consider. While the most important way to avoid liability is through compliance, given the interlinking nature of these obligations and the potential risk of non-compliance, Arbitral Participants should consider taking out insurance, and where appropriate imposing insurance obligations and indemnities on each other during proceedings where there are significant data protection risks.

A. MATERIAL SCOPE OF DATA PROTECTION LAWS

EU-style data protection laws apply whenever:

- “personal data” about a
- “data subject” is
- “processed”,

during activities falling within the jurisdictional scope of the relevant data protection laws.

Understanding the concepts of “personal data”,¹⁸ “data subjects”¹⁹ and “processing”²⁰ is therefore key to understanding how data protection laws function. “Personal data” and “processing” are broadly defined notions, which encompass information that may not traditionally have been thought of as confidential or sensitive, as well as most of the activities typically undertaken by Arbitral Participants in the context of an arbitration.

18. “Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art. 4(1)); information regarding an identified or identifiable natural person (Brazil Act Art. 5(I)).

19. “Data subject” means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art. 4(1)); a natural person to whom the personal data that are the object of processing refers (Brazil Act Art. 5(V)).

20. “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR Art. 4(2)); any operation carried out on personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction (Brazil Act Art. 5(X)).

1. Personal Data

Many data protection laws define personal data to include “any information relating to an identified or identifiable natural person” (*e.g.*, GDPR Art. 4; Brazil Act Art. 5, I; and California Act Sections 1798.140(b) and (o)²¹).

Under many laws, including, for example, the GDPR and the Brazil Act, it is irrelevant that the personal data is contained in a business-related document (such as work files, work emails, laboratory notebooks, agreements, construction logs, etc.). Provided that the data relates to an individual who is identified or identifiable, it is considered to be personal data covered by the data protection laws.

A substantial portion of the information exchanged during a typical international arbitration is therefore likely to contain data that qualifies as personal data.

2. Data Subject

Individuals who are identified or identifiable from the data are referred to as “data subjects”. Legal entities are not data subjects.²²

3. Processing

Data protection laws impose obligations that must be complied with whenever personal data is “processed”.

Processing is broadly defined to include not only active steps such as collecting, using, disseminating and deleting data, but also passive operations such as receiving, holding, organising and storing data. Moreover, data protection laws usually apply not only to electronically processed information, but also to data in (or intended for) a paper filing system (*e.g.*, GDPR Recital 15, Art. 2(1))²³ or similar means (*e.g.*, Brazil Act Art. 1).²⁴

21. While the definition of “personal information” under the California Act is substantially similar to “personal data”, personal information under the California Act does not extend to publicly available information, which is information that is lawfully made available from federal, state, or local government records, if that data is used for a purpose that is compatible with the purpose for which the data is maintained and made available in the government record.

22. See [fn. 19](#).

23. A “filing system” means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (GDPR Art. 4(6)).

24. “This Act provides for the processing of personal data, including by digital means...” (Brazil Act Art. 1).

Most activities undertaken in a typical international arbitration are thus likely to constitute processing.

B. JURISDICTIONAL SCOPE OF DATA PROTECTION LAWS

The jurisdictional scope of EU-style data protection laws is broad, and they often apply extraterritorially. For example, the GDPR applies whenever personal data is processed:

- In the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not (GDPR Art. 3(1)); or
- Where the processing activities are related to the offering (targeting) of goods or services to individuals in the EU (regardless of their residence or citizenship) (GDPR Art. 3(2)(a)).

Moreover, even where the GDPR does not apply as a matter of law, some of its provisions may still apply as a matter of agreement. For example, under the GDPR, whenever personal data is transferred to international organisations or to countries that have not been found by the EU to provide adequate protection,²⁵ transferors are required to put “adequate protections” in place where feasible. In the case of arbitration, as discussed below in [Sections I.E](#) and [II.B.3.c\(2\)](#), this is likely to take the form of standard contractual clauses, pursuant to which the parties agree by contract to abide by the most important provisions of the GDPR. This leads to significant scope creep, even beyond the already broad territorial reach of the GDPR. Similar provisions are found in numerous other EU-style data protection laws throughout the world.²⁶

25. The EU considers that the data protection laws of Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay are adequate (see [Annex 11](#)). The EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the European Commission to provide a basis for data transfers with adequate data protection from the EU to the US, was invalidated by the CJEU in the 2020 *Schrems II* decision. See Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems*, C-311/18, ECLI:EU:C:2020:559. In March 2022, the EU and the US announced an in-principle agreement on a new “Trans-Atlantic Data Privacy Framework” to be put in place to address the *Schrems II* decision.

26. The Brazil Act, for example, applies to any data processing operation carried out by a natural person or by a public or private legal entity, regardless of the medium, the country of its headquarters or the country where the data is located, provided that: (1) the processing operation is carried out in the Brazilian territory; (2) the processing activity aims at offering or supplying goods or services or processing data of individuals located in the Brazilian territory; or (3) the

Example: An EU-based arbitrator is appointed in an arbitration administered by a non-EU based institution. No other Arbitral Participant is subject to the GDPR. The EU-based arbitrator will be bound by the GDPR and obliged to process any personal data in connection with the arbitration in compliance with the GDPR's requirements, including having a lawful basis for transferring data outside the EU in connection with the arbitration. Depending on the circumstances, this may involve putting in place European Commission-approved standard contractual clauses, which will have the practical result that the non-EU based Arbitral Participants agree to be bound by the main provisions of the GDPR. Where it is not feasible to put standard contractual clauses in place for a justifiable reason, it may be possible to transfer based on the derogation for transfers "necessary for the establishment, exercise or defence of legal claims".²⁷

C. ROLES UNDER DATA PROTECTION LAWS

Arbitral Participants covered by an EU-style data protection regime have obligations under the data protection laws that apply to their data processing activities including during an arbitration.

personal data subject to processing has been collected on Brazilian territory (Brazil Act Art. 3). The California Act applies to organisations "doing business in California", a criterion that is not precisely defined within the law. However, citing the California Franchise Tax Board, commentators have written that "out-of-state entities collecting, selling or disclosing personal information of California residents [may be understood to] fall under the scope of the CCPA" if they are "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit." (Data Guidance, *Comparing Privacy Laws: GDPR v. CCPA*, available at https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf).

27. The GDPR provides a specific derogation or exception from certain of its provisions where processing is "necessary for the establishment, exercise or defence of legal claims", which should be applied to arbitration and is referred to herein as the "Legal Claims Derogation". This includes: (1) the derogation from the GDPR's third-country transfer restrictions for transfers (GDPR Art. 49(1)(e)); (2) a lawful basis for processing sensitive data (GDPR Art. 9(2)(f)); (3) an exception to the right to erasure or to stop processing (GDPR Art. 17(3)(e)); and (4) as applied by some Member State laws, to allow the processing of Criminal Offence Data.

The extent of these obligations depends on the Arbitral Participant's status under the applicable data protection law as a controller (who often will be acting in parallel with other independent controllers), a joint controller,²⁸ or a processor.²⁹

1. Data Controllers

Under EU-style data protection laws, the data controller is primarily responsible for compliance and demonstrating compliance. Data controllers can be natural or legal persons, irrespective of (1) whether they are for profit or not;³⁰ (2) whether they are private law or public law entities; and (3) their size.

The data controller determines “the purposes and means of the processing of personal data”.³¹ Applying this definition, most Arbitral Participants are likely to be considered data controllers because, by virtue of their function, they control the purpose and means of the processing of personal data in the context of an arbitration (although they do not control the processing of data by other Arbitral Participants). For example, both barristers³² and solicitors³³ are typically considered to be data controllers by data protection authorities in the EU and the UK when performing case work.

28. “Joint controllers” are where two or more controllers jointly determine the “purposes and means” of the data processing (GDPR Art. 26(1)).

29. A “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR Art. 4(8)).

30. An exception being California where the California Act only extends to controllers that are for-profit.

31. *See, e.g.*, GDPR Art. 4(7); Brazil Act Art. 5(VI).

32. With respect to data controllers, the EU Working Party has illustrated the concept of a data controller in the following example: “A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client’s case. The legal ground for making use of the necessary information is the client’s mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as independent “controllers” when processing data in the course of legally representing their client.” EU Working Party, “Opinion 1/2010 on the Concepts of ‘Controller’ and ‘Processor’”, WP 169, 16 February 2010, at 29 (“Controller/Processor Opinion”).

33. The ICO is the UK Information Commissioner’s Office set up to uphold information rights, including under data protection law. The ICO has taken the view that solicitors are data controllers. *See* Controller/Processor Opinion, at 28; ICO, “Data controllers and data processors: what the difference is and what the governance implications are”, Data Protection Act 1998, paras 40-43.

2. Joint Controllers

The GDPR has introduced the concept of “joint controllers” who “jointly” determine the “purposes and means” of the data processing.³⁴ Where the GDPR applies, each of the joint controllers is responsible for compliance with the GDPR. They are also *jointly and severally liable for any data protection violation* with a possibility for recourse against the other joint controller(s) if it can be established that they were responsible for part of the damage.³⁵ This concept is similarly found in other newer data protection laws enacted after the GDPR, like the Brazil Act, but not in many older data protection laws.³⁶ If Arbitral Participants are joint controllers, they are required to make arrangements to allocate the risks involved, for example through a data protection protocol.³⁷

The possibility of shared or parallel responsibility of Arbitral Participants bears out the importance of data protection compliance by all Arbitral Participants. Although not specifically related to arbitration, decisions of the Court of Justice of the European Union (“CJEU”) under the Data Protection Directive indicate that the notion of joint controllership is to be broadly interpreted. However, the liability of a joint controller is limited to the processing of data for which that controller “actually determines the purposes and means” of the processing and does not extend to the overall chain of data processing for which it does not determine the purposes and means. Nevertheless, under the GDPR, the joint controller would likely be liable in full to the person whose data has been unlawfully processed and will then be able to have recourse against other joint controllers.³⁸

Unless otherwise indicated, this Roadmap is based on the premise that Arbitral Participants are either data controllers (often in parallel with other controllers) or joint controllers as far as their arbitration activities are concerned. To establish whether Arbitral

34. GDPR Art. 26(1). The addition of the joint controller concept to the GDPR followed relevant case law in the EU under its predecessor legislative instrument, the Data Protection Directive, which provided that controllers would be considered “joint controllers” under certain circumstances.

35. GDPR Art. 82(5).

36. The Brazil Act provides that “controllers who are directly involved in the treatment of which damage has occurred to the data subject are jointly and severally liable ...” (Brazil Act Art. 42, Paragraph 1, II).

37. A “data protection protocol” refers to a document addressing data protection whereby the roles and responsibilities of data controllers and processors vis-à-vis the processing of personal data are identified and agreed. This is required by the GDPR for joint controllers.

38. See Judgment of 29 July 2019, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629, paras 74, 85. See also Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* C210/16, EU:C:2018:388; Judgment of 10 July 2018, *Tietosuojaalututustu*, C25/17, EU:C:2018:551; GDPR Art. 82(5).

Participants are either (1) controllers (who are likely to be acting alongside other controllers with parallel responsibilities); or (2) joint controllers, involves a factual assessment, which turns on the question as to whether they can properly be considered to *jointly* determine the “purposes and means” of the processing of personal data.

3. Data Processors

Data controllers (including joint controllers) can delegate the processing of data under their control to a data processor, which is defined as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” (e.g., GDPR Art. 4(8)).³⁹ Under EU-style data protection laws, data controllers may only delegate processing activities to data processors if they enter into data processing agreements on terms prescribed by the applicable law.

To qualify as a data processor, the party must meet the following criteria:

- Act under the instruction of a data controller in undertaking their tasks;
- Not be responsible for deciding the purposes and means of the data processing; and
- Be retained under a (GDPR-compliant) data processing agreement allowing the data controller to direct the processing and stop it at any time.

In the context of arbitration, Arbitral Participants will generally not qualify as data processors because, by virtue of their function, they control the purposes and means of the data processing.

However, an Arbitral Participant may wish to engage a third party to process data, in which case they should ensure that the controller retains control over the purposes and means of the data processing and that a compliant data processing agreement is put in place.⁴⁰

Tribunal secretaries, e-discovery professionals, transcribers, interpreters, online case management platform providers, remote hearing platform providers and other service providers (not being employees of the Arbitral Participants) may be considered data processors, depending on who directs the purposes and the means of the processing, requiring that a GDPR-compliant data processing agreement is entered into with such persons or entities.

39. A similar definition of data processor is found on Art. 5(VII) of the Brazil Act: “natural person or legal entity, of public or private law, that processes personal data in the name of the controller”.

40. See GDPR Art. 28 (3) for the requirements for a GDPR-compliant data processing agreement.

Example: To prepare a claim, a party collects documents containing personal data that it provides to its outside legal counsel.

The collecting and collating of documents relevant to potential claims may be carried out by database service providers, whose job it is to collect data on the instruction of the party or counsel. They would thus be considered to be data processors without the responsibility for deciding the means and purposes for data processing, subject to the rules established in the applicable data protection laws for data processors.

Counsel distils from those documents the relevant information, which includes personal data, and records that information in submissions and evidence, which is then provided to the administering institution and the tribunal. In order to perform their duties, legal counsel, the institution and arbitrators are likely to determine the “purposes and means” of the data processing and will therefore be considered to be data controllers (or joint controllers if they jointly control the purpose and means of the processing) and thus subject to the rules established in the applicable data protection laws for data controllers or joint controllers.

These potentially overlapping individual compliance responsibilities create competing obligations that need to be reconciled. This is further complicated by the fact that Arbitral Participants may not be subject to the same data protection laws and others may not be subject to any data protection law at all. The orderly conduct of the proceedings will therefore be facilitated by the issuance of Data Protection Directions in the first procedural order, the terms of reference or in a data protection protocol (see [Section II.B.3.c](#) and [Annexes 7 and 8](#)).⁴¹

D. LAWFUL BASIS FOR PROCESSING

Where an EU-style data protection law applies to an Arbitral Participant, the most fundamental question one must address is what is the “lawful basis” for the data processing.

41. “Data Protection Directions” are procedural directions issued by an arbitral tribunal in the form of a procedural order, terms of reference, or a data protection protocol setting out how data protection will be addressed during the arbitration. They may be issued on an agreed basis or ordered by the arbitral tribunal.

Arbitral Participants exchange significant amounts of information, often across borders. This information contains personal data (sometimes including sensitive⁴² and criminal data). Those exchanges are essential for the proper administration of justice by means of international arbitration and the enforcement of the parties' rights in the arbitral process. However, these exchanges of information must also be lawful under the applicable data protection laws.

Under most EU-style data protection laws, a specific legal ground for the data processing must exist in order for the processing to be lawful (the so-called "lawful basis" for processing).⁴³ Depending on the purpose of the data processing and the controller's relationship to the data subject, the controller has a number of available lawful bases upon which to process data.

In most jurisdictions, including in the EU, there is no universal legal basis for lawful processing of data in the specific context of arbitration. Rather, the decision as to which legal basis to rely on for the processing of personal data in an arbitration is fact-driven and case-specific. Depending on the circumstances of the case, the potential lawful bases may be different for different Arbitral Participants and for different types of personal data (*e.g.*, witness data, data contained in the documentary evidence, sensitive or "special category" data, criminal data). Moreover, it is also required that the personal data is not processed in a manner that is unlawful generally (for example not in breach of confidentiality obligations).

As set forth below in [Section II](#), the proper functioning of an arbitration where an EU-style data protection law applies to an Arbitral Participant requires establishing the lawful basis of the data processing at the outset of the proceedings.

42. The GDPR refers to "special categories of personal data", which is also commonly referred to as "sensitive data", and is defined in the GDPR as data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. A similar list of sensitive data is found in Art. 5(II) of the Brazil Act. Under the GDPR, processing of special category data is allowed, among other reasons, where necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (GDPR Art. 9(1) and 9(2)(f)).

43. The California Act does not have a list of positive legal grounds required for collecting, selling, or disclosing personal information. Rather, it only provides that businesses must obtain the consent of consumers when they enter into a scheme that gives financial incentives on the basis of the personal information provided. *See* California Act Section 1798.120.

Example: The parties present documents – such as submissions – and evidence including work-related emails, witness statements, contracts and other materials identifying individuals. All the information identifying or allowing individuals to be identified constitutes personal data and requires a lawful basis for processing. In the context of an arbitration under the GDPR, the lawful basis is likely to be based on legitimate interests (*see* [Section II.B.3.c\(1\)](#)).

E. DATA TRANSFER RULES

In addition to a lawful basis for data processing, EU-style data protection laws require a *lawful basis for third-country data transfers*.

This is one of the most obvious ways that data protection laws apply to international arbitrations. Given the transnational nature of international arbitration, it is common for an arbitration to involve Arbitral Participants from different jurisdictions, who are subject to different data protection regimes. Each personal data transfer to each different region or country typically must have a lawful basis.

EU-style data protection laws restrict the transfer of data to third countries to ensure that individuals receive a universal level of rights under the laws and that a party does not circumvent its legal obligations by transferring data to a jurisdiction where the standards of protection of personal data are lower. The same restrictions may also apply to data transfers to international organisations, as is the case in the EU.⁴⁴ Some countries, including China and Russia in some instances, may apply a more stringent transfer regime, essentially prohibiting most data transfers out of the jurisdiction in certain circumstances.

By way of example, below are four scenarios in which third-country data transfers are allowed under the GDPR:

1. First, third-country transfers are allowed if the country has been deemed by the EU Commission to provide an adequate level of data protection (*i.e.*, the country is the subject of an “adequacy decision”);⁴⁵

44. GDPR Art. 44.

45. An “adequacy decision” refers to a decision by the European Commission that a third country’s data protection laws are considered to be adequate. An adequacy decision allows data to be transferred outside the EU/EEA or to an international organisation without any further authorisation or notice because adequate protections apply as a matter of law (GDPR

2. Second, if data is to be transferred to a country without an adequacy decision, one of the expressly listed “appropriate safeguards” should be put in place where feasible, which in the case of arbitration most likely would be the “standard contractual clauses” (see [Annex 6](#));⁴⁶
3. Third, where there is no adequacy decision and appropriate safeguards are not feasible either, a specific derogation can be relied on, which in the case of arbitration will often be the legal claims derogation, allowing transfers where “necessary for the establishment, exercise or defence of legal claims”, and provided that the other conditions for the application of that derogation are met including that the transfer is occasional, necessary for the arbitration, and that the personal data has been minimised;⁴⁷ and
4. Lastly, if none of the express derogations is applicable, a party may rely on its “compelling legitimate interests” as a basis for the transfer of data. However, this is a high threshold to meet, and also requires notification to both the data subjects and the supervisory authority, which means that it is unlikely to be often applied in practice in international arbitration.⁴⁸

As set forth below in [Section II](#), where an EU-style data protection law applies, the basis relied upon for third-country data transfers should be established at the outset of the proceeding to avoid issues at a later stage.

Example: In an arbitration between a Brazilian company and a French company under the rules of an EU arbitral institution, arbitrators are appointed from the EU, Brazil and the USA. The EU arbitral institution and EU-residing arbitrator will have to comply with the GDPR’s data transfer restrictions for data transfer to the Brazilian and USA based arbitrators. Since neither Brazil nor the USA is deemed to provide adequate protection, standard contractual clauses or another adequate safeguard should be put in place where feasible. If that is not feasible, the legal claims derogation can be relied upon, in which case certain requirements must be met, including that the transfer is occasional, necessary for the arbitration, and that the personal data has been minimised. The Brazilian arbitrator will also have to comply with the data transfer

Art. 45(1)). The most recent adequacy decision prior to the publication of the Roadmap covered the UK after Brexit.

46. As described in [Annex 6](#), the standard contractual clauses include the most important obligations under the GDPR, in which case data can be transferred outside the EU without any further protections because adequate protections apply as a matter of contract..
47. GDPR Art. 49(1)(e).
48. GDPR Art. 49(2); EDPB, “Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679”, 6 February 2018 (“Data Transfer Guidance”).

restrictions in the Brazil Act whenever personal data covered by that Act is transferred to the other Arbitral Participants, and the US arbitrator will need to consider what data protection laws apply to them and what can be done to facilitate personal data transfer during the arbitration, including entering into standard contractual clauses if requested to do so.

F. DATA PROTECTION PRINCIPLES APPLICABLE IN ARBITRATION

As a survey of all data protection laws in force globally is not feasible, the Roadmap focuses on nine principles of data protection law that are common to EU-style data protection laws adopted around the world:⁴⁹

1. **Fair and Lawful Processing.** Personal data must be processed in a manner that is fair and lawful, which means that data can only be processed if there is a lawful basis for it (as discussed in [Section I.D](#)).
2. **Proportionality.** Data protection laws should be applied in a proportionate manner, taking into consideration the rights and interests of the data subject, as well as the rights and interests of third parties, for example, including parties to the arbitration and the need for fair and efficient administration of justice, keeping in mind that in all cases adequate protection must be afforded to the data subject and their personal data.
3. **Data Minimisation.** The amount of personal data must be limited to what is necessary for the purpose of the data processing.
4. **Purpose Limitation.** Personal data may only be collected for a specific and legitimate purpose and may not be processed in a manner that is not compatible with that purpose.
5. **Data Subject Rights.** Individuals whose personal data is collected and processed have the right to access their personal data and other important rights with respect to the processing of their data.

49. These principles overlap to some extent, and the list could be expanded, but they are common to most data protection laws around the world. In the EU, these principles are consolidated in Articles 5 and 12–22 of the GDPR, and in Brazil in Article 6 of the Brazil Act. *See, e.g.*, Daniel Cooper and Christopher Kuner, “Data Protection Law and International Dispute Resolution”, 382 *Recueil des cours/Collected Courses of the Hague Academy of International Law* 9-174 (2017), at 43 (describing similar principles as they applied under the Data Protection Directive).

6. **Accuracy.** Personal data that is collected and processed must be valid, relevant, complete for the purposes for which it is used and must be kept up to date.

7. **Data Security.** Data controllers must take appropriate technical and organisational security measures to protect personal data against the potential risks involved in processing, including procedures in the case of data breach.

8. **Transparency.** Data subjects have a right to information regarding the processing of their personal data, which includes the right to be notified that such processing is taking place and their rights under the relevant law.

9. **Accountability.** Data controllers are required to keep a record of their data protection compliance efforts in order to demonstrate compliance.

The remainder of this Section considers each of these nine principles in turn.

1. Fair and Lawful Processing

Personal data must be processed fairly and lawfully in relation to the data subject.

As discussed in the preceding Section, lawfulness entails that personal data may only be processed if there is a legal basis for it.

With respect to fairness, the notion of fairness in data protection law aims to ensure that personal data is processed typically only in ways that data subjects would reasonably expect. The data subject's expectations are framed by considerations such as: (1) how the personal data was obtained; (2) whether they have been notified; (3) if notice was given, what purpose for the processing was notified to them; and (4) whether they could have expected that their personal data would be used in the manner in which it is being used. The notion of fairness also entails that personal data cannot be used in a manner that has an unjustified adverse effect on the data subject (note that the processing can have adverse effects, provided they are justified).

In the arbitration context, fairness triggers the question as to whether the data subject, whose data is processed during the arbitration, could have anticipated the processing thereof in view of how it was collected and the notices given to the data subject. It will also take into account whether processing will have adverse effects on the data subject that are not justified by the needs of the processing for the arbitration. This may depend on the role the data subject played in the underlying dispute as well as in the arbitration.

Example: Email correspondence is submitted in an arbitration, identifying individuals who are employees of the parties. The emails also identify other data subjects who are not employed by either party. Applying the fairness principle, the party and its counsel that are processing the document for the arbitration should query: (1) whether, considering all the facts, the individuals would have expected this processing; (2) whether it will have adverse consequences for them; and (3) if so, whether the consequences are justified. While the outcome will depend on the nature of the personal data in question and the purposes of the use in the arbitration, the fairness doctrine will typically not prevent personal data most commonly found in business email correspondence from being adduced as evidence (although culling and redaction/pseudonymisation may be required in certain circumstances).

2. Proportionality

As a general matter, data protection laws are intended to be of a mandatory nature. Yet, the fundamental right to the protection of personal data is not an absolute right. Under the GDPR, this requires consideration of the nature, scope, context and purpose of processing and the risks posed to the data subject, taking into consideration the nature and extent of the personal data being processed (e.g., GDPR, Recital 4, Art. 24).⁵⁰ This “proportionality principle” is found throughout many modern data protection laws.

Proportionality cannot lead to the inapplicability of data protection laws, but rather may impact how data protection laws should be given effect based on the context of the data processing, the risk posed to the individual whose data is being processed, and the nature and extent of the personal data being processed.

In the context of an arbitration, this means that, where the law so provides, consideration should be given to the rights and interests of the data subject, the rights and interests of parties to the arbitration, those of third parties, and the need for a fair and efficient administration of justice.

Depending on the context, relevant considerations could be, among others: (1) the type of personal data being presented in the arbitration; (2) what risks the processing for the

50. See, for the EU, European Data Protection Supervisor, “EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data”, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (Dec. 19, 2019); see also Handbook on European Data Protection Law, European Union Agency for Fundamental Rights (2018).

arbitration poses to the data subject as an individual; (3) what purpose for the processing was notified to them; (4) whether they are involved in the arbitration; (5) how the personal data was collected; and (6) what were/are their expectations about the processing of that data based on the notices they have been provided. Consideration should also be given to the parties' rights and interests at stake in the arbitration, as well as those of third parties that may be impacted.

In practice, for example, proportionality would generally entail that sensitive data (such as medical records) is subject to a higher level of protection than business related personal data (such as business email communications) because the data subject could reasonably expect data contained in professional email correspondence may be processed for a legal claim, while such expectation may be much less obvious for the data subject's medical records depending on the case. Moreover, the risk posed to the data subject may be greater from the processing of their medical records compared with standard business correspondence.

However, although the means by which the data protection rules are applied may vary based on the rights at stake and the risks to the data subject, this does not mean that those rules do not apply, but rather that the manner in which they are applied may vary – for example the extent of the security requirements to be applied or how much data minimisation is required. In all cases, however, adequate protection must be afforded to the data subject and their personal data.

3. Data Minimisation

The concept of data minimisation is fundamental to EU-style data protection regimes. For example, Article 5(1)(c) of the GDPR states that “personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).”⁵¹

In the context of arbitration, data minimisation is required in all stages of the arbitral process. Data minimisation requires Arbitral Participants to ensure that the amount and type of personal data processed is adequate, relevant and limited to what is necessary for the lawful purpose of the processing (*i.e.*, preparing a case for arbitration, prosecuting, defending against, or deciding a claim, administering the proceedings, or retaining data in relation to the arbitration after completion of the proceedings).

51. According to Article 18(IV) of the Brazil Act, for example, data subjects have the right to obtain the anonymisation, blocking or deletion of unnecessary or excessive data or data processed in a manner that is not compliant with the law.

Data minimisation obligations are particularly relevant in the selection, production and disclosure of documents. It remains to be seen whether in practice timely and more extensive culling for relevance and redaction of unnecessary personal data will become more widespread as a result of EU-style data protection laws, keeping in mind that document production for arbitration is more limited than in litigation.

Example: A law firm asks its client (a potential party to an arbitration) to provide a copy of the email boxes of anyone potentially related to the transaction at issue in a potential arbitration from the time the transaction was first contemplated until the present time. The data minimisation principle requires both client and law firm to consider whether the personal data likely to be contained in the email boxes is relevant for the purpose of bringing or defending the claim and whether the request has been limited to what is necessary for the purpose of bringing or defending a claim in arbitration. If not, efforts should be made to limit: (1) the volume of data collected, for example by restricting date ranges to the most relevant time periods and custodians to those specific employees who were directly involved in the transaction in question; and (2) the amount of personal data that is included.

In the case of the GDPR, for example, if the law firm is based in the US and the party in the EU, this will also raise third-country data transfer concerns.⁵² Standard contractual clauses or another adequate protection should be put in place where feasible, and where this is not feasible, transfer may be lawful on the basis of the legal claims derogation on certain conditions. In terms of what conditions may apply when the derogation is relied on, the transfers must be occasional and, for example, the EU Working Party provided guidance in the context of data transfers to the US for purposes of discovery for US litigation, setting out that the data set should be culled for relevance,⁵³ efforts should be made to redact or pseudonymise personal data⁵⁴ and confidentiality provisions put in place where possible *before* the transfer is made.

52. Under the GDPR, a “third country” means any country outside of the European Union and the EEA, including, for example, the US and the UK after Brexit.

53. “Culling” means filtering data.

54. “Pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. *See* GDPR Art. 4(5); Brazil Act Art. 13 Paragraph 4; California Act Sections 1798.100(e), 1798.140(r), 1798.145(i).

4. Purpose Limitation

The principle of purpose limitation is related to the transparency requirement, in that the data subject should receive a notice, identifying the purpose of the processing of their personal data. The subsequent processing activities should then be limited to the purpose that was notified to the data subject.⁵⁵

Typically, a large portion of personal data contained in documents exchanged during an arbitration will be personal data of the parties' employees/staff, clients or business counterparties, gathered in the context of the ordinary business or other activities that led to the dispute. The evidence processed by a party will normally not have been created for the purpose of bringing a claim, but is collected and processed for use in an arbitration.

If personal data is processed by Arbitral Participants who did not originally collect the data, which is often the case, the possibility of processing for the purpose of the arbitration must either have been included in the original notice given to the data subject or be compatible with the purpose identified therein.

For example, under the GDPR, the factors to be considered when deciding whether further data processing is compatible with the originally notified purpose are: (1) the presence of any link between the original purpose and the new purpose; (2) the context in which the data was collected ("in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use"); (3) the nature of the personal data (for example, business correspondence and documents as opposed to patient medical information); (4) the possible consequences of the further processing; and (5) the existence of appropriate safeguards.⁵⁶

Deciding whether the purpose is compatible with the originally notified purpose involves a fact-specific analysis. Compatibility depends on the original purpose notified to the data subject. For example, the use of employee and business-related information in an arbitration, in which the specific data subject's actions are at issue, may well be compatible with the purpose for which the data was originally processed, given their role in the organisation. Depending on the employee's role, they may have known or expected that information containing their personal data could potentially be processed for legal proceedings. This may be the case where the personal data is contained in business emails and other business correspondence and documents. Making this determination depends

55. GDPR Art. 5(1)(b) states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ... ('purpose limitation')".

56. GDPR Recital 50.

on the purpose for which the data was originally collected. Although not determinative, it is helpful if the data subject was informed in advance of the possibility that their personal data could be used in a dispute resolution procedure.

In the EU, Member States can derogate from the application of the purpose limitation. In Germany, for example, controllers are permitted to process personal data for a purpose other than the one for which the data was collected where the legal claims derogation applies,⁵⁷ unless the data subject has an overriding interest in not having the data processed.⁵⁸ In Brazil, new uses – for other purposes – of personal data made manifestly public by the data subject are permitted, provided that the purposes for the re-processing are legitimate, that the data subject rights are guaranteed, as well as that the fundamental rights and principles set out in the Brazil Act are preserved.⁵⁹

Example: When the General Counsel was hired at Company X, they were informed that their personal data would be processed where necessary in the normal course of their activities as General Counsel. They have now left the company. A dispute arises with Company Y and an arbitration is commenced. Company X would like to submit evidence in the arbitration that contains the General Counsel’s personal data, including their signature on a contract, minutes of meetings they attended and emails they exchanged. The further processing of their personal data for purposes of the arbitration would be within the scope of their function at the company as notified to them. Hence, it would likely fall within the purpose limitation.

5. Data Subject Rights

EU-style data protection laws, including for example, the GDPR and the Brazil Act, grant data subjects important rights with respect to the processing of their personal data, several of which are likely to apply to Arbitral Participants. Data subject rights is an area in which there are significant differences among countries with EU-style data protection regimes.⁶⁰

57. Meaning that the processing is “necessary for the establishment, exercise or defence of legal claims”.

58. German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 Section 24.

59. Brazil Act, Art. 7, Para. 7.

60. Art. 18 of the Brazil Act lists the main data subject rights in Brazil, which are similar to those in the GDPR.

When the GDPR applies, data subjects are granted the following rights:

- The right of access and to obtain a copy of the personal data being processed (also referred to as a “data subject access request”),⁶¹ except that “[t]he right to obtain a copy ... shall not adversely affect the rights and freedoms of others”;⁶²
- The right to request modification of their data, including the correction of errors and the updating of incomplete information;⁶³
- The right to withdraw consent if consent was the basis for processing, provided that “[t]he withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal”;⁶⁴
- The right to object to data processing where the lawful basis relied upon is a legitimate interest, in which case the controller should demonstrate that a compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject;⁶⁵ and
- The right to erasure – also referred to as the right to deletion or the right to be forgotten – which allows a data subject to request, under certain circumstances, that their personal data be erased.⁶⁶

Arbitral Participants subject to the GDPR should also keep in mind that national laws may provide derogations from the GDPR, which may impact the extent of the data subject rights in arbitration proceedings.

Example: An individual who acted as a sub-contractor to the claimant makes a data subject access request to respondent’s counsel (or the tribunal) requesting access to all personal data about them that has been processed in the context of the arbitration proceeding. Under the GDPR, for example, respondent’s counsel (or the tribunal) must address the request without undue delay and in any event within one month, unless extended. The responding party should bear in mind, however, that the right to electronic access or to obtain a copy “shall not adversely affect the rights and freedoms of others” (GDPR Art. 15(4)) and that it must consider its own legal and ethical obligations before providing the requested information. This may affect whether documents

61. GDPR Art. 15; California Act Sections 1798.100(d), 1798.110, 1798.115.

62. GDPR Art. 15(4).

63. GDPR Art. 16; in contrast to the GDPR, no right of rectification exists under the California Act.

64. GDPR Art. 7(3).

65. GDPR Art. 21; California Act Section 1798.120.

66. GDPR Arts. 12, 17; California Act Sections 1798.105, 1798.130(a), 1798.145 (g)(3).

or document extracts are provided to the sub-contractor, and if so which ones. The responding party should also consider whether an exception applies under national law (for example, in Germany with respect to privileged information). Considering these issues before they materialise through Data Protection Directions will help minimise any impact on the process (see [Section II.B.3.c](#) and [Annex 7](#)).

6. Data Accuracy

Data controllers are expected to take all reasonable steps to ensure the personal data they process is not incorrect or misleading as to any matter of fact.⁶⁷ There is also a general obligation to keep the personal data up to date, although this will depend on the purpose of the processing (for example, in an arbitration, it should not be required to update personal data in the record about facts which occurred in the past, unless it becomes clear that the facts in the record are wrong or misleading). If it comes to light that personal data is incorrect or misleading, reasonable steps should be taken to promptly correct or erase it.

Example: Evidence is submitted in an arbitration including evidence involving an employee of the respondent, for which the claimant submits emails and photographs as evidence. The employee claims that the evidence has been falsified and brings a data subject request to the claimant, claimant’s counsel, the institution and the tribunal asking that their personal data be corrected. This question is complex, and addressing these issues will be highly case specific, but advance planning, for example, through the adoption of Data Protection Directions may limit any negative impact the rights request will have on the arbitration (see [Section II.B.3.c](#) and [Annex 7](#)).

7. Data Security and Data Breach

EU-style data protection laws require all users of personal data, including both data processors and data controllers, to apply reasonable data security to personal data, referred to in this Roadmap as information security measures and in the GDPR as “appropriate

67. See, e.g., GDPR Art. 5(1)(d): “personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)”.

technical and organisational measures”.⁶⁸ Deciding what security measures are “appropriate” requires consideration of the potential risk to data subjects, the existing information security measures of the Arbitral Participants, and what physical and technical measures are appropriate given the risks to the data subjects. Moreover, as part of entering into standard contractual clauses, the parties to those clauses are required to provide a description of the data security provisions that will be in place after the transfer (see [Annex 6](#)).

As discussed further in [Section II](#), Article 32 of the GDPR imposes the primary obligation on controllers and processors to ensure that data is processed securely, which will need to be applied during an arbitration where the GDPR applies. When deciding what information security measures are appropriate, consideration must be given to the “state of the art”, implementation costs, data minimisation, and the circumstances and the risk level of the processing, with a focus on the risks to the data subject.

When a data breach occurs, this raises important questions about what notification requirements apply to the Arbitral Participants. Given the risks associated with data breaches, as discussed in [Section II](#), these questions should be addressed at the outset of the arbitral proceedings, and agreeing to a data breach protocol as part of the Data Protection Directions is usually advisable.

Example: An arbitrator involved in a case in which significant personal data has been exchanged in the record uses a personal email account with an insecure email password and no encryption. They travel frequently, fail to use a screen protector and regularly connect from public Wi-Fi and have documents printed at their hotel. It is unlikely that the degree of information security applied by the arbitrator is appropriate to protect the personal data exchanged in the arbitration and it would likely violate applicable data protection standards.

The arbitrator becomes aware that their system has been compromised and that access to all their files in 20 ongoing cases have been exposed. The arbitrator will need to comply with their obligations under any data breach protocols in place in those cases. In cases where data breach protocols are not in place, the arbitrator will usually want to promptly notify the other Arbitral Participants so they can comply with their data protection and other obligations.

After becoming aware of the data breach, each Arbitral Participant will then need to decide what notification obligations apply to them. Whether the Arbitral Participant

68. See GDPR Art. 32.

has a duty to notify the supervisory authority or the data subject and the extent of this duty is fact specific.

Under the GDPR, they will need to consider whether this breach is likely to result in a risk to the rights and freedoms of those data subjects whose data has been exposed, in which case they must notify the breach to the relevant supervisory authority or authorities without undue delay and, where feasible, do so not later than 72 hours after becoming aware of the breach. If the risk is high, notification is also required to the data subjects impacted (see [Section II.B.3.c\(4\)](#)).

8. Transparency

Transparency requires data subjects to be provided with notice in plain language about the processing of their personal data and the purpose for the processing. This can be done through general notices, specific notices or a combination of the two, as long as the data subject has actual notice of the processing or potential processing of personal data.

Arbitral Participants should determine what transparency requirements apply to them: (1) generally, including the publication of adequate data privacy notices; (2) when preparing a file for arbitration; (3) when initiating arbitral proceedings; and (4) during the arbitral proceedings when new personal data is introduced or processed for a different purpose. Arbitral Participants should consider issuing (or updating pre-existing) privacy notices to meet those requirements.

Privacy Notices. Even before a specific arbitration is contemplated, Arbitral Participants should consider issuing privacy notices, explaining to actual and potential data subjects why and how they process their personal data and what rights data subjects have. Privacy notices will often be posted on the Arbitral Participant's website and should address dispute resolution specifically. These notices will be aimed at third parties whose personal data is being processed. Adopting a privacy notice and posting it on the Arbitral Participant's website will often be part of complying with the obligations imposed by, for example, GDPR Articles 13 and 14.⁶⁹

69. [Annex 9](#) provides the structure of sample privacy notices for consideration by institutions, arbitrators and legal counsel governed by the GDPR and other countries with similar notification requirements. This Annex may be a starting point for Arbitral Participants when deciding what to put in their privacy notices, but privacy notices are fact-specific and require careful consideration and tailoring to each Arbitral Participant's particular situation, activities and needs.

Notifications. In addition to general privacy notices, Arbitral Participants who are data controllers or joint controllers are responsible for ensuring that data subjects in a specific arbitration have been provided with sufficient notification of the data processing. It is important to note that exceptions to the notification requirements may apply where a data subject has already been notified of the processing by someone else (in this case, likely another Arbitral Participant).

Example: Evidence is collected for an arbitration from 25 employees identifying at least 100 individuals. Subject to consideration of other potential restrictions under applicable labour law, the transparency doctrine requires that (i) each individual identified (or identifiable) in those emails has been sufficiently notified of the processing of their personal data for the arbitration (for example when their email boxes are screened for relevant information) unless an exception applies and (ii) the processing of personal data is compatible with the purpose identified in the notice provided to them at the time of collection. However, the emails will likely also identify persons from the opposing party and individuals with no ongoing relationship to either party. Notifying those persons may be problematic. The question is whether the data subjects have been given adequate notice of the data processing, either at the time of original processing of the data in the ordinary course of business, or in the context of collection for the arbitration. If not, it needs to be considered whether there is an exemption from notice requirements in the circumstances of the particular case. In the case of confidential arbitrations, notifying third parties or even employees at the time of the dispute can compromise the confidentiality of the process or create strategic concerns. Where possible, these issues should be addressed and agreed in the Data Protection Directions (*see* [Section II.B.3.c](#) and [Annex 7](#)).

9. Accountability

Accountability requires those processing personal data to document the compliance approach they have adopted and measures they have taken towards the protection of such data. It is a central feature of the GDPR and other EU-style data protection laws.

Under the GDPR, for example, data controllers are expected to be able to “demonstrate compliance” with these principles as they are implemented throughout the GDPR.⁷⁰ Adequate records should be kept of what compliance measures were taken and why, in such a manner that they can be shown to the competent authorities if compliance issues were

70. GDPR Art. 5(2); *see also* GDPR Art. 24(1).

to arise.⁷¹ Although the obligations of Arbitral Participants may be interrelated, they each have their own independent recording obligations. Similar provisions are found in other data protection laws that are modelled on the GDPR, such as in Brazil Act (Art. 6(X)).

As there is no specific guidance from courts or data protection authorities at present in respect of the application of data protection laws in arbitration, the documentation of the Arbitral Participants' approach and measures is particularly important to demonstrate their good faith efforts towards their compliance with data protection laws.

Example: A complaint is brought before a supervisory authority that the data processing during an arbitration violated applicable data protection laws. The supervisory authority asks the arbitral institution and the arbitrators to provide records evidencing data protection compliance during the case. A failure to be able to provide records would likely be a violation of the GDPR's or Brazil Act's accountability principle. Arbitral Participants should therefore agree to how records will be kept of the steps taken to comply with applicable data protection laws in a manner that can be shown to a competent authority.

71. Organisations with more than 250 employees must document compliance in accordance with Article 30 of the GDPR, which provides a list of record-keeping obligations.

II. DATA PROTECTION COMPLIANCE IN INTERNATIONAL ARBITRATION PROCEEDINGS

Based on the overview in [Section I](#) describing the general framework for the application of data protection laws and principles to arbitration and Arbitral Participants, this Section II considers how data protection compliance may affect a specific arbitration and the implications for Arbitral Participants from the time that a party starts to prepare for the arbitration, until the case has been concluded and the documents are stored or destroyed.

This Section II is organised around the typical procedural steps of an arbitration. It should be considered together with the [Annexes](#), which contain samples of privacy notices, generic language to be considered for Data Protection Directions and Data Protection Protocols, as well as non-exhaustive checklists of issues that parties, their legal counsel, institutions and arbitrators may want to consider in establishing whether data protection laws apply to them and how they can be complied with in the context of the arbitration proceedings.

Arbitral Participants should consider from the outset what data protection laws will apply to them and the other Arbitral Participants. For the parties and their legal counsel, that moment may be prior to the initiation of the arbitration when they start to prepare the case. For the institution, applicability should be considered as of the moment a party indicates that it is or may be starting an arbitration. For the arbitrators, that moment is when they are contacted with a view to their appointment as arbitrator in a specific case. In organisations that have appointed a data protection officer, which will often be the case for example in a large law firm or company, the officer may be involved in decisions regarding the protection of personal data during the arbitration.⁷²

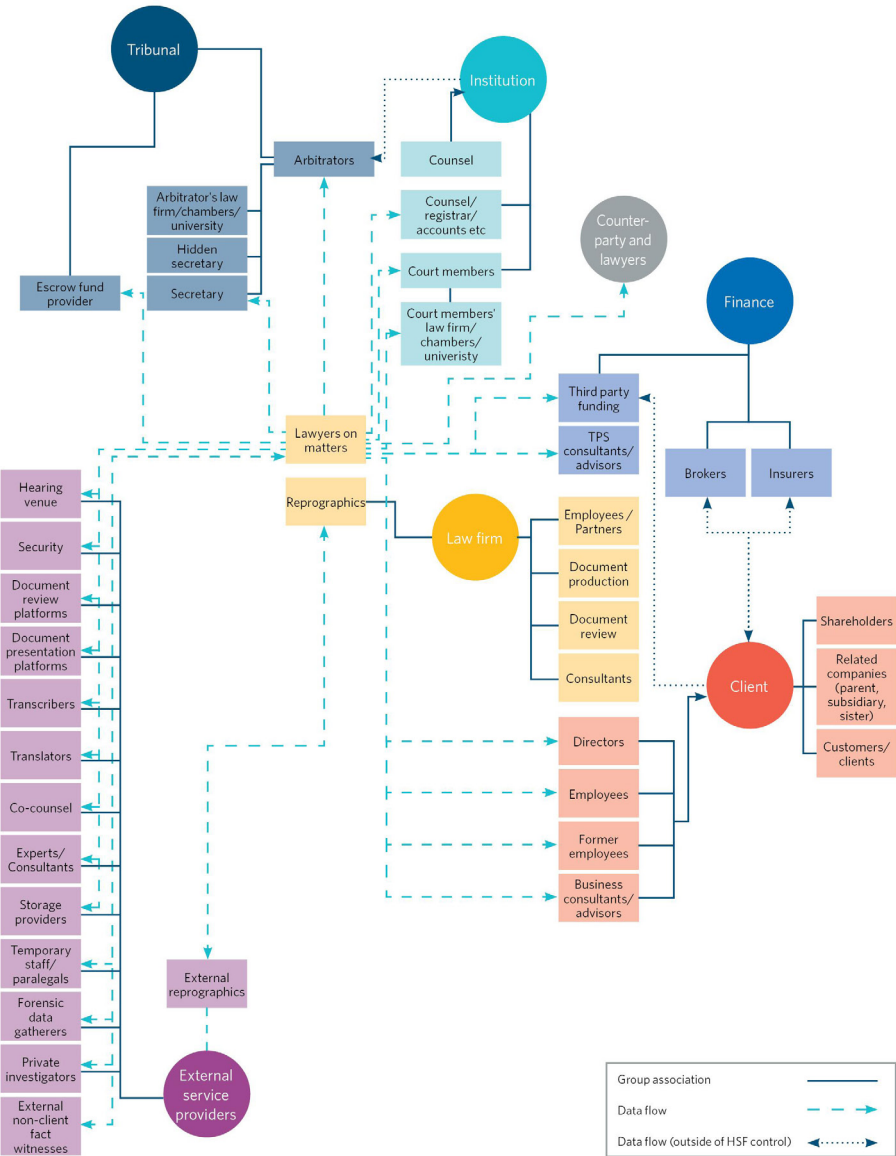
A. PREPARING FOR THE ARBITRATION

It is important to recall that data protection laws apply not only during the arbitration, but also when preparing for an arbitration. This Section reviews the data protection implications while preparing for arbitration, which will principally concern parties and their legal counsel.

72. GDPR Art. 38(1).

Figure 1.

Data flows in arbitration for one side



1. Applicable Data Protection Laws

In preparing for the arbitration, parties and their legal counsel should consider how data protection may affect the proceedings. Determining what data protection obligations may arise in relation to the arbitration requires advance examination as to whether the various Arbitral Participants fall within the scope of a relevant data protection law.⁷³

In the first place, any privacy notices issued by the Arbitral Participants will provide insight into the approach that the Arbitral Participant takes to data protection compliance, as well as their view of what data protection law may be applicable as well as their status under that law as a controller, a joint controller with other controllers or a processor.

In the second place, it is important to consider how data flows are likely to occur in the case and what the legal basis would be for any necessary data transfers that would be subject to data protection limitations. So-called “data mapping” in the arbitration context involves determining where the data processed during the arbitration is located and where it would need to be transferred and processed for the purposes of the arbitration. This mapping exercise allows parties and their legal counsel to adopt an approach to data protection compliance with a minimum impact on the arbitration.

Data Flows. *Figure 1* depicts typical data flows in an international arbitration and reveals how extensive and interconnected they are.⁷⁴

For example, where an Arbitral Participant in the EU transfers data to another country or jurisdiction, they will want to consider the lawful basis for the transfer, including whether the country has been found by the EU to provide adequate protection (*see Section II.B.3.c(2)*). If this is not the case, the Arbitral Participant should consider whether it is feasible to enter into standard contractual clauses to permit the transfer. Where this is not feasible, the Arbitral Participant may be able to rely on the legal claims derogation for the transfer, in which case it will need to consider the extent to which it needs to review, minimise, cull and potentially redact personal data before transferring a more limited data set to Arbitral Participants located outside the EU.

73. In the case of arbitrations administered by an international organisation, *see* fn. 6.

74. This chart was first published by Herbert Smith Freehills LLP (HSF) in *Inside Arbitration* – Issue 8, dated 16 July 2019 and is reprinted with permission.

2. Roles of Arbitral Participants

Data protection obligations fall on the individual Arbitral Participants, rather than governing the arbitration proceedings as such. However, the interlinked nature of compliance means that when any Arbitral Participant is bound by data protection laws, this may have an impact on the other Arbitral Participants and the process. This makes it important to identify potential issues early, even if no action is required.

Parties should form a view early in their case preparation as to which of the Arbitral Participants are likely to be processing data during the arbitration and whether they will do so as controllers (generally in parallel with other controllers), processors, or potentially joint controllers. After the arbitration commences, each Arbitral Participant will need to determine their own status and ensure that they comply with their data protection obligations under the law applicable to them (*see* [Section I.C](#)).

For example, once an Arbitral Participant receives copies of a party's submissions and evidence, it likely becomes a data controller of the personal data contained therein (often in parallel with other controllers) or, depending on the circumstances, joint controllers as far as their arbitration activities are concerned. On the other hand, tribunal secretaries, e-discovery professionals, transcribers, interpreters, online case management platform providers, remote hearing platform providers and other service providers (not being employees of the Arbitral Participants) may be considered data processors, depending on who directs the purposes and the means of the data processing.

3. Use of Service Providers

Arbitral Participants often use third-party service providers to render services in relation to the preparation and conduct of an arbitration, all of whom may have access to parts of the record. Examples include:

- Arbitral Participants may engage network, cloud hosting and data platform service providers, and other independent contractors;
- Parties and their legal counsel may engage e-discovery professionals, translators, transcribers, online case management platform providers, and remote hearing platform providers;
- Parties, their legal counsel, and arbitrators may engage experts who are likely to be considered data controllers themselves;⁷⁵
- Arbitrators may engage *ad hoc* tribunal secretaries or other assistants (who are not employees of their firm); and

75. *See, e.g.*, Controller/Processor Opinion at 28.

- Institutions may assist the parties with hearing facilities where translation and transcription services are provided, as well as other services performed by third parties.

The personal data related to the arbitration will need to be processed, and may also need to be transferred, by each of these third-party service providers in order for them to provide their services. Depending on who controls the purpose and means of the processing, some of the above service providers (for example, experts) may be considered data controllers in their own right, while others are data processors acting only under the instructions of the data controller (*see Section I.C*). In all cases, it will be important that relevant data protection laws are complied with. Specifically for data processors, it will be important that they enter into an EU-compliant data processing agreement with the Arbitral Participant who is the controller.

4. Data Collection and Review

When a dispute arises, the first thing that parties and their legal counsel typically do is to review the facts by going back through the chain of events that led to the dispute. This often involves the review of emails, other communications (texts, WhatsApp messages, etc.) and other contemporaneous evidence of the relevant events. Moreover, in advance of the arbitration, the potential for disclosure during the arbitration may require the parties and others to suspend their usual data destruction policies or to make changes to their usual retention or deletion processes to cater for a “litigation/arbitration hold” in contemplation of arbitration proceedings.

The act of collecting or obtaining documents for the purpose of preparing for an arbitration, or in the context of an arbitration in a broader sense, will constitute processing of the personal data contained in the documents. This means that during the document collection and review process, parties and their legal counsel will need a lawful basis for their data processing activities, as well as a lawful basis for any third-country data transfer that may be necessary in that framework. For example, third-country data transfers during the preparation or prosecution of an arbitration between a party and their lawyer, between the offices of a law firm, between co-counsel, or between opposing counsel all require a lawful basis, in which case standard contractual clauses or other adequate protection measures can be put in place to ensure compliance.

When preparing cases, parties and their legal counsel should identify and document: (1) the relevant data subjects or categories thereof; (2) the categories of personal data, sensitive data, personal data of children and any data related to criminal proceedings that are likely to be processed, as well as whether it is primarily low risk business correspondence and documentation; (3) the likely impact of that processing on the relevant individuals;

(4) the lawful basis for processing that data for the arbitration; (5) how applicable transparency obligations have been, or can be, complied with, including whether it is feasible to provide additional notices without infringing the parties' rights or the integrity of the proceedings; and (6) the steps to minimise the processing of personal data to what is necessary for the lawful basis pursued (*e.g.*, by limiting data collection to specific custodians, data ranges or applying search terms, redaction, pseudonymisation, etc.).

Online case management platforms, which will often be administered by a third-party provider, can assist Arbitral Participants to comply with their data protection obligations. The consistent use of an online case management platform can make it easier to comply with these obligations – the relevant data flows and data security arrangements can be discussed beforehand with the platform provider (*e.g.*, using the questionnaire at [Annex 4](#), Online Case Management Platform Provider Checklist). Once the purposes and manner of processing arbitration data has been agreed, user access permissions can help to ensure that data is shared only with necessary parties and only for as long as is necessary. Furthermore, as discussed below in [Section II.B.3.c\(8\)](#), online case management platforms can also assist with discrete data protection obligations during the course of the proceedings.⁷⁶

B. DURING THE ARBITRATION

This Section considers on a step-by-step basis how data protection obligations may affect Arbitral Participants and the conduct of the arbitration after an arbitration is initiated.

1. Filing the Request for Arbitration

The first step in an arbitration is filing the request for arbitration or the equivalent thereof, which will include personal data. The filing of the request for arbitration thus falls squarely within the realm of data processing.

Ad hoc Arbitration. In the case of an *ad hoc* arbitration, the request for arbitration is typically filed directly with the opposing party at which point the relevant data protection obligations come into effect. In *ad hoc* proceedings, at least after the appointment of the tribunal, communication is directly with the arbitrator(s), which will also involve the processing and transfer of personal data.

76. For further information on the drivers for using online case management software in arbitration, reference can be made to the “Protocol for Online Case Management in International Arbitration” Working Group on LegalTech Adoption in International Arbitration (2020) (“**Online Platform Protocol**”).

Institutional Commercial Arbitration.⁷⁷ In the case of institutional commercial arbitration, the request for arbitration will typically be filed with an arbitral institution. The filing of the request for arbitration will amount to the processing and transfer of the personal data contained in the request. This means that from the time that the arbitral institution receives the request, it becomes bound by the relevant data protection laws applicable to it.

In an institutional arbitration or in arbitrations where recourse to an appointing authority is anticipated, parties should consider whether it may be helpful to raise the potential impact of data protection laws on the arbitration with the institution in advance of the filing. This is especially necessary in cases where the filing of the request raises data protection concerns, data security is in doubt, or where the transfer of the file to the opposing party could raise a data protection concern.

The first step for arbitral institutions is to consider and determine as a general matter what data protection law(s) apply to them, if any. If the institution is subject to the GDPR or a similar data protection regime, and is not exempted, it will typically become a controller of the data set included in the claimant's request for arbitration and the subsequent filings, at least for certain purposes. From that point onwards, when processing personal data, the arbitral institution must comply with the applicable data protection law, as described in [Section I](#).

In this regard, institutions need to consider their potential data protection obligations at the time of the receipt of a request for arbitration; the registration and/or administration of arbitrations; the appointment of arbitrators; the receipt of advances and fundholding for arbitration and administration costs; the disclosure of data to parties, their legal counsel and arbitrators; the processing of data during the arbitral process; any challenge decisions of the institution; the scrutiny, approval, issuance or publication of awards or excerpts thereof; and data retention or deletion policies (including retention for archiving purposes).

In practice, where the GDPR applies, for example, the institution will need to have a lawful basis for the processing of personal data and any transfer outside the EU, appropriate data security measures, a system for the exercise of data subject rights and to maintain adequate records, as well as data breach and data retention policies. These obligations may affect the manner in which institutions are able to publish awards and decisions and to archive personal data.

77. In the case of arbitrations administered by an international organisation, *see* fn. 6.

If the institution is covered by the GDPR, for example, all these aspects of processing should be included in its privacy notice, which must comply with GDPR Articles 13 and 14. It is good practice to post and update the arbitral institution's privacy notice on its website. Data protection may also be addressed in the arbitration rules and specific explanatory notes that institutions publish from time to time for reference by parties, counsel and arbitrators.

[Annex 9A](#) contains an example of a notice that arbitral institutions subject to GDPR or a similar law (that are not an international organisation) may consider, and many of the issues addressed therein will also be relevant to non-EU based institutions.

***Example:** An arbitral institution in the EU sends the name and contact details of an arbitrator to a potential claimant in Egypt. Egypt is not the subject of an EU adequacy decision and the institution does not have any standard contractual clauses (or any of the other permitted appropriate safeguards) in place with the potential claimant. Because the transfer contains personal data, the transfer would need to be justified under one of the permitted derogations, for example, because the transfer of personal data is “necessary for the establishment, exercise or defence of legal claims”.*

2. Appointment of Arbitrators

When selecting arbitrators for cases in which the GDPR or other relevant data protection law(s) may apply, best practice is for those making the appointment to consider how it will implicate the application of the relevant data protection laws. Where the potential arbitrator is not subject to the same data protection obligations as the other Arbitral Participants, it would be prudent to consider how this will be managed during the arbitration and whether steps should be taken as part of the appointment to ensure that data can freely be transferred during the proceedings (for example through standard contractual clauses).

Potential arbitrators will also have to process the personal data of parties, legal counsel, and other arbitrators. They will do so when, for example, carrying out conflict checks and making any disclosures relevant to their impartiality and independence as may be required by applicable procedural rules and their legal professional obligations. If appointed, data processing will be carried out on an ongoing basis during the arbitration.

Before an arbitral appointment is made, personal data is often exchanged about potential arbitrators by arbitral institutions, international organisations, parties and their legal

counsel. Most of this data is obtained from the public domain, and some may be based on word of mouth or other sources.

The general privacy notices of Arbitral Participants (like institutions) who possess, use, disclose and transfer the personal data of potential arbitrators should put potential arbitrators on notice that their personal data may be processed and transferred during the selection and appointment process and indicate the legal basis for such processing. Institutions may consider including specific notices as part of any procedure for potential arbitrators to be considered for appointment, for example when lists are employed.

In addition to any standard notice, once an arbitrator is otherwise made aware they are being considered for appointment, it is best practice to put them on express notice that their personal data is being processed for this purpose, especially in cases of third-country data transfers. Note that this is a mere notice, not consent. Asking arbitrators to consent to data processing and transfer triggers risks associated with relying on consent that will be further discussed below (*see* [Section II.B.3.c\(1\)](#)). If it is decided that an appointment will be made, as mentioned above, consideration should be given to whether the use of standard contractual clauses should be raised.

3. Documenting Data Protection Compliance

a. First Procedural/Case Management Conference (referred to collectively as “CMC”)

Once the arbitration is underway, Arbitral Participants should promptly consider and attempt to agree how data protection compliance during the proceedings will be addressed. The earlier the existence of, and the allocation of, responsibilities for compliance with data protection obligations is settled or decided, the lower the data protection risks and the impact on the proceedings.

In order to ensure the orderly conduct of the arbitration and compliance with applicable data protection laws, the tribunal and the parties will need to address some, if not all, of the issues addressed in [Section I](#) at the CMC. This is required or recommended by the rules of most major international organisations (including for example, the LCIA and the ICDR) and the most recent version of the IBA Rules on the Taking of Evidence, which was adopted in 2020 (“**IBA Rules**”). The IBA Rules provide that the parties should consult on evidentiary issues, including the “treatment of any issues of cybersecurity and data protection” early in the process. The Commentary on the IBA Rules expressly suggests that parties and tribunals may want to consult this Roadmap and the ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitration (2022 Edition) (“**Cybersecurity Protocol**”) when considering these issues.

In cases where data protection laws may apply to one or more Arbitral Participants, which is often the case, data protection compliance should be put on the agenda of the CMC. As a practical matter, arbitrators that are not themselves bound by any data protection regime (for example those based in the parts of the United States where no such general regime is in place) may be inclined to avoid a discussion of data protection at the CMC if it is not raised by the parties. This is inadvisable as a matter of sound case management because, for example, a party could decide as a strategic matter not to raise data protection concerns during the first procedural conference but may later raise data protection issues in the context of the production of documents or other obligations during the arbitration, at which point it may be more difficult to manage such issues.

b. Data Protection Protocol/Procedural Order 1/Terms of Reference Directions

In the interest of compliance with data protection laws, as well as time and cost efficiency of the arbitration, data protection issues are best addressed and managed from the outset at the first CMC and then set forth either in a procedural order, terms of reference, or in a data protection protocol (referred to collectively as “**Data Protection Directions**”).

The term “**Data Protection Protocol**” refers to a document agreeing on how data protection is to be applied in a particular context, if possible, signed by all Arbitral Participants, and potentially included by reference in the first procedural order or terms of reference (see [Annex 8](#) for sample language that may be considered). To the extent permissible under the applicable law(s), the Arbitral Participants may wish to allocate roles and responsibilities in relation to data protection compliance, recorded in a data protection protocol. These types of agreements are widely used to ensure compliance among controllers with parallel and interlinked obligations, as is the case in arbitration. A data protection protocol is required by the GDPR where some or all of the Arbitral Participants are joint controllers.

Where a data protection protocol is not employed, another possibility is to set data protection compliance standards in a procedural order or terms of reference. Although this is highly case and fact specific, [Annex 7](#) provides sample language that may be considered for inclusion in a procedural order or terms of reference using the GDPR as an example (and this language may also form part of a data protection protocol). A procedural order may also be used by the arbitral tribunal to issue Data Protection Directions, all with the underlying goal of enabling the data protection rules to be applied in an orderly manner and preventing parties from using them to delay or disrupt the proceedings.

The question as to whether data protection should be addressed in a procedural order, terms of reference, or in a data protection protocol is case specific. Many cases do not have terms of reference. Furthermore, a signed data protection protocol may be unachievable

in practice and may not be justified in smaller cases or where data protection is unlikely to be a major issue. On the other hand, in other cases, even small ones, a data protection protocol may be required (for example by joint controllers in the EU).

Regardless of the size of the case or the type of Data Protection Directions employed, such directions assist in resolving issues that may subsequently arise about how data protection compliance may impact the proceedings.

[Annex 7](#) includes sample language for Data Protection Directions when the GDPR applies and [Annex 8](#) contains a sample data protection protocol, and [Annex 3](#) contains a checklist of items to be considered for data protection compliance during an arbitration.

c. Issues for Data Protection Directions

This Section will briefly consider the most important data protection issues to be considered at the CMC and recorded in Data Protection Directions from the perspective of compliance and ensuring orderly proceedings, including: (1) lawful basis for processing; (2) lawful basis for data transfer; (3) disclosure or production of documents; (4) data security and data breach protocols; (5) managing data subject rights; (6) notification; (7) documenting data protection compliance; and (8) any use of online case management platforms to assist with compliance. This is not an exhaustive list, and some of these issues may be more important than others in specific cases. However, these are issues which if not addressed early can create problems down the road either from a compliance or case management perspective. Although this is highly case and fact specific, [Annex 7](#) provides sample language addressing each of these issues that may be considered for inclusion in Data Protection Directions using the GDPR as an example.

(1) Lawful Basis for Personal Data Processing

Arbitral Participants should identify and document at the outset of proceedings what data will need to be processed for the arbitration and the lawful basis that will be relied upon for the processing of any personal data, sensitive data, and criminal offence data during the arbitration. Arbitral Participants should be aware that a specific identified purpose is required for the processing of personal data and the use of catch-all provisions referring to numerous alternative bases is generally not allowed.

As discussed below, the lawful basis may vary depending on the relevant data protection law that is applicable. Some data protection laws have established a specific lawful basis for data processing of personal data and/or sensitive data and/or criminal offence data for arbitration. This is the case in Brazil. It is also the case under the GDPR with respect to sensitive data and for some EU Member States with respect to criminal offence data,

where there is a lawful basis in relation to making or defending legal claims (which is likely to apply to arbitration). In other cases, where a legitimate interest is relied upon as a lawful basis for the processing of personal data, a Legitimate Interests Assessment should generally be undertaken and documented (as is recommended for personal data under the GDPR) (*see* [Annex 5](#)).

In most jurisdictions, the lawful basis for data processing can be met by obtaining the consent of a data subject. However, under the GDPR and many other EU-style data protection laws, this needs to be informed consent in the case of general personal data processing and explicit consent in the case of sensitive data. Consent can always be withdrawn.⁷⁸

Moreover, although the arbitration community frequently relies on consent for other purposes, the EU Working Party has referred to consent as a “false good solution”.⁷⁹ It is not recommended to rely upon consent as a lawful basis for the processing or transfer of personal data in an arbitration where the GDPR applies because:

- In order to be valid, consent must be specific, informed and freely given;
- Consent must be obtained from the data subjects themselves rather than the Arbitral Participant who provides the personal data, including each data subject identified or identifiable from the submissions or evidence (not only the parties and the witnesses);
- In an employment context, consent is likely to be an invalid legal basis for the processing of personal data; and
- Processing on the basis of consent may need to be stopped if consent is withdrawn or refused, and it is difficult to then rely on another lawful basis for processing.⁸⁰

Due to the inherent risk that consent is refused or withdrawn at some point, it is therefore strongly preferred to rely on other legal bases. This is not to say that consent should never be employed under the GDPR, but rather that it should only be used as a basis for

78. “Consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them (GDPR Art. 4(11)). A similar definition is found in Art. 5(XII) of the Brazil Act.

79. EU Working Party, “Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995”, WP 114, 25 November 2005, at 11.

80. In the EU, for example, the European Data Protection Board has stated that processing on another basis is not permitted if consent is withdrawn. European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679, paras. 121-123.

processing when all these considerations are acceptable under the circumstances. By contrast, in other countries like India, consent is the primary basis for data processing.⁸¹

Some data protection laws have created a specific legal basis to allow the processing of data in arbitral proceedings. According to the Brazil Act, for example, processing of personal data, including sensitive data, is expressly authorised “for the regular exercise of rights in judicial, administrative or arbitration procedures”.⁸² This is similar to the legal claims exemption in the GDPR, which applies to special category data processing and third-country transfers, but not to general personal data processing (and does not refer expressly to arbitration although its coverage is broad enough to include arbitration).

Where the GDPR applies, the following bases are generally best suited to data processing in the context of international arbitration:⁸³

- **Personal Data.** The processing of personal data is lawful when it is necessary for the purposes of the legitimate interests of the data controller (in this case one or more Arbitral Participants) or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring protection of their personal data.⁸⁴ For example, the data subject’s rights might override the legitimate interest in processing if the processing could raise significant risks to a data subject’s professional or personal life and the personal data is not likely to be determinative for the parties’ dispute. When relying upon legitimate interests for processing of personal data, the EU Working Party has taken a view that a Legitimate Interests Assessment should be undertaken and recorded (*see Annex 5* for a checklist), which is to be updated if events occur that might affect the original assessment.⁸⁵ If issues are raised about the processing of personal data during the arbitration, it will be helpful to be able to show the competent authority that a Legitimate Interests Assessment was undertaken contemporaneously.

81. *See* India Act.

82. Brazil Act, Arts 7(VI) and 11(II, d).

83. Note that there are other bases for lawful processing, but we only mention those that are most likely to be the suited to arbitration, taking into account the circumstances.

84. A “Legitimate Interests Assessment” refers to an analysis undertaken to identify the particular interests being relied upon when a data controller uses “legitimate interests” as the lawful basis for processing (*see Annex 5*).

85. EU Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, 844/14/EN, WP 217, 9 April 2014; EDPB, “Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects”, 8 October 2019.

- **Sensitive (Special Category) Data.** The processing of sensitive (special category) data is lawful when it is “necessary for the establishment, exercise or defence of legal claims”, which we refer to as the “legal claims derogation”.⁸⁶ The legal claims derogation will often be the preferred basis for processing sensitive data. It may apply to allow data processing where, for example, the processing of the sensitive data is likely to have a significant impact on a claimant or respondent’s case. Personal data of children is also given special consideration.⁸⁷
- **Criminal Convictions and Offences, or Related Security Measures.** In addition to requiring a lawful basis for the processing of data,⁸⁸ the processing of personal data relating to “criminal convictions and offences or related security measures” shall be “carried out only under the control of official authority or when the processing is authorised by Union or *Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*.”⁸⁹ Deciding whether the data falls under this provision is fact specific, and the CJEU has recently said that the objective of Article 10 should be kept in mind in making this determination, which it said is “to protect the data subject from processing that could risk leading to serious interference with his or her private or professional life, for example ... social disapproval or stigmatisation of the data subject.”⁹⁰ However, not all data regarding suspected criminal offences is covered as the data should be sufficiently specific and related to the potential offence.⁹¹ When it is determined that the data in

86. GDPR Art. 9(2)(f).

87. In the event that an arbitration involves the processing of special category data on a large scale, as well as in other circumstances likely to create a high risk to the rights and freedoms of individuals, a data protection impact assessment is required under the GDPR prior to processing (GDPR Art. 35(1), (3)).

88. GDPR Art. 9(2)(f).

89. GDPR Art. 10 (emphasis added).

90. Judgment of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504.

91. In Sweden, for example, the data must be concrete to a certain degree to qualify as personal data relating to criminal offences, which it is if it concerns a certain crime or category of crime or if data is compiled in such a way that the data corresponds to the objective criteria in a penal provision. If the purpose of the processing is wholly or partly to process data related to criminal offences, this indicates that the data is covered by the scope of Article 10 of the GDPR. Regulatory statement of the Swedish Authority for Privacy Protection (IMY) (8 December 2021); see Magnusson Law, “Processing of personal data relating to criminal offences in Sweden – New regulatory guidance on the interpretation of Article 10 of the GDPR”, available at <https://www.magnussonlaw.com/news/processing-of-personal-data-relating-to-criminal-offences-in-sweden-new-regulatory-guidance-on-the-interpretation-of-article-10-of-the-gdpr/>.

question is criminal offence data, whether it can be processed in an arbitration, either commercial or investor-State, will typically turn on whether processing is allowed under *Member State law*, which law may apply to the legal claims derogation to criminal offence data, and raises the question as to which Member State law should be applied. This all requires careful consideration in the context of the specific case.

After considering these factors, the Data Protection Directions should set forth the lawful basis for the processing of personal data during the arbitration proceeding. This will preclude, for example, parties potentially using lack of consent or the withdrawal of consent as a basis to resist the processing of personal data during the arbitration.

(2) Lawful Basis for Personal Data Transfer

Arbitral Participants should identify and document at the outset of the proceedings any applicable restrictions on third-country transfer of personal data and what steps will be taken to transfer personal data in compliance with the restrictions. This includes any applicable data localisation laws which might impact the conduct of proceedings. Compliance with these laws during an arbitration can impact the process and requires advance planning.

Each Arbitral Participant that is required to make transfers to other jurisdictions in the context of an arbitration is required to comply with the data transfer restrictions applicable to them. However, to make this workable in the context of the arbitration proceedings, the rules applicable to transfer should be harmonised where possible. Under the GDPR, for example, the following criteria apply:

- Does an adequacy decision apply to the country to which transfer would be made? For example, at the time of publication, data transfers from the EU to a party in Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay are lawful because they have been declared to be adequate jurisdictions.
- If not, is it feasible to put appropriate safeguards in place? For example, data transfers from the EU to third countries can be based on standard contractual clauses, which can be agreed by the Arbitral Participants. Standard contractual clauses require those entering into them to follow a light version of the GDPR. EU guidance suggests that standard contractual clauses or another adequate safeguard should be put in place where feasible, which also means that, provided they are complied with, it is not necessary to take additional

safeguards in advance of transfer because the presumption is that the personal data will be sufficiently protected after transfer.

- Where standard contractual clauses or other adequate safeguard cannot feasibly be put in place for a justifiable reason, is it possible to rely on an express derogation? In the context of an arbitration, this is most likely to be the legal claims derogation which, in the context of the transfer of personal data, requires the third-country transfers to be “occasional” and “necessary for the establishment, exercise or defence of legal claims.” Moreover, advice from the EU Working Party suggests that additional safeguards should be put in place in advance of transfer, including that the personal data should be minimised (including culling for relevance, and potentially redaction or pseudonymisation of personal data), and confidentiality provisions should be entered into.⁹²
- If not, is there a compelling legitimate interest in the data being transferred? In such a case both the data subjects *and* the supervisory authority must be notified. In practice, this derogation is unlikely to be applied because notifying both the data subjects and the supervisory authority in advance of transfer may prejudice a party’s case, jeopardise attorney-client privilege or compromise the confidentiality of the arbitration.

It may be even more difficult to transfer data out of jurisdictions that have localisation regimes. The reference to localisation refers to the fact that in principle certain types of data, often including personal data, cannot be transferred abroad.

After considering these factors, the Data Protection Directions should set forth the lawful basis for the transfer of personal data during the arbitration proceedings. Where they can be agreed, standard contractual clauses are the legally preferred means of legitimising a data transfer and do not require additional safeguards, which may facilitate document production. Where this is not feasible and the legal claims derogation is relied upon, it is advisable to state that the transfers will be occasional, that they are considered to be necessary for the establishment, exercise or defence of legal claims in the arbitration, that they will be treated confidentially, and how the data transferred will be minimised in advance of the transfer, including culling for relevance and possible redaction or pseudonymisation of personal data (although this will not always be necessary). Adding this language in the Data Protection Directions reduces the chances that data protection will be relied on as a basis to avoid data transfers in the context of the arbitration, most likely during disclosure.

92. EU Working Party, “Working Document 1/2009 on pre-trial discovery for cross border civil litigation”, WP 158, 11 February 2009 (“Document Disclosure Guidance”), at 10-11.

(3) Disclosure or Production of Documents

Document disclosure is an important part of the international arbitration process, and the impact of data protection laws should be specifically considered in the context of document production. To the extent required by the applicable laws, third-country transfers may need to be limited and the information disclosed may need to be minimised, for example by culling for relevance and materiality, the application of search terms and artificial intelligence during review, or redacting or pseudonymising personal data prior to disclosure, and otherwise limiting the personal data produced to that which is necessary for the resolution of the dispute in line with the applicable lawful basis for processing.

The IBA Rules will often be applied as guidance to document disclosure. Under the IBA Rules, the parties should first attempt to agree on disclosure, followed by tribunal decision when agreement is not possible. Where the data protection laws apply, one aspect of that agreement should be to consider how the data protection laws will impact the disclosure process.

This means that, where possible, the impact of the data protection rules on the document production process should be addressed in the Data Protection Directions, to avoid these arguments being raised later and to reduce cost and time. Issues to be addressed may include: (1) limiting disclosure/data minimisation (taking into account the IBA Rules where applicable); (2) redaction/pseudonymisation in light of the applicable data protection standard; (3) entering into confidentiality provisions/protective orders; and (4) entering into standard contractual clauses or another adequate safeguard for third-country data transfers so that additional safeguards are not required, or where that is not feasible, employing a derogation when possible.

In deciding what data protection measures to adopt, Arbitral Participants should consider the scope of the necessary compliance requirements and the importance of the data for the arbitration. This may be complicated in the event that only one of the parties is subject to strict data protection obligations, which may lead to issues concerning equality of treatment. In cases where the IBA Rules are applied, relevant data protection restrictions will need to be considered and applied in conjunction with the standards applied by the IBA Rules, with the data protection rules being mandatory.

The impact of data protection laws on document disclosure, with specific reference to the GDPR and the IBA Rules, is considered in more detail the following Section.

(4) Data Security and Data Breach Protocols

(a) *Data Security*

Arbitral Participants should apply a proportionate, risk-based approach to data security. Data security should be addressed at the CMC, which is required or recommended by many institutional arbitration rules (including for example the LCIA and the ICDR).

In terms of what should be considered, the GDPR provides that “appropriate” technical and organisational measures should be put in place. Deciding what security measures are “appropriate” requires consideration of the potential risk to data subjects, the existing information security measures of the Arbitral Participants, and what physical and technical measures are appropriate given the risks to the data subjects, and includes, as pertinent:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.⁹³

In assessing the appropriate level of security under the GDPR, account shall be taken of the risks that are presented by the processing,⁹⁴ in particular from:

- Accidental or unlawful destruction;
- Loss;
- Alteration;
- Unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.⁹⁵

93. GDPR Art. 32(1).

94. Under Art. 42 of the Brazil Act, processing of personal data shall provide the level of security that a data subject can expect, considering the relevant circumstances (such as the risks that one can reasonably expect and the available techniques for processing personal data). Under Indian law, there are certain measures that an entity can take to comply with this requirement, one of which includes obtaining an IS/ISO/IEC 27001 certification, compliance with which would also be relevant to compliance with the GDPR.

95. GDPR Art. 32(2).

Applying data security standards in an arbitration will depend on many factors, including the Arbitral Participants' existing information security measures and their function in the proceedings, the size and types of organisations involved (including number of employees, their premises and data systems), the type of processing being undertaken and whether external service providers are used. Information security also depends on the types of data being processed, including how valuable, sensitive or confidential it is, and the damage or distress that may be caused to the data subject if the personal or sensitive data were to be compromised. In international arbitration practice these issues are increasingly being addressed through the use of secure platforms for the exchange of written submissions and evidence.

The fact that there is no one-size-fits-all solution to information security is stressed in the Cybersecurity Protocol (2022 Edition) and the IBA Cybersecurity Guidelines (2018). While these initiatives are not directed at data protection compliance, they provide a useful resource for the reasonableness test in relation to information security and how information security may be addressed in international arbitration.

The data security obligations of Arbitral Participants are inter-linked, and a breach of security by one will have an impact on all. In this respect, all Arbitral Participants should:

- Consider what information security measures they already have in place;
- Employ information security measures appropriate to the size and use of their network and information systems;
- Take into account the state of technological development (though the cost of implementation can also be a factor);
- Employ information security measures appropriate to their business practices, the nature of the personal data processed and the harm that might result from any data breach; and
- Undertake a risk analysis in deciding what information security measures to employ and document the findings.

In deciding what should be included in the Data Protection Directions concerning data security to help manage risks, Arbitral Participants should consider whether additional information security measures are required for the arbitration in addition to those already employed by the Arbitral Participants in their ordinary course of business. Reference may be made to the Cybersecurity Protocol (2022 Edition) and the IBA Cybersecurity Guidelines (2018) where appropriate.

(b) Personal Data Breach Protocols

Where data security measures in place fail to prevent a data breach, EU-style data protection laws impose strict notification requirements.

Personal data breach is defined by the GDPR, for example, as a breach of security “leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed for purposes of the arbitration” (GDPR Art. 4 (2)). Under the GDPR, there are three types of data breaches:

- “Confidentiality breach” means an unauthorised or accidental disclosure of, or access to, personal data.
- “Integrity breach” means an unauthorised or accidental alteration of personal data.
- “Availability breach” means an accidental or unauthorised loss of access to, or destruction of, personal data.

Under the GDPR, not all data breaches require notification, but they must all be recorded. Where the GDPR applies, Arbitral Participants are required to:

- Notify the supervisory authorities in case of a data breach unless it can be shown that it is not “likely to result in a risk for the rights and freedoms of the data subject.” They must also notify the data subjects themselves of the breach without undue delay if the risk to personal data and data subjects from a breach is considered to be “high” (*e.g.*, GDPR Art. 34).⁹⁶ The burden of proving the absence of risk in a data breach rests on the data controller (*e.g.*, GDPR Arts. 33-34).
- Where notification is required, it must be made without undue delay and, where feasible, not later than 72 hours after becoming “aware” of the breach (*e.g.*, GDPR Arts. 33-34). The EU Working Party has indicated that a data controller is deemed to become aware of a breach when it has a “reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised”.⁹⁷ With respect to content, a breach notification must include the cause and nature of the breach (if known) and recommendations as to how the potentially affected individuals can mitigate the risks of the breach.

96. Art. 48, Para.1 of the Brazil Act requires a notification “within a reasonable period of time”.

97. EU Working Party, ‘Guidelines on Personal data breach notification under Regulation 2016/679’, WP250rev.01, 3 October 2017 (last revised and adopted 6 February 2018), at 11 (“Data Breach Guidelines”).

- In all cases, a record of the breach must be kept.

Given these obligations, when a personal data breach occurs or is suspected, it is important for Arbitral Participants to determine quickly whether mandatory reporting requirements may be triggered and by whom. A data breach may impact personal data provided in the context of the arbitration by the parties, the arbitral tribunal and/or any arbitral institution, each of whom may have legal or ethical obligations arising out of that data breach, including notification. In most cases, a party or its counsel will have collected the personal data processed during an arbitration, exchanged that personal data with the other party(ies) and their counsel, and potentially submitted the personal data to the tribunal and the institution. A personal data breach suffered by any of these Arbitral Participants may trigger a requirement that any or all of them notify relevant authorities and potentially the data subjects.

Given the risks associated with data breaches and the short time allowed to address them, it is therefore advisable that the Data Protection Directions include a data breach protocol to be applied amongst those involved in the proceedings. This should cover (1) what will constitute a data breach; (2) the procedure that will be followed if a breach occurs; (3) what information shall be provided about a data breach; (4) who will be notified and when, including that Arbitral Participants shall be obligated to inform each other of a data breach without undue delay; and (5) duties to provide information and to cooperate with respect to notification.

Note that a personal data breach protocol adopted for an arbitration typically would not seek to address the individual reporting obligations of individual Arbitral Participants, but rather seek to ensure that all participants are made aware in a timely fashion of incidents that may trigger obligations under EU-style data protection laws and to define how they should address such breaches vis-à-vis each other when they impact arbitral data and to require cooperation and communication amongst them with respect to notification.⁹⁸ Arbitral Participants governed by the GDPR may refer to useful guidance issued by the European Commission in terms of when notification is required and what needs to be done.⁹⁹

In order to assist Arbitral Participants, Schedule D-1 of the Cybersecurity Protocol (2022 Edition) includes a sample personal data breach protocol, which is drafted taking the GDPR requirements into consideration. [Annexes 7](#) and [8](#) of this Roadmap also include

98. See Schedule D-1 of the Cybersecurity Protocol (2022 Edition) for a sample personal data breach protocol based on the GDPR.

99. See Data Breach Guidelines and the recently issued Guidelines 01/2021 on Examples regarding Personal Data Breach Notification Adopted on 14 December 2021 Version 2.0.

general language that may be employed to address data breaches, preferably with reference to a personal data breach protocol, such as that found in Schedule D-1 of the Cybersecurity Protocol (2022 Edition).

(5) Managing Data Subject Rights

The Data Protection Directions should include measures to comply with data subject rights, including data subject access requests, update and correction requests.

Arbitral Participants may receive requests from data subjects seeking to exercise their rights during the arbitration process. These requests may come from any individual whose personal data is handled during the arbitration process, including, but not limited to, individual parties, witnesses, experts or even persons not directly involved in the proceedings but about whom personal data may have been adduced (*e.g.*, an employee of a party, who is not involved in the proceedings directly, or an employee of a third party, who is not a party to the arbitration), and who believes that their data is being processed. These data subject requests will need to be addressed within a prescribed time frame (under the GDPR this is “without undue delay and in any event within one month”). It is therefore important to consider procedures for doing so in advance.

In the arbitration context, data subject access requests may be aimed either at preventing data from being used in the arbitration or at obtaining access to processed data, both of which may trigger issues of confidentiality and privilege. The GDPR and the Brazil Act, for example, provide that the data subject has the right to obtain from the controller (in this case an Arbitral Participant) confirmation as to whether or not their personal data is being processed, and, if that is the case, the right of access, which should include electronic access, to a broad range of information about that processing, as well as a copy of the data processed, provided that the provision of a copy does not interfere with the rights and freedoms of others.¹⁰⁰

Upon receipt of a valid data subject access request, Arbitral Participants are required to provide the data subject with electronic access to the personal data they hold about them or a copy thereof, provided the provision of electronic access or a copy does “not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software”.¹⁰¹ Furthermore, in some EU Member States, including Germany, a client’s right to secrecy may prevail over the data subject’s right of access. However, the GDPR provides expressly that “the

100. See GDPR Recital 63 and Art. 15(4).

101. *Ibid.*

result of those considerations should not be a refusal to provide all information to the data subject”.¹⁰²

When acceding to a data subject access request, each Arbitral Participant should carefully consider the impact that meeting the request might have on its own legal and ethical obligations and those of others (both Arbitral Participants and third parties) and identify and implement measures to reduce any potential adverse impact. For example, Arbitral Participants might redact personal data relating to individuals that are not relevant to the dispute or restrict access to those documents or portions thereof that are strictly necessary to meet the exact terms of the data subject’s request rather than adopting a blanket (and likely less time consuming) approach. National courts have also suggested that striking a balance between different stakeholders’ interests might involve obtaining undertakings from the data subject to restrict the onward transfer of any information disclosed in response to the data subject access request.¹⁰³

Data Protection Directions should provide the mechanisms for complying with data subject rights, including data subject access requests, update and correction requests. This should include who is responsible for addressing the request in the first instance. For example, it is usually preferable for the party who initially collected the personal data to address the request, or the party who presented the personal data in the arbitration, depending on the circumstances. In any case, it is generally advisable to provide that the arbitrators will not be required to respond to data subject right requests unless and until other means of responding have been exhausted.

(6) Notification

Arbitral Participants who are data controllers or joint controllers are responsible for ensuring that data subjects are put on notice that their personal data is being processed for the purposes of the arbitration and are informed of other details about the data processing. However, in the case of a confidential arbitration, providing such notices could compromise the confidentiality of the arbitration. Moreover, in the absence of a relationship with the data subject, arbitrators and institutions may have no realistic means of providing notice.

The requirement to give notice applies to each data controller, of which there will be many in an arbitration. Given that any arbitration involves multiple data controllers, this could lead to one data subject receiving multiple notices.

102. GDPR Recital 63.

103. *B v. General Medical Council* [2018] EWCA Civ 1497, 28 June 2018 (UK).

Many of the data controllers in an arbitration will not have originally collected the personal data from the data subjects. In order to avoid overlapping notices, the GDPR, for example, provides significant exemptions from the notice requirements for data controllers who did not originally collect the data from the data subject. Many of those exceptions are potentially applicable to processing by Arbitral Participants who did not directly collect data from individuals (like the arbitrators, the institution and the opposing party/counsel), which means that they would not be required to provide an additional notice.¹⁰⁴

However, each Arbitral Participant will need to determine their notification obligations on a case-by-case basis. These obligations may differ based on where the Arbitral Participant is established, where the personal data was collected, where the data subjects are located and where the personal data is processed.

In order to ensure notice is given without overburdening the arbitration process, the Data Protection Directions may be employed to place the burden to provide notice either on the Arbitral Participant that collected the personal data for purposes of the arbitration or the one that originally collected the data, depending on the circumstances.

(7) Documenting Data Protection Compliance

Accountability requires data controllers to take personal responsibility for data protection compliance and to record the measures they take to comply with their data protection obligations. Under the GDPR, for example, data controllers are expected to be able to “demonstrate compliance” with the data protection principles it establishes as they are

104. Under the GDPR Art. 14(5) and Recital 62, where the data controller did not originally collect the personal data, they are not required to provide notice, *inter alia*, where:

1. The individual data subject already has the required information on the processing of his or her personal data;
2. Providing information on the processing of personal data to the individual would be impossible;
3. Providing such information to the individual would involve a disproportionate effort;
4. Providing such information to the individual would render impossible or seriously impair the achievement of the objectives of the processing; or
5. The data controller is subject to an obligation of professional secrecy regulated by EU or EU Member State law that covers the personal data.
6. In the cases mentioned in the second, third and fourth bullet points above, the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available.

implemented throughout the GDPR.¹⁰⁵ Adequate records should be kept of what compliance measures were taken and why, in a manner that they can be shown to the competent authorities if compliance issues were to arise.¹⁰⁶

In the context of an arbitration, particularly a confidential arbitration, it will be important to document in the Data Protection Directions who is responsible for documenting compliance, the form of such documentation and that when requested by a data protection authority, it can be provided.

(8) Use of Online Case Management Platforms to assist with Compliance

Online case management platforms can assist with discrete data protection obligations during the course of the proceedings, taking into account that use of the platform will itself constitute data processing and need to comply with applicable data protection laws.

The use of AI tools on the platform (particularly through unsupervised learning, which may help to cluster documents that appear to have personal data within them), may facilitate compliance with data minimisation obligations. Using a platform can also help to ensure (through agreement at the outset of the setup process) that data will be deleted and destroyed once the purpose for which it was being processed has ended (*i.e.*, normally within an agreed period of time following completion of the arbitration and receipt of the award by the parties).

Compliance with transparency and accountability obligations can also be facilitated by using online case management platforms. Data controllers and processors are required to keep a record of their data protection compliance efforts in order to demonstrate compliance, respond to data subjects' requests for information regarding the processing of their personal data, notifying data subjects when their personal data is being processed, etc. A platform can help provide an audit trail of data flows, which can make it simpler and more cost effective to respond to such queries and demonstrate compliance. Setting formulaic "on-platform" processes that must be complied with enables a more efficient and accurate tracking of data flows than can readily be achieved manually at similar costs.¹⁰⁷

Use of an online case management platform during the course of the proceedings should be discussed at the CMC and potentially included in the Data Protection Directions particularly when the platform is used to assist in managing an Arbitral Participant's data

105. GDPR Art. 5(2); see also GDPR Art. 24(1).

106. Organisations with more than 250 employees must document compliance in accordance with GDPR Article 30, which provides a list of record-keeping obligations.

107. See Online Platform Protocol.

protection obligations during the course of the proceedings, or otherwise impacts data protection compliance.

(9) Conclusion on Documenting Data Protection Compliance

The key to avoiding data protection compliance from becoming an issue during the proceedings is to address and document the means adopted to address data protection from the outset:

- Data protection should be on the agenda for the initial CMC. This Section of the Roadmap has addressed the most important issues to be addressed and potential solutions for each of them using the GDPR as an example.
- Whenever possible, agreement should be reached, but where agreement is impossible, the tribunal can issue directions after hearing the parties.
- Data Protection Directions, whether agreed or ordered, should then be documented through a data protection protocol (*see* [Annex 8](#)) or through language included in the terms of reference or procedural order (*see* [Annex 7](#)), which should indicate where agreement was reached.
- Although this is highly case and fact specific, [Annex 7](#) provides sample language addressing each of these issues that may be considered for inclusion in Data Protection Directions using the GDPR as an example and [Annex 8](#) provides sample language for a Data Protection Protocol when appropriate.

4. When Data Protection Issues Arise During the Proceedings

Data protection issues may arise during the course of the proceedings. The most common source of data protection issues is the document disclosure process, which has become an important part of both international commercial arbitration and investor-State arbitration. Data breaches and data subject rights requests are also possible during an arbitration and will need to be managed to avoid potential disruptions.

Document Production. The document production process involves the collection, review, transfer to counsel, production of the documents to the other party, and potential presentation as evidence to the tribunal. It is important to recall that anything that is used or produced during an arbitration that allows an individual to be identified is personal data of that individual (emails, texts, WhatsApp messages), and that each of these activities is an activity of processing personal data. Therefore, the data protection laws apply to the document production process from start to finish and that process typically involves the processing, often including cross border transfers, of significant amounts of personal data.

Among other things, issues that may be raised under data protection laws may concern:

- Lawful basis for the processing;
- Lawful basis for the transfer;
- Data minimisation including any need for redaction/pseudonymisation; and
- Whether the data subjects (especially third parties) are on notice of the processing.

Using the EU data protection laws as an example, this Section considers the data protection principles applicable to document disclosure, and how these principles may be applied generally and taking into account the IBA Rules.

Data Protection Principles Applicable to Document Disclosure. The obligation to minimise data, which is found in most data protection laws, is particularly relevant to document disclosure. Although data minimisation is a general obligation,¹⁰⁸ there is no guidance as to how this should be applied in the arbitral process generally or during the document disclosure/production phase in particular.

Using the EU data protection laws as an example, the EU Working Party has provided guidance on the application of the EU Data Protection Directive to data transfer for purposes of discovery for US litigation, which guidance remains applicable. The EU Working Party suggested that data minimisation is likely to require: (1) culling the documents to be disclosed for relevance; (2) redacting unnecessary personal data; (3) entering into confidentiality provisions/protective orders; and (4) putting adequate safeguards in place for third-country transfer.¹⁰⁹ Similar principles would be expected to apply under the GDPR in the context of an arbitration.

The approach taken by the Working Party suggests the application of a three-step process aimed at minimising the personal data disclosed, followed by considerations of confidentiality and third-country transfer:

1. Limiting the data disclosed to what is relevant to the dispute and non-duplicative (often referred to as “culling”);
2. Where justified by the risk posed, identifying and redacting or pseudonymising unnecessary personal data.

108. The EDPB has stated that “the principle of data minimization ... emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which [it is] processed.” Data Transfer Guidance, at 13.

109. Document Disclosure Guidance, at 10-11.

In considering how these principles apply to international arbitration, culling for relevance is a measure already used in practice in arbitration to reduce the volume of data processed and disclosed. However, different approaches are taken to the extent to which culling is required and allowed, and at what stage it is undertaken. Moreover, redaction of personal data is not yet common practice and is not always required.

Application of Data Protection Principles in Practice, Including in Conjunction with the IBA Rules. The IBA Rules are widely applied to the disclosure of documents in international arbitration. Given the prevalence of the IBA Rules, it is useful to consider how data protection requirements may impact disclosure under the IBA Rules, keeping in mind that data protection requirements are legally required and therefore must be applied to supplement the IBA Rules or any other standard generally applied to disclosure in international arbitration.

The IBA Rules provide that the parties may agree on the disclosure of documents, and where agreement is not possible, the parties may petition the tribunal to order disclosure. Even where the IBA Rules are not applied to the process, a similar process is likely to be applied.

As described above, the best place to address data protection compliance during the disclosure process is through agreed Data Protection Directions. However, even where Data Protection Directions are given, issues may arise in interpreting those directions. In other cases, there will not be any Data Protection Directions or they will not have addressed disclosure, in which case, these issues will be addressed by the tribunal for the first time when making decisions on document requests.

Under the IBA Rules, the standard to be applied by the tribunal in deciding on a document request is whether the document “is relevant to the case and material to its outcome”. This standard is consistent with the concept of data minimisation and the guidance given by the EU Working Party. Article 9(2) of the IBA Rules empowers the tribunal to exclude from evidence or production a document for a number of reasons, including “legal impediment or privilege under the legal or ethical rules determined by the Arbitral Tribunal to be applicable”¹¹⁰ and “grounds of commercial or technical confidentiality that the Arbitral Tribunal determines to be compelling.”¹¹¹ The Commentary on the IBA Rules identifies that personal data protection considerations under the GDPR

110. IBA Rules Art. 9(2)(b).

111. IBA Rules Art. 9(2)(e). IBA Task Force for the Revision of the IBA Rules on the Taking of Evidence in International Arbitration, “Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration” (January 2021) <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D>, at 29.

and similar national legislation may come under the limb of “commercial or technical confidentiality”, and consideration should also be given to whether it constitutes a “legal impediment”.

The IBA Rules do not address the possibility of redacting and/or pseudonymising unnecessary personal data, although the redaction and/or pseudonymising of personal data is not inconsistent with their principles when necessary for data protection compliance.

The question as to whether data protection considerations may limit document disclosure generally, or whether, if production is allowed, redaction and/or pseudonymising of personal data is necessary (and if so, the extent to which it is required, and the method to be applied), is highly case specific, and the parties may disagree. Considerations to be taken into account by the tribunal in deciding these issues may include:

- Has the party objecting to disclosure and/or arguing that redaction and/or pseudonymising is necessary, established to the satisfaction of the tribunal that this is required by applicable data protection laws?
- Is third-country data transfer required, and if so, can effective safeguards be put in place? For example, where cross border disclosure of documents including personal data is contemplated, this would favour putting in place standard contractual clauses or another safeguard where feasible, rather than relying on a derogation (like the legal claims derogation).
- Are alternatives available allowing the documents to be produced (or to be produced without redaction and/or pseudonymising) – for example, if third-country data transfer is an obstacle, could standard contractual clauses be employed or could the documents initially be reviewed locally?
- How extensive is the document disclosure being sought from the tribunal?
- Have reasonable measures been agreed to cull for relevance/materiality and lack of duplication?
- To what extent would a decision to allow the document disclosure with or without redaction affect the rights of interests of the data subjects identified in the documents? This may be impacted by what type of personal data is likely to be included, and whether it is likely to contain sensitive or criminal offence data. For example, in a case where the documents being disclosed contain a limited set of documents that were exchanged during the course of a business relationship by those involved in the facts at issue, this may be considered in deciding the extent to which the production should be allowed and/or redaction/pseudonymising be required.
- To what extent would a refusal to allow the disputed document disclosure impact the rights of a party to be heard?

- Are confidentiality/protective orders in place covering the documents to be disclosed either through entering into standard contractual clauses or other means?

A blanket refusal to disclose documents in light of applicable data protection restrictions is not justified. In most situations, the entire document will not be considered personal data, but only the words, phrases or parts of the document relating to the data subject. This distinction is important in relation to document production, as data protection requirements would rarely justify withholding an entire document, but may justify redaction.

However, the tribunal will need to consider what means should be put in place to ensure reasonable data protection compliance and at the same time allowing the necessary disclosure to ensure justice is served. As discussed above in [Section II.B.3.c\(3\)](#), technology, including artificial intelligence, may assist in both culling the data for relevance and in redacting personal data through the use of an online case management platform or otherwise. However, it should be recalled that these measures themselves constitute data processing and can be costly and time consuming, especially with large amounts of data.

Under the GDPR, for example, given the broad definition of personal data,¹¹² a practical approach may need to be applied to whether, and if so the extent to which, redaction is required, taking the concept of proportionality into consideration. As discussed in [Section I](#), a data subject has a mandatory right to have their personal data protected, but that right is not absolute. Similarly, the parties to an arbitration have a right to be heard, but that right does not include unfettered disclosure, and by agreeing to arbitration they agree to a process that needs to comply with data protection laws. Therefore, these rights need to be balanced and the data protection laws applied in proportion to the risk to the data subject posed by the document disclosure, keeping in mind the important role that arbitration plays in the administration of justice but in all cases, the rights of the data subject must be adequately protected.

Data Breach. Security incidents are becoming increasingly common and Arbitral Participants are no exception. This stresses the importance of including a data breach protocol in the Data Protection Directions, so if a security incident occurs everyone knows what to do and when.

112. The CJEU held for example that “the term personal data ... undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies”, Judgment of 6 November 2003, *Lindqvist*, C-101/01, 2003 I-12971, para. 24.

Whenever a personal data breach occurs in a case where an EU-style data protection laws applies, Arbitral Participants will need to notify each other without undue delay that a personal data breach has occurred that may impact personal data being processed for the arbitration, as discussed in [Section II.B.3.c\(4\)](#) above.

This will allow each Arbitral Participant to decide whether a notification is required applying the principles discussed in the preceding Section. This has to happen quickly because, for example, when an Arbitral Participant experiences a personal data breach falling within the notification requirements of the GDPR, the data controller will be required to make a notification without undue delay (and where possible within 72 hours) unless the data controller can establish that the data breach is not “likely to result in a risk for the rights and freedoms of the data subject.” Moreover, notification may impact the arbitration and the other Arbitral Participants, and as more than one Arbitral Participant may be required to notify, it is important to stress communication and cooperation amongst the Arbitral Participants with respect to any notifications.

Data Subject Rights Requests. As discussed in [Section II.B.3.c\(5\)](#) above with respect to Data Protection Directions, another issue that may arise during an arbitration is that a data subject may seek to enforce its rights to have access to their personal data (or another right) from an Arbitral Participant. This can be a genuine request or an attempt to derail the process.

Regardless of whether Data Protection Directions are in place, when a data subject right request is received concerning arbitral data, the Arbitral Participant receiving the request should usually inform the other Arbitral Participants of the request. The issue then arises as to who should address the request. Where possible, given the nature of the arbitral process, it is usually advisable for the Arbitral Participant that collected the personal data from the data subject to address the request in the first instance and to inform the data subject. This is especially the case when the request is directed at an arbitrator.

5. Remote Hearings

During the COVID-19 pandemic, it has become the norm to hold remote hearings. Moving forward, conducting remote hearings, and partially remote hearings, will continue to occur regularly.

When it is decided to hold a remote hearing, it will be important to establish a protocol for the hearing, not least because the remote hearing platform provider may be considered as a processor of personal data. For example, the IBA Rules address remote hearings in Article 8.2 and suggest that the tribunal must consult with the parties to establish a remote hearing protocol that addresses several issues, including: (1) the technology to

be used; (2) advanced testing of the technology or training; (3) starting and ending times, considering varying time zones; (4) how documents may be placed before a witness; and (5) measures to ensure that witnesses giving testimony are not distracted or improperly influenced.

It will also be important that any data protection and data security issues posed by a remote hearing are also addressed in the protocol. There are many examples of such protocols. However, many remote hearing protocols do not address the data protection issues that may be faced. [Annex 7](#) includes sample language that may be included in the Data Protection Directions when the GDPR or a similar EU-style data protection law applies, and similar language should be considered for inclusion in any remote hearing protocol that may be issued or agreed.

6. Arbitral Awards and Other Decisions

Arbitral tribunals process personal data (including potentially sensitive data and criminal offence data) when preparing, drafting and rendering their orders, decisions and awards, while arbitration institutions process personal data when constituting tribunals, dealing with applications of the parties, rendering challenge decisions, overseeing the proceedings, scrutinising and notifying awards, etc.

Even in confidential arbitrations, the award may become public if it is enforced in a country where awards (or parts thereof) become public in the enforcement process. Moreover, in investment and treaty-based arbitrations, awards are often published and commercial institutions are increasingly considering the publication of awards if the parties do not object and subject to possible redaction, and (excerpts of) challenge decisions.

Before the award is rendered, Arbitral Participants should consider the extent to which personal data should be included in the award and any steps that might be taken to minimise the inclusion of personal data in the award and to ensure its confidentiality when applicable. For example, while reference may be made to the evidence of a certain witness and that witness's role for weighing the evidence, it may not be necessary to provide any further personal data about that witness in the award. Further, even where the personal data has been minimised, it remains personal data, and before publishing awards, consideration should be given to the impact this has on data protection compliance.

In this framework, arbitrators and institutions should consider the basis and necessity for the inclusion of personal data in awards and decisions and whether they wish to raise this issue with the parties before rendering an award or decision. In some EU countries, for example, it is standard practice to redact personal data from court decisions. It is important to bear in mind that even where personal information about a witness has been minimised, the references in the award remain their personal data because they are still

identifiable from the remainder of the award or related materials, and therefore the data in the award must be processed in compliance with data protection laws.

C. AFTER THE ARBITRATION

Arbitral Participants should consider how long to retain personal data connected with proceedings and the time after which such personal data and/or the documents containing it should be destroyed or permanently deleted.

Both data retention and deletion are considered data processing under many EU-style data protection laws. The GDPR, for example, provides that personal data shall be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed” (GDPR Art. 5(1)(e)).¹¹³

This principle ensures that personal data is only stored for as long as necessary for the purpose for which it is being processed. This requires controllers to consider, document and be able to justify the duration of storage. Moreover, the personal data being stored should periodically be reviewed, and securely erased or anonymised when it is no longer required. Personal data may be retained for longer intervals for public interest archiving, scientific or historical research, or statistical purposes (which is an important driver for data retention by arbitral institutions).

Arbitral Participants will be required to store personal data for a certain period after a case is completed. They will each need to consider what data retention period is reasonable in light of the purpose of the processing, including the arbitration itself and the enforcement of any award, as well as any attendant processing in light of, for example, future conflict checks and legal and regulatory compliance (for example, for income tax and audit purposes). In this regard, the purpose limitation principle also applies to the storage of personal data (*see* [Section I.F.4](#)). Arbitral Participants should bear in mind that potential use in other legal proceedings may not be a sufficient basis to retain data beyond an otherwise reasonable period of time.

Arbitral Participants, like all data controllers, should consider how long to retain personal data connected with proceedings and the time after which such personal data and/

113. Similarly, under Articles 15 and 16 of the Brazil Act, the processing of personal data shall be terminated as soon as its purpose has been achieved. Further, unless there is a legal basis for keeping personal data, it shall be deleted following the termination of the processing of the data. Under Indian law, sensitive personal data of an individual should not be stored or retained for longer than is necessary to fulfil the purpose for which it is collected.

or the documents containing it should be destroyed or permanently deleted. This means that they should:

- Retain personal data only for as long as reasonably necessary;
- Be able to justify how long they retain personal data, which will depend on the purposes given to the data subject for holding the data;
- Periodically review the data held, and erase or anonymise it when they no longer need it; and
- Carefully consider any challenges to their retention of data.

CONCLUSION

When an Arbitral Participant is subject to a data protection law, compliance is legally required. In practice, this means that data protection principles need to be applied during the arbitration to supplement the applicable laws, the arbitration rules, and soft law instruments (including the IBA Rules). The aim of this Roadmap is to enable Arbitral Participants to identify and effectively address data protection issues in the context of arbitral proceedings.

Sensible solutions exist permitting data protection laws to be applied during the arbitral process, which is facilitated when: (1) Arbitral Participants adopt a reasonable, cooperative, and proportionate approach to data protection compliance; (2) data protection is addressed at the initial case management conference; (3) Data Protection Directions are employed; and (4) compliance efforts are documented in a manner that can be shared with data protection authorities, if requested.

ANNEXES

All views expressed in these Annexes are those of the Task Force and not those of ICCA, the IBA, their governing bodies, or members. These Annexes are the result of the collective efforts of the Task Force, the views expressed are not attributable to any particular Task Force member and all Task Force members served in their individual capacity.

ANNEX 1

Glossary¹

A

“adequacy decision” refers to a decision made by the European Commission that a third country’s data protection laws are considered to be adequate and therefore data can be transferred outside the EU/EEA or to an international organisation without any further authorisation or notice because adequate protections apply as a matter of law (GDPR Art. 45(1)).

“Annexes” refers to the present set of annexes to the Roadmap.

“Arbitral Participants” is defined in the Roadmap as, and limited to, the parties, their legal counsel, the arbitrators and arbitral institutions.² While it is not explicitly addressed to them, the guidance provided in the Roadmap is also relevant to those working for or with Arbitral Participants during an arbitration, such as tribunal secretaries, experts and service providers (*e.g.*, e-discovery experts, information technology professionals, transcribers, translation services, online case management platform providers, remote hearing platform providers, etc.).

C

“California Act” or **“CCPA”** means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq.

“consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them (GDPR Art. 4(11)).

-
1. The glossary refers mainly to the GDPR. However, throughout the text of the Roadmap references are provided to similar concepts used in other EU-style data protection laws.
 2. In the case of arbitrations administered by an international organisation, determining whether any relevant privileges and immunities will impact the application of data protection laws turns on the breadth and scope of the relevant privileges and immunities both in terms of whether data protection laws would come within their scope, and, if so, which Arbitral Participants would be covered by them. This is an institution-specific enquiry.

“controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (GDPR Art. 4(7)).

“Controller/Processor Opinion” means the Opinion 1/2010 on the Concepts of “Controller” and “Processor”, EU Working Party, 00264/10/EN WP 169, 2010.

“criminal offence data” means data relating to criminal convictions and offences or related security measures (GDPR Art. 10).

“culling” means filtering data, including in the context of data minimisation (for example, during the disclosure process).

“Cybersecurity Protocol” means the ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitration (2022 Edition).

D

“data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (GDPR Art. 4(12)).

“data controller” – *see* “controller” above.

“data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about their health status (GDPR Art. 4(15)).

“data minimisation” is a principle established by the GDPR and other data protection laws according to which the processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed (GDPR Art. 5(1)(c)).

“data processor” is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (*e.g.*, GDPR Art. 4(8)).

“data protection authority” or “DPA” – *see* “supervisory authority” below.

“data privacy notice” or “data protection notice” refers to a document whereby the controller notifies the data subject in a concise and accessible form that their personal data is being processed and the purpose of the processing (*e.g.*, GDPR Arts. 12-14).

“Data Protection Directions” are procedural directions issued by an arbitral tribunal in the form of a procedural order, terms of reference, or a data protection protocol setting out how data protection will be addressed during the arbitration. They may be issued on an agreed basis or ordered by the arbitral tribunal.

“Data Protection Directive” means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281/31 (24/10/1995).

“Data Protection Protocol” refers to a document in which the roles and responsibilities of data controllers and processors vis-à-vis the processing of personal data are identified and agreed.

“data subject” means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art. 4(1)). Legal entities are not data subjects.

“data transfer” refers to transfers of data, which is broadly defined by the EU.

“Data Transfer Guidance” refers to the EDPB “Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679” dated 6 February 2018.

“Document Disclosure Guidance” refers to the EU Working Party “Working Document 1/2009 on pre-trial discovery for cross border civil litigation”, WP 158, dated 11 February 2009.

E

“establishment” implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect (GDPR Recital 22).

“European Data Protection Board” or “EDPB” is a body of representatives of national data protection authorities, the entity empowered to issue guidelines, recommendations and best practices to encourage consistent application of the GDPR and the setting of administrative fines (replaced the EU Working Party).

“European Economic Area” or “EEA” encompasses the twenty-seven EU Member States and three additional states: Iceland, Liechtenstein and Norway. The scope of application of the GDPR extends to the EEA, therefore, for ease of reference, the term **“EU”** as used in the Roadmap includes the EEA countries as well.

“European Union” or “EU” means the twenty-seven EU Member States: Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the Netherlands. The term EU as used in the Roadmap includes the EEA countries as well.

“EU Working Party” was a body of representatives of national data protection authorities, established under Article 29 of the EU Data Protection Directive, the GDPR’s predecessor. The EU Working Party was tasked with providing guidance on the application of data protection rules under the previous EU Data Protection Directive. The advice rendered by the EU Working Party remains valid until replaced, amended or abrogated by the EDPB, which performs a similar function under the GDPR.

F

“filing system” means any structured set of personal data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (GDPR Art. 4(6)).

G

“General Data Protection Regulation” or “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

I

“IBA Rules” means the IBA Rules on the Taking of Evidence in International Arbitration (International Bar Association, revised in 2020).

“Indian Act” means the India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011. India has not yet passed a comprehensive data protection law.

“international organisation” means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries (GDPR Art. 4(26)).

“ICO” means the UK Information Commissioner’s Office.

J

“joint controller” – refers to the situation where two or more controllers jointly determine the purposes and means of processing (GDPR Art. 26). Joint controllers are jointly responsible for compliance with the GDPR and jointly and severally liable for noncompliance.

L

“lawful basis” refers to one of the six possible lawful bases for the processing of personal data under the GDPR, one of which must apply whenever processing personal data (GDPR Art. 6).

“legitimate interests” is one of the lawful bases for data processing, and can be applied except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (GDPR Art. 6(1)(f); *see* [Annex 5](#)). The GDPR does not define what constitutes “legitimate” interests and a wide range of interests may be considered to be legitimate interests, including those of the data controller and third parties. When legitimate interests are relied upon as a basis for processing, a Legitimate Interests Assessment should be considered (*see* [Annex 5](#)).

“Legitimate Interests Assessment” refers to an analysis undertaken to identify the particular interests being relied upon when a data controller uses “legitimate interests” as the lawful basis for processing (*see* [Annex 5](#)).

“LGPD” or “Brazil Act” means the Brazilian General Data Protection Act (Statute 13709/18).

O

“Online Platform Protocol” means the Protocol for Online Case Management in International Arbitration, Working Group on LegalTech Adoption in International Arbitration (2020).

P

“personal data” means any information relating to a “data subject” (GDPR Art. 4(1)). See “*data subject*” above.

“personal data breach” – see “*data breach*” above.

“personal data of a child” is given special protection under the GDPR. Where personal data of a child is processed based on consent and the child is below the age of 16 years, such processing shall be lawful when the consent is provided by the holder of parental responsibility over the child. Member States may provide by law for a lower age provided that such lower age is not below 13 years (GDPR Art. 4(2)).

“processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR Art. 4(2)).

“processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller (GDPR Art. 4(8)).

“pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (for example, a coding system) provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. It is similar to redaction but requires that the data subject not be identifiable without additional measures (GDPR Art. 4(5)).

R

“Roadmap” refers to this ICCA-IBA Roadmap to Data Protection in International Arbitration.

S

“sensitive data” – see “*special category data*” below.

“special category data” is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data

concerning health or data concerning a natural person's sex life or sexual orientation. (GDPR Art. 9(1) and 9(2)(f)).

“standard contractual clauses” refers to clauses that have been adopted by the European Commission (or in some cases by a supervisory authority), which if entered into allow data to be transferred outside the EU in the absence of an adequacy decision (GDPR Art. 46). *See* Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) C/2021/3972 OJ L 199, 7.6.2021, 31–61. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

“supervisory authority” means an independent public authority which is established by a Member State pursuant to Article 51 GDPR (GDPR Art. 4(21)). It is also referred to as a **“data protection authority”** or **“DPA”**.

T

“targeting” is the term used to refer to activities whereby an individual or entity that is not “established” in the EU nevertheless comes within the jurisdictional scope of the GDPR, including when they (1) offer of goods or services to data subjects in the EU or (2) monitor the behaviour of data subjects in the EU (GDPR Art. 3(2), Recs. 23-24). The EDPB has published “Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3)” providing further guidance on when data processing activities will be considered to constitute targeting for the purposes of the application of the GDPR.

“third country” means any country outside of the European Union and EEA.

“third country data transfer(s)” refers to data transfers of personal data outside of the EU or to an international organisation (GDPR Arts. 45, 46(1), 49).

“third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (GDPR Art. 4(10) GDPR).

ANNEX 2

Data Protection Practice Tips

Before the Arbitration

1. Applicability – Arbitral Participants (defined to include the parties, counsel, arbitrators and the arbitral institution) should consider at the outset of the arbitration (or prior to issuing proceedings in the case of parties and their legal counsel) what data protection laws will apply during the arbitration, keeping in mind that data protection laws are mandatory and apply alongside the applicable arbitration law, arbitration rules, and any soft law such as the IBA Rules, to both commercial and investor-State arbitration.

2. Proportionality – Data protection laws should be applied in a proportionate manner, taking into consideration the rights and interests of the data subject (considering, for example, the nature and amount of data being processed and the circumstances), the rights and interests of third parties, including the parties to the arbitration and the need for fair and efficient administration of justice, provided that the rights and interests of the data subject must always be adequately protected.

3. Data Collection and Review – When preparing for a case, parties and their legal counsel should identify and document: (1) the types of personal data, sensitive data, personal data of children and any personal data related to criminal proceedings that is likely to be processed; (2) the lawful basis for processing that data for the arbitration; (3) what data transfers will likely need to be made and the lawful basis for them; (4) what notices have been or will need to be given to the data subjects; (5) what adequate security measures will be put in place to protect the data; and (6) any steps to be taken to minimise the processing of personal data (including any use of online case management tools to assist in that process, *e.g.*, by limiting data collection to specific custodians, data ranges or applying search terms, redaction, pseudonymisation, etc.).

4. Service Providers – When engaging third parties to assist with an arbitration (experts, transcribers, translators, online case management platform providers, remote hearing platform providers etc.), Arbitral Participants should consider what is required to comply with data protection laws in those relationships, including whether a data processing agreement is necessary.

5. Arbitrator Selection – How an arbitrator’s appointment will impact the application of data protection laws to the arbitration should be considered and steps taken

to ensure that personal data may be processed by and transferred to the arbitrator in accordance with any applicable data protection law, including the possibility of entering into standard contractual clauses for data transfers, where necessary.

During the Arbitration

6. Initial Case Management Conference (CMC) – Data protection issues should be put on the agenda and addressed at the initial CMC.

7. Data Protection Directions – In order to facilitate compliance with data protection laws and the orderly conduct of proceedings, the following data protection issues should be considered for inclusion in the first procedural order, terms of reference, or, where appropriate, in a data protection protocol (referred to as “Data Protection Directions”): (1) lawful basis for processing; (2) lawful basis for data transfer; (3) disclosure or production of documents; (4) data security and data breach protocols; (5) managing data subject rights; (6) notification; (7) documenting data protection compliance; and (8) any use of online case management platforms to assist with compliance. This is not an exhaustive list, and some of these issues may be more important than others in specific cases. However, these are issues which if not addressed early can create problems down the road either from a compliance or case management perspective.

8. During the Proceedings – Three important data protection issues that may arise in the course of the proceedings are: (1) data protection in document disclosure; (2) potential data breaches; and (3) possible data subject rights requests.

- **Document Disclosure** – Data protection laws may impact the means and amount of data to be processed and transferred to third countries for purposes of disclosure. In addition to having a lawful basis for processing and transfer, data minimisation obligations may require the culling of the documents to be produced, and/or redacting or pseudonymising personal data prior to disclosure, and otherwise limiting the personal data produced to that which is necessary for the resolution of the dispute in line with the applicable lawful basis for processing.
- **Data Breach Notification** – Given the short deadlines for data breach notification, Arbitral Participants should document in advance what will constitute a data breach, the procedure within the arbitration that will be followed if a breach occurs, who will be notified, and that they will communicate and cooperate with respect to notification. In any case, Arbitral Participants

should inform each other whenever a data breach occurs impacting arbitral data so that they can comply with any notification requirements.

- **Data Subject Rights** – Arbitral Participants should set out in advance the mechanisms that will be used to address compliance with data subject rights, including data subject access requests.

9. Award. Before the award is rendered, Arbitral Participants should consider the extent to which personal data should be included in the award and steps that might be taken to minimise the inclusion of personal data in the award and to ensure its confidentiality where applicable.

After the Arbitration

10. Data Retention – Arbitral Participants should consider how long to retain personal data connected with proceedings and the time after which such personal data and/or the documents containing it should be destroyed or permanently deleted.

ANNEX 3

Checklist: Data Protection Considerations

Introductory Remarks

This checklist contains a non-exhaustive list of data protection considerations that may impact Arbitral Participants when the GDPR or another EU-style data protection law applies.

Caution: Use of this checklist does not ensure compliance with any data protection law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Where an EU-style data protection law applies, careful consideration should be given to these issues during the proceedings and when considering Data Protection Directions. Not all of these issues arise in every arbitration and in some cases data protection issues will be raised that are not listed.

<i>General Considerations</i>
<i>Are you covered by the GDPR?</i>
<i>Establishment</i> – Consider whether you are established in the EU through stable arrangements. – Does the data processing in question occur “in the context of the activities” of that EU establishment? – If so, subject to certain exceptions (<i>e.g.</i>, household information), all world-wide data processing activities associated with the activities of that EU establishment are covered by the GDPR.
<i>Targeting</i> – If you decide you are not established in the EU, consider whether you have targeted EU data subjects for the purposes of offering services. – If so, your data processing related to the offering of those services may be covered, but not necessarily your activities generally.
<i>Am I data controller, processor or joint controller?</i>
– Do you decide the purpose and means of the processing?

- If so, then you are a data controller responsible for compliance and being able to demonstrate compliance with the GDPR. Such control is generally inherent in the function of institutions, arbitrators, and legal counsel.
- Consider whether you jointly control the purpose and means of the processing with others involved in the arbitration, in which case you may be a joint controller together with the others with whom you exercise such joint control. **Caution:** joint control has been broadly defined and carries joint and several liability.
- If you process personal data but do not control the purpose and means of the data processing, then you are likely to be a data processor, for which you would require a GDPR-compliant data processing agreement with the data controller that has engaged you for the processing. This may be the case, for example, for online case management or hearing platforms, e-discovery firms, transcribers, and interpretation and translation services in certain contexts.

Preparing for a Case

Document Collection and Review: General

- Is any likely Arbitral Participant subject to a data protection law or regulation that may impact the arbitration?
- Does the arbitration agreement expressly address data protection or data security?
- Have any of the likely Arbitral Participants issued data privacy notices that may provide information about their status under data protection law or how they will treat data protection issues? What do they say?
- What kind of personal data is likely to be processed during the arbitration?
- Does it include sensitive data? Data related to a child? Criminal offence data?
- What is the lawful basis for processing the personal data in each of these categories?
- Where is the personal data in each of these categories likely to be located?
- Does the data collection and review require third country data transfer, and, if so, what is the lawful basis for the transfer? Consider mapping the data flows and putting in place standard contractual clauses.
- How will the personal data be collected and by whom?
- Is the amount of data being collected fair and proportionate to the claim?
- How has notice been provided to the data subjects identified in the data to be processed for the arbitration:

- If notice has been provided, does it address the use of personal data for arbitration or dispute resolution?
- If not, is data processing for the arbitration compatible with the purpose that was notified?
- Is it necessary to send a further data privacy notice informing the individual data subjects that their personal data is being collected for use in a potential arbitration? Could this be done together with any arbitration hold that may be issued?
- What impact would specific notification have on any confidentiality of the proceedings (that may have yet to be brought)?
- Have efforts been made to minimise the amount of data collected and reviewed? Has the data been culled? Has consideration been given to redacting or pseudonymising the personal data or sensitive data?
- Are adequate record-keeping measures in place to demonstrate compliance with data protection laws and regulations during the collection and review of data?
- What data retention and destruction policy is in place?
- Have you considered using an online case management platform to assist with data protection compliance, among other things?

What is my lawful basis for processing personal data?

- Consider the lawful basis for your processing of personal data.
- Consider whether the processing of data is necessary for the legitimate interests (of you or other Arbitral Participants), provided that the legitimate interest is not overridden by the rights and freedoms of the data subject.
- When relying on legitimate interests, consider undertaking a Legitimate Interests Assessment (see [Annex 5](#)).

Is consent a reliable lawful basis for processing personal data?

- Relying on consent creates uncertainty.
- Consent must be obtained from each data subject, not from the parties. Employee consent is often considered to be invalid.
- Consent may be refused or withdrawn at any time, in which case it may be difficult to rely upon another lawful basis for continued processing of the personal data. Consent is therefore not recommended as a lawful basis in the arbitration context and is only appropriate in limited circumstances, including in countries with consent-based data protection laws (like Canada under PIPEDA).

What is my lawful basis for processing special category data or personal data of a child?

- Consider your lawful basis for the processing of any special category data or personal data relating to a child.
- Is the processing of any special category data necessary to establish, exercise or defend a legal claim?

Can I process any criminal offence data?

- Consider whether you can process criminal offence data, which must be done under a supervising authority's control or as authorised by EU or Member State law.
- Member State law may allow the processing of personal data relating to criminal activity, for example, Member State law may allow processing where necessary to establish, exercise or defend a legal claim, including in arbitration.

What is my lawful basis for transferring any data outside the EU?

- Consider whether data will be transferred to third countries or international organisations.
- What is your lawful basis for the transfer of any personal data?
- Transfer is lawful to countries or international organisations: (1) where a country has been granted an adequacy decision; (2) if this is not the case, where appropriate safeguards (e.g., standard contractual clauses) have been put in place; (3) if this is not feasible, a derogation can be relied upon, including where data transfers are necessary to establish, exercise or defend legal claims, provided that the personal data transfers are occasional and the personal data is minimised through culling and/or pseudonymisation/redaction, as appropriate; or (4) “compelling legitimate interests” support the transfer, which is a high threshold to meet, and also requires notification to both the data subjects and the supervisory authority.
- Standard contractual clauses should be put in place where this is feasible to do.
- Is any relevant data located in a country with a localisation regime (possibly Russia or China)? How will this be managed?

<i>Arbitration agreement and arbitrator selection</i>
– In reviewing potential legal counsel and/or arbitrator candidates, has consideration been given to how their appointment will impact the data protection profile of the arbitration? If located outside the EU, are they willing to enter into standard contractual clauses?
<i>During the Arbitration</i>
<i>Case Management Conference</i>
– Has data protection/data security been placed on the agenda for the initial procedural/case management conference?
<i>Data Protection Directions</i>
– Should data protection be addressed in the terms of reference, a procedural order, or by agreement of the parties in a data protection protocol?
<i>Issues for potential inclusion in the Data Protection Directions</i>
<i>Lawful basis</i>
– Identify the lawful basis for the processing during the arbitration process of any: (1) personal data; (2) sensitive data; (3) criminal offence data; or (4) personal data of a child.
<i>Third country transfer</i>
– Identify the lawful basis for the transfer of any: (1) personal data; (2) sensitive data; (3) criminal offence data; or (4) personal data of a child.
<i>Document production</i>
– Has consideration been give to how data protection compliance may impact document production? – Have standard contractual clauses been put in place for any third country data transfers? – What efforts will be taken to minimise the personal and sensitive data processed for the arbitration?

– Has consideration been given to the possibility of redaction and pseudonymisation of personal data, where necessary under the applicable data protection law?
<i>Data security and data breach</i>
<i>Information security</i> – Have reasonable measures been put in place to protect the security of the information, including personal and sensitive data, to be processed in relation to the arbitration? – Has consideration been given to the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration? – Taking into consideration the existing information security practices of the Arbitral Participants, has consideration been given to agreeing in advance whether any additional information security measures may be required for the arbitration? <i>Data breach</i> – Has consideration been given to what constitutes a data breach? – Have Arbitral Participants put a process in place for complying with their notification obligations if there is a data breach, taking into account the very short deadlines established in the GDPR and many other data protection laws for informing the relevant supervisory authority and/or data subjects of the data breach and the need for communication and cooperation among Arbitral Participants when notifying (<i>see</i> Cybersecurity Protocol, Schedule D-1)?
<i>Data subject rights requests</i>
– Have the Arbitral Participants identified what steps will be undertaken and who will be responsible for taking them if a data subject exercises their data subject rights, including data subject access requests, during the arbitration?
<i>Notices</i>
– Have data subjects been adequately notified of the personal data processing for the arbitration?

THE ICCA REPORTS

Record-keeping

- Have the Arbitral Participants put record-keeping measures in place to demonstrate compliance with the relevant data protection laws and regulations in a manner that can be shared with the data protection authorities if needed?

Use of on-line case management platforms

- Has consideration been given to the use of case management platforms as a means of facilitating data protection compliance during the arbitration, among other potential benefits?

ANNEX 4

Checklist: Online Case Management Platform

Introductory Remarks

Use of an Online Case Management Platform can assist Arbitral Participants to comply with their data protection and cybersecurity obligations, although it is important to recall that the use of the Platform itself constitutes data processing and must comply with applicable data protection laws. In the event that Arbitral Participants decide to use a platform, the checklist below may assist in discussions with a platform provider about compliance with data protection and cybersecurity requirements applicable to their particular arbitration.

Caution: Use of this checklist does not ensure compliance with any data protection law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. This checklist is not exhaustive of the questions that should be asked of a platform provider. Rather, it should only be considered a starting point for discussions about relevant data flows and data security arrangements. For further information on the questions to ask and practical steps to take before implementing online case management software in your arbitration, please refer to the Protocol for Online Case Management in International Arbitration.¹

Platform Providers

Data Security

- Accountability for data security
 - Identify who has responsibility for the information security policy and when this was last updated.
 - Identify who manages and controls the operation of the platform and the physical security of the facilities in which the data is stored?
 - Determine if the platform relies on any external information systems or providers and their data access rights.
 - Identify who is responsible for managing system encryption. Determine if Arbitral Participants have (or want) the option to manage their own encryption keys.

1. <https://protocol.techinarbitration.com/p/1>.

- Ensure that the platform provider's staff are vetted, trained and monitored to ensure compliance with non-disclosure or confidentiality requirements.
 - Identify the platform provider's data protection officer with responsibility for the tasks foreseen in GDPR and other relevant data protection laws. If located within the United Kingdom, for example, procure ICO data protection registration number and details or similar information for other jurisdictions.
- Standards the platform must meet
 - Enquire into the information security or quality standards in relation to the services to be provided, *e.g.*, ISO 27001, ISO 27017, ISO 27018.
 - Enquire into applicable certifications for data storage, *e.g.*, SSAE 16, SOC 2, SOC 3.
 - Legal aspects of the relationship with the platform provider
 - Review which information security legislation and regulatory policies have been considered in the design and operation of the platform.
 - Does the platform provider have a fully executed non-disclosure agreement for the engagement?
 - Review the platform provider's privacy policy.
 - If the platform provider develops any aspect of the platform, what is the system development lifecycle in place to support this process?
 - If the platform provider develops any mobile elements for the platform, how does it ensure this technology is appropriately secured?
 - Contingency plans
 - What is the platform provider's business continuity plan? What are the results of its last business continuity test?
 - How does the platform provider protect against data leakage to ensure the continuous protection of data?
 - How does the platform provider ensure the integrity of data?
 - What is the platform provider's risk tolerance in the areas of threat and vulnerability remediation? What types of threats would it consider acceptable and what time frames does it target for remediation of those that are not acceptable?
 - How is the platform and data backed up (including frequency and the technologies in use)? How are these backups tested for recovery?

Data Storage

- Encryption and security controls
 - Is data on the platform encrypted, both in transit and at rest?
 - What are the physical security controls protecting the location where platform data would be stored (*e.g.*, physical entry arrangements - locked server cages, guarded access, video monitoring, visitor access controls etc.)?
- Jurisdictional concerns
 - What is/are the jurisdiction(s) in which data on the platform can be stored?
 - Does the platform provider have the ability to replicate and back up content in more than one jurisdiction, if needed?
 - Are there any bases on which the platform provider would seek to:
 - move or replicate data outside of the chosen region(s) without express consent from all relevant Arbitral Participants?
 - access, disclose or use platform data for any purpose beyond the services commissioned for this arbitration?

Data Privacy

- Access to data
 - Identify the employees or contractors in the platform provider who would be able to access platform data and the approval process for granting access.
 - What is the level of security applicable to remote access?
 - How would the platform provider respond to data subject access requests under applicable data protection laws?

Data Retention

- Do parties have the ability to delete permanently all or part of the information uploaded to the platform, including the ability to make permanent (*i.e.*, irreversible) redactions to documents?
- What is the platform provider's proposed retention period for platform data?
- Determine how data is destroyed when necessary.

ANNEX 5

Checklist: Legitimate Interests Assessment

Introductory Remarks

When the GDPR or another data protection law applies to an Arbitral Participant, the Arbitral Participant will be required to have a lawful basis for processing personal data during the arbitration.

When the GDPR applies, the preferred lawful basis will often be the legitimate interests of either the data controller, or a third party, or both (*see* Roadmap [Section II.B.3.c\(1\)](#)). When legitimate interests are employed as the lawful basis, the EU Working Party has taken the view that a Legitimate Interests Assessment should be performed.

This checklist contains a non-exhaustive list of considerations that should be applied in performing a Legitimate Interests Assessment.

Caution: Use of this checklist does not ensure compliance with the GDPR or any other law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Where an EU-style data protection law applies, careful consideration should be given to the lawful basis for the processing of personal data for the arbitration.

Am I relying on a legitimate interest for the processing of personal data for the arbitration?

- Controllers must have a lawful basis for processing personal data, which are set out in Article 6(1) of the GDPR.
- Among other reasons, data processing is lawful where the processing is necessary for the legitimate interests of the controller or a third party, unless these interests are overridden by the individual's interests or fundamental rights. This lawful basis may be best suited for arbitration.
- The EDPB has indicated that when relying on legitimate interests, a Legitimate Interests Assessment should be undertaken and documented.

What is the three-part test for applying a legitimate interest for the processing of personal data for the arbitration?

The EU Working Party has explained that there is a three-part test that should be applied when undertaking a Legitimate Interests Assessment:

- Identify the legitimate interest
- Carry out a “necessity test”
- Carry out a “balancing test”

What is my or a third party’s legitimate interest?

The first step in a Legitimate Interests Assessment is to identify a legitimate interest – what is the purpose for processing the personal data and why is it important to you as a controller? In the context of an arbitration, the legitimate interest may involve the administration of justice, ensuring the parties’ rights are respected and the expeditious and fair resolution of claims under the applicable arbitration rules, in addition to other interests.

The “necessity test”: Is the processing necessary to achieve my or a third party’s legitimate interests?

This prong of the test asks whether the processing of the personal data is necessary to achieve a party’s legitimate interest. In applying this standard, Arbitral Participants might consider whether data minimisation techniques could be used to reduce the amount of personal data processed without infringing on all parties’ rights to present and defend their respective cases.

The “balancing test”: Have I balanced the interests?

The third prong of the test requires balancing the legitimate interest of the controller or a third party against those of the data subject and considering whether the legitimate interests of the data controller or a third party are overridden by those of the data subject. The balancing test should always be conducted fairly and must give due regard and weight to the rights and freedoms of individuals. Some factors to consider when deciding whether an individual’s rights would override a controller’s legitimate interest are:

- The nature of the data subject’s interests;
- The potential impact of processing on the data subject’s interests; and
- Any safeguards which are, or could be put, in place.

Have I documented the Legitimate Interests Assessment?

The EU Working Party has explained that the Legitimate Interests Assessment should be documented and if an issue arises, a supervisory authority is likely to review the documentation. This should therefore be done in a manner that can be disclosed on request.

ANNEX 6

Sample Standard Contractual Clauses for Controller-Controller Transfers under the GDPR

Introductory Remarks

Third country transfers by Arbitral Participants subject to the GDPR require a lawful basis. When the transfer involves a country that has not been granted an adequacy decision by the EU Commission, an “appropriate safeguard” should be put in place where feasible. In the case of arbitration, the most appropriate safeguard will likely be the “standard contractual clauses” (SCCs), which are the subject of this Annex. If entering into SCCs is not feasible, a specific derogation related to legal claims may be relied on if the conditions for doing so are considered to be met. However, the EDPB has indicated that where an appropriate safeguard can be put in place, it should be, rather than relying on a derogation.

The substantive obligations included in the SCCs impose a lightweight form of the GDPR on the data importer (i.e., the recipient of the personal data), supported by third party rights for data subjects. The precise obligations vary depending on the status of the parties to the transfer. After the CJEU decision of 2020 in *Schrems II* (Case C311/18), the European Commission put in place new, and stricter, SCCs reflecting the Court’s decision and the requirements of the GDPR. The SCCs follow a modular approach, containing a set of provisions allowing draft transfers from:

- Controller to controller (Module 1);
- Controller to processor (Module 2);
- Processor to sub-processor (Module 3); and
- Processor to controller (Module 4).

The SCCs operate on a multi-party basis, allowing a single set of SCCs to cover transfers of personal data between a number of parties. Moreover, they include a “docking clause” allowing new parties to be added over time. This will be useful in an arbitration context.

As discussed in the Roadmap, Arbitral Participants will usually be data controllers, therefore Module 1 (controller-controller transfers) will apply. This Annex therefore provides a compiled version of the SCCs for controller-controller transfers, which includes the following obligations:

- *Transfer impact assessment*: The parties to SCCs must assess and document the impact of the transfers before they are entered into.

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

- *Purpose limitation*: The data importer can only use personal data for the purposes described in the SCCs, unless the processing is necessary for legal claims, which will usually be the case in arbitration.
- *Transparency*: The data importer must, directly or via the data exporter (*i.e.*, the sender), provide data subjects with certain information, including its identity and any onward transfers.
- *Other principles*: The data importer must comply with the principles of accuracy, data minimisation and limited data retention.
- *Security*: The data importer must keep the personal data secure. If there is a breach, it may need to notify the data exporter, data subjects and the supervisory authority(ies), depending on the severity of the breach.
- *Onward transfer*: There are specific controls on onward transfers to third parties outside the EU (including a third party signing up to the SCCs), unless certain conditions are met.
- *Data subject rights*: The data importer must comply with data subject rights, including data subject access rights, and rights to correct, object to processing and erase personal data where applicable.
- *Complaints mechanism*: The data importer must provide a complaints handling process for data subjects.
- *Submission to jurisdiction*: The data importer must submit to EU jurisdiction. This includes submitting to the jurisdiction of the relevant supervisory authority(ies) and the courts in which the data subjects have their residence. Data subjects will be entitled to material and non-material damages and the data exporter and the data importer will be jointly and severally liable.
- *Access by public authorities*: Notification to the data exporter and, where possible, the data subject must be made if the personal data held by the data importer is subsequently accessed by public authorities.

Note that the Appendices of the SCCs need to be completed. The SCCs provide for choices to be made in relation to certain provisions. However, in order to be valid, the SCC terms cannot be changed. The SCCs can be included in another agreement, provided that the terms remain the same.

The following is directly excerpted from Module 1 for controller-to-controller data transfers only, of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) C/2021/3972.

Disclaimer: This document was generated based on the text available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 and is provided for convenience purposes. It should not be considered an authoritative text or legal guidance

CONTROLLER-TO-CONTROLLER STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)¹ for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in [Annex I.A](#) (hereinafter each “data exporter”), and

1. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

- (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in [Annex I.A](#) (hereinafter each “data importer”) have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in [Annex I.B](#).
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

THE ICCA REPORTS

- (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in [Annex I.B.](#)

Clause 7 – Optional **Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing [Annex I.A.](#)

- (b) Once it has completed the Appendix and signed [Annex I.A](#), the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in [Annex I.A](#).
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in [Annex I.B](#). It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
 - (i) of its identity and contact details;
 - (ii) of the categories of personal data processed;
 - (iii) of the right to obtain a copy of these Clauses;
 - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation² of the data and all back-ups at the end of the retention period.

2. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with Recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.5 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in [Annex II](#). The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to

significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union³ (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

3. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

Not applicable.

Clause 10

Data subject rights

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the

enquiry or request.⁴ The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

- (b) In particular, upon request by the data subject the data importer shall, free of charge:
 - (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in [Annex I](#); if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
 - (ii) rectify inaccurate or incomplete data concerning the data subject;
 - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
 - (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
 - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

4. That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body⁵ at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

5. The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

THE ICCA REPORTS

- (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) **[Where the data exporter is established in an EU Member State:]** The supervisory authority with responsibility for ensuring compliance by the data exporter with

Regulation (EU) 2016/679 as regards the data transfer, as indicated in [Annex I.C](#), shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in [Annex I.C](#), shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in [Annex I.C](#), shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one

of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;⁶
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

6. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to

document its best efforts in order to be able to demonstrate them on request of the data exporter.

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the

THE ICCA REPORTS

country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).

Clause 18 **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of _____ (*specify Member State*).
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIXES

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor):

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor):

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

THE ICCA REPORTS

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

[Examples of possible measures:]

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

ANNEX III – LIST OF SUB-PROCESSORS

Not applicable.

ANNEX 7

Sample Provisions for Data Protection Directions

Introductory Remarks

This language contains possible wording that could be considered for inclusion in Data Protection Directions. The wording takes into account the GDPR, and indications are given where the GDPR is referred to.

Caution: Use of this generic language does not ensure compliance with any law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Before including any language addressing data protection issues, careful consideration should be given to what is appropriate for the specific case. This generic language therefore must be modified to reflect the circumstances of the case, the procedural context, and the instrument in which it will be recorded. For example, the language will need to be modified depending on whether it is being entered into by agreement or by order.

Responsibility for Compliance

1. The Parties and their Legal Representatives shall be responsible:
 - i. To ensure that their processing of all personal data of the Arbitral Participants and other data subjects for the purpose of use in this Arbitration has been carried out in compliance with the [GDPR] and any other applicable data protection laws in so far as applicable;
 - ii. To take steps to ensure that data subjects whose personal data may be processed in this Arbitration are provided with any legally required notice unless an exemption applies; and
 - iii. To ensure that all third parties with whom they share information personal data (including sensitive/special category) obtained during the Arbitration (for example, service providers) are aware of and abide by their data protection obligations with respect to that data, including entering into a [GDPR compliant] data processing agreement where required.

Legal Basis for the Processing and Transfer of Personal Data

2. Personal data in this Arbitration is processed for the purpose of the legitimate interests of the Parties in resolving this dispute and to ensure that the arbitral process operates efficiently and expeditiously and that the rights of the Parties are

respected except where such interests are overridden by the interests or fundamental rights of the data subject.

3. In so far as any special category of personal data is processed it is because it is necessary for the establishment, exercise or defence of legal claims.
4. All Parties, Legal Representatives and arbitrators who are not based in the EEA or in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission, have agreed to enter into controller-to-controller standard contractual clauses as promulgated by the European Commission.
5. If a transfer of personal data is made to a recipient who is [**outside of the EEA**] and not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission and who has not entered into standard contractual clauses, such transfers will be occasional and made to the extent necessary for the Parties to establish, exercise or defend their legal claims.
6. If any Party or Legal Repetitive considers that processing and transfer on these bases is not appropriate, it shall notify the Tribunal forthwith.
7. The Parties and their Legal Representatives agree that they shall not do anything contrary to the principles set forth in paragraphs 2-6, including but not limited to seeking data subject consent, without first raising the issue with the Tribunal and obtaining directions.

Confidentiality [To be omitted in non-confidential arbitrations, but see footnote]¹

8. This Arbitration, including all communications between the Tribunal, Institution, and the Parties, shall be confidential.
9. The Parties have undertaken as a general principle to keep confidential all awards in the Arbitration, together with all materials in the Arbitration created for the purpose of the Arbitration and all other documents produced by another Party in the proceedings not otherwise in the public domain (the “**Arbitration Materials**”).

1. Confidentiality of the proceedings is not required by data protection laws, but the extent to which the proceedings are confidential may be considered in deciding whether the rights of the data subjects have been adequately protected.

This obligation applies save and to the extent that disclosure may be required of a Party by legal duty, to protect or pursue a legal right, or to enforce or challenge an award in legal proceedings before a state court or other legal authority (a “**Specified Disclosure Purpose**”).

10. To the extent that any Arbitral Participant needs to disclose any of the Arbitration Materials for a Specified Disclosure Purpose, such Arbitral Participant shall seek to ensure that the confidentiality of those materials is respected so far as possible under the applicable national law.

Document Disclosure

11. The Parties and their Legal Representatives agree that they shall minimise the personal data (including any sensitive/special categories of personal data) that is processed for the Arbitration including during document disclosure.
12. [Document disclosure will be pursuant to the IBA Rules to ensure focused and specific disclosure which is relevant and material to the outcome of the dispute, and documents not falling within this category shall not be processed for the Arbitration.] **[To be included where IBA Rules apply.]**
13. The Parties and their Legal Representatives will attempt to agree whether redaction or pseudonymisation is necessary and shall take such steps as are necessary to redact or otherwise remove any personal data (including any special categories of personal data) that is not relevant or necessary for the purpose of this Arbitration.
14. Parties, witnesses and data subjects who are referred to in the evidence or the pleadings in particular should be made aware by their Legal Representatives that it may be necessary to refer to their personal data (including any special categories of personal data) in an arbitral award.

Security and Cybersecurity [refer to ICCA-NYC Bar-CPR Cybersecurity Protocol for other possible measures to be considered]

15. The Parties and their Legal Representatives shall ensure that the storage and exchange of the personal data processed in this Arbitration is protected by way of appropriate technical and organisational safeguards, including through the use of secure servers and password-protected access, and taking into account the scope and risk of the processing, including 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 the extent to which it includes personal data or sensitive commercial, proprietary or confidential information. This should include, as appropriate:

- i. The pseudonymisation and encryption of personal data;
- ii. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- iii. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

16. The individuals who shall have access to such personal data shall be limited to individuals based on a need-to-know basis in connection with this Arbitration.

Personal Data Breach

17. The Arbitral Participants shall monitor the security of their electronic systems and the location of any hard or soft copies of personal data in their possession which is being or has been processed in this Arbitration.

18. Should any Arbitral Participant determine that a data breach has occurred involving the personal data processed by them in this Arbitration, they shall without undue delay, and in any case within 72 hours, notify the other Arbitral Participants including all information they are aware of concerning the data breach.

19. Each Arbitral Participant shall take appropriate steps to address and mitigate the consequences of such breach and comply with applicable legal requirements.

20. To the extent that any Arbitral Participant decides to notify the data breach to a supervisory authority or to a data subject, they shall also inform the other Arbitral Participants of the notification in advance.

21. The Parties agree that they shall inform each other, and, to the extent feasible, cooperate in relation to the notification of any data breach impacting arbitral data.

Hearings

22. With respect to hearings and conferences, whether remote or in person, the Parties and their Legal Representatives shall:

- i. Ensure that the processing of all personal data of the Arbitral Participants and other data subjects during the course of any hearing is carried out in compliance with the [GDPR] and any other applicable data protection laws, taking into account that the transmission of data during a remote hearing generally will constitute a data transfer.
- ii. Ensure that any platform used for a remote hearing complies with the security measures set forth herein, and is protected by way of appropriate technical and organisational safeguards.
- iii. Consider the impact on data protection compliance and the rights and interests of data subjects, including witnesses, of any means employed to memorialise the hearing, including the use of transcripts and recording devices.
- iv. Include measures aimed at compliance with this paragraph in any protocol, directions or agreement that are adopted for the hearing.

Data Subject Rights

23. Any Arbitral Participant who receives any request from any data subject in respect of the processing of their personal data in relation to this Arbitration, shall promptly notify the other Arbitral Participants of such request unless it is prohibited from doing so by applicable law.
24. Where the Arbitral Participant who receives the data subject request did not originally collect the personal data from the data subject, the Arbitral Participant receiving the request may (but is not obliged to) consult with the data controller who originally collected the personal data to decide how best to address the data subject request within the applicable law.
25. The Arbitral Participants agree that they shall consider such requests fairly and promptly and make any necessary alteration to that data subject's personal data promptly and notify all Parties and the Tribunal of the need to do the same.
26. The Arbitral Participants agree that they shall cooperate to ensure that data subject requests are made in good faith and minimise the impact on the Arbitration of any data subject request.

Documentation of Compliance

27. It is agreed that the Tribunal shall maintain a non-confidential version of the data protection compliance efforts in this arbitration, in a form that can be shared with third parties, including supervisory authorities. It is agreed that these data protection directions together with any other documentation of compliance efforts

shall be maintained by the Tribunal and can be shared as necessary to establish compliance.

Use of Online Case Management Platform

28. The Parties have agreed to use an online case management platform to assist with information security, data protection compliance, and document production and shall agree the parameters in advance with each other, and also with the Tribunal as appropriate.

ANNEX 8

Sample Data Protection Protocol under the GDPR

Introductory Remarks

This language contains possible wording for a Data Protection Protocol where a relevant data protection law applies to one or more Arbitral Participants. Where possible, preferred practice would be to enter into a signed Data Protection Protocol and by this means to enter into the SCCs. The main difference between the Data Protection Directions found in [Annex 7](#) and this Data Protection Protocol is that the protocol is set up as an agreement and has broader coverage. Note that where the same issue is covered by both documents, the treatment is largely the same. The wording takes into account the GDPR, and indications are given where the GDPR is referred to.

Caution: Use of this generic language does not ensure compliance with any law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Before including any language addressing data protection issues, careful consideration should be given to what is appropriate for the specific case, including a Legitimate Interest and Transfer Assessment where appropriate. This generic language therefore must be modified to reflect the circumstances of the case, the procedural context, and the instrument in which it will be recorded. For example, the language will need to be modified depending on whether it is being entered into by agreement or by order.

DATA PROTECTION PROTOCOL
<i>Introduction</i>
1. This protocol addresses data protection issues under the [General Data Protection Regulation 2016 (“GDPR”) and other data protection laws, namely relevant national law implementing and supplementing data protection including the GDPR to the extent applicable] (“Data Protection Laws”) for the purpose of this Arbitration. It is subject to review and amendment as appropriate during the course of the Arbitration. 2. The definitions and meanings used [in the GDPR] apply to this Protocol including references to the following: “data controller”; “data subject(s)”; “personal data”; “personal data breach”; “process/processing”; “processor”; and “special categories of personal data”.

3. The seat of this Arbitration is **[location]**.
4. The following individuals and entities (and their respective individual representatives), in addition to the arbitrator(s) (the “**Tribunal**”), are or are likely to be involved in the Arbitration:
 - i. The Claimant;
 - ii. The Respondent (together the “**Parties**”);
 - iii. The legal representatives of the Claimant and Respondent namely **[LAW FIRMA]** (“**Firm A**”) and **[LAW FIRM B]** (“**Firm B**”) and any **[barristers/advocates]** engaged by the Parties (together the “**Legal Representatives**”);
 - iv. The Arbitral Institution **[insert name]** (the “**Institution**”); and
 - v. (i-iv) together being the “**Arbitral Participants**.”

Responsibility for Compliance

5. The Arbitral Participants are data controllers for the purposes of the Data Protection Laws.
6. Each data controller to which **[the GDPR]** applies has a responsibility to comply with **[the provisions of the GDPR]** and to be able to demonstrate compliance. Each Arbitral Participant agrees to keep adequate records of its data protection compliance activities during the course of the Arbitration in a non-confidential form which they may, at their discretion, disclose to any competent regulatory authority after informing the other Arbitral Participants.
7. Any natural or legal person involved in the Arbitration that considers itself or others acting on its behalf to be bound by a relevant data protection law or regulation shall inform the Tribunal as soon as practicable taking into consideration the orderly conduct of the proceedings. This means that, absent unusual circumstances, general data protection issues will be raised at the case management conference if not before to the extent the Parties and their Legal Representatives are aware of them. Issues coming to light later in the proceedings may be raised at that time.
8. The Tribunal may issue binding directions applying data protection principles during the Arbitration to the extent appropriate for the efficient resolution of the dispute.
9. The Parties and their Legal Representatives shall be responsible:

- i. To ensure that their processing of all personal data of the Arbitral Participants and other data subjects for the purpose of use in this Arbitration has been carried out in compliance with the [GDPR] and any other Data Protection Laws in so far as applicable;
- ii. To take steps to ensure that data subjects (including those who are not Arbitral Participants, such as those mentioned in witness statements and evidence) whose personal data may be processed in this Arbitration are provided with any legally required notice unless an exemption applies;
- iii. To ensure that all third parties with whom they share personal data (including sensitive/special category) obtained during the Arbitration (for example, service providers) are aware of, and abide by, their data protection obligations with respect to that data, including entering into a [GDPR compliant] data processing agreement where required; and
- iv. To indemnify the Tribunal and hold the Tribunal members harmless to the full extent legally allowed from any third-party claims or regulatory proceedings arising from any breach of any applicable data protection laws during the course of, or otherwise related to, the Arbitration.

Personal Data Likely to be Processed during the Arbitration

10. The following personal data may be processed during this Arbitration:

- i. Personal identification information and biographical and contact information;
- ii. Financial information;
- iii. Information as to any legal or regulatory impediment including international sanctions;
- iv. Employment related information;
- v. Information concerning the events surrounding the facts of the arbitration; and
- vi. Other personal information such as ethnicity, family members, medical conditions (*i.e.*, sensitive or special categories of personal data).

Personal data relating to criminal convictions or offences shall not be processed or presented to the Tribunal without advance notice and permission to do so.

How and When Such Information will be Processed

11. Personal data (including sensitive or special categories of personal data) may be processed as follows:

- i. In the preparation, transmission and service of all arbitral pleadings, memorials, evidence and submissions;
- ii. In the preparation, transmission and service of any witness statement or expert report;
- iii. During the process of document production;
- iv. During the transmission of communications, in particular e-mails, between the Tribunal and the Legal Representatives and between the Parties and the Legal Representatives;
- v. In preparing and delivery of orders of the Tribunal and the preparation and delivery of any arbitral awards;
- vi. In communications with the Institution; and
- vii. To other third parties for the purpose of the smooth running of the Arbitration, such as transcribers and interpreters.

Legal Basis for the Processing and Third Country Transfer of Personal Data

12. Personal data in this Arbitration is processed for the purpose of the legitimate interests of the Parties in resolving this dispute and to ensure that the arbitral process operates efficiently and expeditiously and that the rights of the Parties are respected, except where such interests are overridden by the interests or fundamental rights of the data subject. **[The Tribunal has undertaken a Legitimate Interests Assessment.] [See [Annex 5](#)]**
13. Insofar as any special category of personal data is processed it is because it is necessary for the establishment, exercise or defence of legal claims.
14. All Parties, Legal Representatives and arbitrators who are not based in the EEA or in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission, have agreed to enter into controller-to-controller standard contractual clauses as promulgated by the European Commission in the form attached hereto **[copy of [Annex 6](#) with Annexes completed should be attached].**
15. If a transfer of personal data is made to a recipient who is **[outside of the EEA]** who is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission and who has not entered into standard contractual clauses, such transfers will be occasional, the personal data shall be minimised including redaction and/or pseudonymisation where appropriate and shall be made only to the extent necessary for the Parties to establish, exercise or defend their legal claims.

16. If any Party or Legal Representative considers that processing and transfer on these bases is not appropriate, it shall notify the Tribunal forthwith.
17. The Parties and their Legal Representatives agree that they shall not do anything contrary to the principles set forth in paragraphs 12-14, including but not limited to seeking data subject consent, without first raising the issue with the Tribunal and obtaining directions.

Confidentiality [To be omitted in non-confidential arbitrations, but see footnote]¹

18. This Arbitration, including all communications between the Tribunal, Institution, and the Parties, shall be confidential.
19. The Parties have undertaken as a general principle to keep confidential all awards in the Arbitration, together with all materials in the Arbitration created for the purpose of the Arbitration and all other documents produced by another Party in the proceedings not otherwise in the public domain (the “**Arbitration Materials**”). This obligation applies save and to the extent that disclosure may be required of a Party by legal duty, to protect or pursue a legal right, or to enforce or challenge an award in legal proceedings before a state court or other legal authority (a “**Specified Disclosure Purpose**”).
20. To the extent that any Arbitral Participant needs to disclose any of the Arbitration Materials for a Specified Disclosure Purpose, such Arbitral Participant shall seek to ensure that the confidentiality of those materials is respected so far as possible under the applicable national law.

Document Production

21. The Parties and their Legal Representatives agree that they shall minimise the personal data (including any sensitive/special categories of personal data) that is processed for the Arbitration including during document disclosure.
22. [Document production will be pursuant to the IBA Rules to ensure focused and specific disclosure which is relevant and material to the outcome of the dispute,

1. Confidentiality of the proceedings is not required by data protection laws, but the extent to which the proceedings are confidential may be considered in deciding whether the rights of the data subjects have been adequately protected.

and documents not falling within this category shall not be processed for the Arbitration.] **[To be included where IBA Rules apply.]**

23. The Parties and their Legal Representatives will attempt to agree whether redaction or pseudonymisation is necessary and shall take such steps as are necessary to redact or otherwise remove any personal data (including any special categories of personal data) that is not relevant or necessary for the purpose of this Arbitration.
24. Parties, witnesses and data subjects who are referred to in the evidence or the pleadings in particular should be made aware by their Legal Representatives that it may be necessary to refer to their personal data (including any special categories of personal data) in an arbitral award.

Security and Cybersecurity [refer to ICCA-NYC Bar-CPR Cybersecurity Protocol for other possible measures to be considered]

25. The Parties and their Legal Representatives shall ensure that the storage and exchange of the personal data processed in this Arbitration is protected by way of appropriate technical and organisational safeguards, including through the use of secure servers and password-protected access, and taking into account the scope and risk of the processing, including 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 the extent to which it includes personal data or sensitive commercial, proprietary or confidential information. This should include, as appropriate:
 - i. The pseudonymisation and encryption of personal data;
 - ii. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - iii. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
 - iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
26. The individuals who shall have access to such personal data shall be limited to individuals based on a need-to-know basis in connection with this Arbitration.

Personal Data Breach

27. The Arbitral Participants shall monitor the security of their electronic systems and the location of any hard or soft copies of personal data in their possession which is being or has been processed in this Arbitration.
28. Should any Arbitral Participant determine that a data breach has occurred involving the personal data processed by them in this Arbitration, they shall without undue delay, and in any case within 72 hours, notify the other Arbitral Participants including all information they are aware of concerning the data breach.
29. Each Arbitral Participant shall take appropriate steps to address and mitigate the consequences of such breach and comply with applicable legal requirements.
30. To the extent that any Arbitral Participant decides to notify the data breach to a supervisory authority or to a data subject, they shall also inform the other Arbitral Participants of the notification in advance.
31. The Parties agree that they shall inform each other, and to the extent feasible, cooperate in relation to the notification any data breach impacting arbitral data.

Hearings

32. With respect to hearings and conferences, whether remote or in person, the Parties and their Legal Representatives shall:
 - i. Ensure that the processing of all personal data of the Arbitral Participants and other data subjects during the course of any hearing is carried out in compliance with the [GDPR] and any other applicable data protection laws, taking into account that the transmission of data during a remote hearing generally will constitute a data transfer.
 - ii. Ensure that any platform used for a remote hearing complies with the security measures set forth herein, and is protected by way of appropriate technical and organisational safeguards.
 - iii. Consider the impact on data protection compliance and the rights and interests of data subjects, including witnesses, of any means employed to memorialise the hearing, including the use of transcripts and recording devices.
 - iv. Include measures aimed at compliance with this paragraph in any protocol, directions or agreement that are adopted for the hearing.

Data Subject Rights

33. Any Arbitral Participant who receives any request from any data subject in respect of the processing of their personal data in relation to this Arbitration, shall promptly notify the other Arbitral Participants of such request unless it is prohibited from doing so by applicable law.
34. Where the Arbitral Participant who receives the data subject request did not originally collect the personal data from the data subject, the Arbitral Participant receiving the request may (but is not obliged to) consult with the data controller who originally collected the personal data to decide how best to address the data subject request within the applicable law.
35. The Arbitral Participants agree that they shall consider such requests fairly and promptly and make any necessary alteration to that data subject's personal data promptly and notify all Parties and the Tribunal of the need to do the same.
36. The Arbitral Participants agree that they shall cooperate to ensure that data subject requests are made in good faith and minimise the impact on the Arbitration of any data subject request.

Documentation of Compliance

37. It is agreed that the Tribunal shall maintain a non-confidential version of the data protection compliance efforts in this arbitration, in a form that can be shared with third parties, including supervisory authorities. It is agreed that this data protection protocol together with any other documentation of compliance efforts shall be maintained by the Tribunal and can be shared as necessary to establish compliance.

Use of Online Case Management Platform

38. The Parties have agreed to use an online case management platform to assist with information security, data protection compliance, and document production and shall agree the parameters in advance with each other, and also with the Tribunal as appropriate.

ANNEX 9

Sample Privacy Notices

Introductory Remarks

Arbitral Participants covered by the GDPR or another EU-style data protection law should consider whether to issue a Data Privacy Notice in relation to their arbitration-related activities, and if so, the content of that notice, taking into account that their data processing practices must reflect the notice given.

We have prepared sample Data Privacy Notices below. They are based on the GDPR, although most data protection laws require similar notices.

The language suggestions below are tailored for arbitration-related activities only. Arbitral Participants should consider either issuing a separate privacy notice addressing any other data processing activities they are engaged in (for example, marketing), or modifying the sample notice to include all activities.

Caution: Use of these notices does not ensure compliance with any law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Where an EU-style data protection law applies, careful consideration should be given to whether a Data Privacy Notice is required and if so, its content. The Sample Notices are not intended to be exhaustive and Arbitral Participants must assess and reflect their specific data processing activities. Where applicable, these considerations will impact each Arbitral Participant.

ANNEX 9A
Data Privacy Notice for Arbitral Institutions¹

SAMPLE ONLY

SAMPLE DATA PRIVACY NOTICE FOR ARBITRAL INSTITUTIONS	
Last Updated: [●]	
Purpose of this Privacy Notice	
The [Name of Institution] (“[Name of Institution]” “we” or “us”) performs dispute resolution services and carries out other activities in relation to disputes or potential disputes, both during their pendency and after their conclusion, including under the [Name of Institution] Arbitration Rules (and the [Name of Institution] Mediation Rules) (“[Name of Institution] Proceedings” or “Proceedings”). This Privacy Notice describes how [Name of Institution] collects and processes personal data in the context of those services and activities. This Privacy Notice is not intended to override any other privacy-related orders or notices that may be issued in the context of [Name of Institution] Proceedings or that we may provide you in specific circumstances. Our privacy notice for all other activities that do not relate to [Name of Institution] Proceedings can be found here. [Link] [Name of Institution] Proceedings may finally determine the rights and interests of persons (both individuals and legal entities) and must therefore be undertaken fairly and impartially. While the [Name of Institution] does not determine the outcome of disputes itself, we play an important role in ensuring that justice is administered in [Name of Institution] Proceedings, and that the parties’ fundamental rights to due process, equal treatment and to present their case and to be heard are protected.	

1. In the case of arbitrations administered by an international organisation, determining whether any relevant privileges and immunities will impact the application of data protection laws turns on the breadth and scope of the relevant privileges and immunities, as well as the language of the relevant data protection law, both in terms of whether data protection laws would come within their scope, and, if so, which Arbitral Participants would be covered by them. This is an institution-specific and arbitration-specific enquiry, which goes beyond the scope of this Roadmap.

The conduct of **[Name of Institution]** Proceedings requires that personal data is processed that relates to arbitrators, mediators, adjudicators, experts and others acting or potentially acting in similar roles (“**Neutrals**”), as well as tribunal secretaries, members of the **[Name of Institution]** Court, parties, their authorised representatives and legal counsel, witnesses and all other individuals that may be identified or identifiable in any information that is processed by the **[Name of Institution]** in the context of the **[Name of Institution]** Proceedings.

The **[Name of Institution]** acts as a controller of personal data for some of its activities in the context of **[Name of Institution]** Proceedings. You should be aware that others may also act as data controllers during **[Name of Institution]** Proceedings, for example, the parties, their authorised representative or legal counsel and Neutrals. The **[Name of Institution]** is the responsible entity for the data processing activities that it undertakes as an institution, but not for the activities undertaken by other data controllers in the context of **[Name of Institution]** Proceedings. Their activities are not the subject of this Privacy Notice.

Please note that when, in the context of **[Name of Institution]** Proceedings, you provide any personal data relating to an individual with whom we or the person to whom the personal data is submitted have no direct relationship, it is your duty to provide the individual data subject with adequate notice that their data is being processed for this purpose and to comply with your other applicable data protection obligations.

This Privacy Notice is in effect as of the date indicated at the end of this Privacy Notice. A footer to this Privacy Notice will be placed on all communications during **[Name of Institution]** Proceedings. If we make material changes to this Privacy Notice, we will indicate this in the footer and update this Privacy Notice on our website with a changed date at: **[Link]**.

If you have any questions about this Privacy Notice, or how we treat your personal data in the context of **[Name of Institution]** Proceedings, or if you wish to exercise any of your data subject rights, please refer to the details found at the end of this Privacy Notice.

What personal data do we collect and how do we collect it?

Depending on the circumstances, we may obtain the following personal data about you:

*Neutrals/Tribunal Secretaries/Members of the **[Name of Institution]** Court*

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and

other personal data submitted to us by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the **[Name of Institution]** Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with **[Name of Institution]** Proceedings;

- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Individual Parties/Party's Authorised Representatives/Legal Counsel

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to us by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the **[Name of Institution]** Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with **[Name of Institution]** Proceedings;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Fact and Expert Witnesses

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to us by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the **[Name of Institution]** Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with **[Name of Institution]** Proceedings;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment;
- Personal data you choose to include in your witness statement or expert report and any oral testimony you may give (which may be transcribed), as submitted to us during **[Name of Institution]** Proceedings in which you provide written or oral evidence;
- Any other personal data of yours submitted to us by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the **[Name of Institution]** Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with **[Name of Institution]** Proceedings in which you provide written or oral evidence.

Other Individuals

- Personal data of yours submitted to us by a party, a party’s authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the **[Name of Institution]** Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with **[Name of Institution]** Proceedings.

How do we use your personal information and on what legal basis?

Depending on the circumstances in which we process your personal data, we may use your personal data in the following ways and on the legal bases described below:

*Neutrals/Tribunal Secretaries/Members of the **[Name of Institution]** Court*

- To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in **[Name of Institution]** Proceedings, as necessary to further our and the parties’ legitimate interests² in ensuring that only suitable candidates are appointed and that conflicts of interest do not arise that could undermine the actual or perceived integrity of **[Name of Institution]** Proceedings;
- To maintain a database of potential Neutrals and tribunal secretaries as necessary to further our and potential parties’ legitimate interests in identifying and appointing suitable Neutrals and tribunal secretaries;
- To decide and potentially publish **[to be completed where the institution publishes arbitration-related materials]**;
- To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of **[Name of Institution]** Proceedings, as necessary for the performance of our agreements with you and duties under them;
- To facilitate the general conduct of **[Name of Institution]** Proceedings, including to communicate with you, facilitate communications between arbitral participants, and to fulfil other administrative tasks in relation to **[Name of Institution]** Proceedings, as necessary for furthering the parties’ legitimate interests in resolving the dispute between them, and the parties’ and the **[Name of Institution]**’s interests in ensuring that the arbitral process

2. Any time legitimate interests are relied on in the EU, consideration should be given to undertaking a documented Legitimate Interests Assessment (see [Annex 5](#)).

operates efficiently and expeditiously and that the rights of the parties are respected; – Where necessary to meet our legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering (“Legal Compliance Obligations”).
<i>Individual Parties/Party’s Authorised Representative and Legal Counsel</i>
– To provide services in relation to [Name of Institution] Proceedings (including remitting funds) and to communicate with you in your capacity as a party to [Name of Institution] Proceedings or an authorised representative or legal counsel of a party, as necessary for furthering the parties’ legitimate interests in resolving the dispute between them, and the parties’ and the [Name of Institution]’s interests in ensuring that the arbitral process operates efficiently and expeditiously and that the rights of the parties are respected; – Where we have entered into an agreement to provide services to you as an individual in connection with [Name of Institution] Proceedings (for example, claims brought by individuals), we may process your personal data (only) as necessary to perform our obligations and duties under that agreement; – Where necessary to meet our Legal Compliance Obligations.
<i>Expert and Fact Witnesses</i>
– To facilitate your giving of evidence in [Name of Institution] Proceedings, and the examination of such evidence, as necessary for furthering the parties’ legitimate interests in resolving the dispute between them, and the parties’ and the [Name of Institution]’s interests in ensuring that [Name of Institution] Proceedings operate efficiently and expeditiously and that the rights of the parties are respected; – Where necessary to meet our Legal Compliance Obligations.
<i>Other Individuals</i>
– As necessary for furthering the parties’ legitimate interests in resolving the dispute between them, and the parties’ and the [Name of Institution]’s interests in ensuring that [Name of Institution] Proceedings operate efficiently and expeditiously and that the rights of the parties are respected; – Where necessary to meet our Legal Compliance Obligations.

How do we share your personal information?

Depending on the circumstances in which we handle your personal data, we may share it with the following natural and legal persons, as necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the **[Name of Institution]**'s interests in ensuring that **[Name of Institution]** Proceedings operate efficiently and expeditiously and that the rights of the parties are respected or as otherwise set out below:

- **[Name of Institution]** Court members to further the administration of cases **[add other activities of the relevant Court]**;
- Other participants in **[Name of Institution]** Proceedings in which you are involved, for example professional transcribers or other service providers;
- Our service providers such as our third-party data hosting providers in order for us to provide services in connection with **[Name of Institution]** Proceedings;
- Third parties including our professional advisors, financial institutions or law enforcement agencies, where necessary to comply with our Legal Compliance Obligations, or where it is otherwise in our or a party's legitimate interests to do so.

Where do we transfer your personal data?

From time to time we transfer personal data to third countries in connection with the services we perform in relation to **[Name of Institution]** Proceedings in which you are involved, or as may otherwise become necessary in the course of our operations. We make such transfers where there is a lawful basis for doing so.³

How long do we retain your personal information?

We will only keep your personal data for as long as is reasonably necessary in the circumstances. Retention periods vary depending on the category of data, taking into

3. Where the GDPR applies, consideration should be given to the following language:
If the recipient is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the relevant regulatory body, we make such transfers in accordance with our legal obligations, for example where the standard contractual clauses or another adequacy mechanism promulgated by the European Union have been entered into, or if this is not feasible, the transfers are necessary to establish, exercise or defend legal claims in the context of **[Name of Institution]** Proceedings, or where there is another lawful basis to do so.

account legal and regulatory requirements, limitation periods for taking legal action, good practice and the lawful basis on which we process your personal data.

What rights do you have over your personal data?

Depending on the circumstances, you have a number of rights over the personal data that we process about you. These may include the right to:

- Request access to your personal data and to obtain a copy of it from us, where this would not adversely affect the rights and freedoms of others;
- Correct your personal data that we hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for us continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defence;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defence;
- Request us to stop processing your personal data when it is being processed based on your consent;
- Object to your personal data being processed if the lawful basis for processing it is either our or a third party's legitimate interests, unless there are overriding legitimate grounds for the processing;
- Require certain of your personal data to be transferred to you or a third party to the extent that the data was collected directly from you; and
- Lodge a complaint with the relevant data protection authority.

If you wish to exercise any of these rights, or if you have any questions about this notice or how we treat your personal data, you can contact us:

- By email: **[TO BE ADDED]**
- By post: **[TO BE ADDED]**

Please note that if you are an employee of, nominated or engaged by, or otherwise affiliated with a party to an **[Name of Institution]** Proceeding, we suggest that you raise your concerns with that party in the first instance before contacting the **[Name of Institution]** regarding the processing of your personal data in the context of **[Name of Institution]** Proceedings.

Date: **[dd mm year]**

ANNEX 9B

Data Privacy Notice for Arbitrators

SAMPLE ONLY

SAMPLE DATA PRIVACY NOTICE FOR ARBITRATORS	
Last Updated: [●]	
Purpose of this Privacy Notice	
[Name of Arbitrator] (“I” or “me”) acts as an arbitrator and carries out other activities in relation to disputes or potential disputes, both during the pendency of such disputes and after their conclusion (“Arbitral Proceedings”). This Privacy Notice describes how I collect and process personal data in the context of those services and activities. This Privacy Notice is not intended to override any other privacy-related orders or notices that either I or a tribunal of which I am a part may issue in the context of the Proceedings or that I may provide to you in specific circumstances. My privacy notice for all other activities that do not relate to my activities in relation to Arbitral Proceedings can be found here. [Link] Arbitral Proceedings may finally determine the rights and interests of persons (both individuals and legal entities) and must therefore be undertaken fairly and impartially, which requires me to ensure that the parties’ fundamental due process rights, rights to equal treatment and their right to present their case and to be heard are protected. My activities as an arbitrator may require me to process personal data that relates to arbitrators, mediators, adjudicators, experts and others acting or potentially acting in similar roles (“Neutrals”), as well as tribunal secretaries, employees of arbitral institutions, parties, their authorised representatives and legal counsel, witnesses and other individuals that may be identified or identifiable in any information that is processed during the Arbitral Proceedings. I act as a controller of personal data for some of my activities as an arbitrator. You should be aware that others may also act as data controllers during Arbitral Proceedings in which I act as an arbitrator, for example, the parties, their authorised	

representative or legal counsel, the arbitral institution and other Neutrals. When I act as an arbitrator, I am responsible for the data processing activities that I undertake in that function, but not for the activities undertaken by other data controllers acting in the context of Arbitral Proceedings, including other Neutrals. Their activities are not the subject of this Privacy Notice.

Please note that when, in the context of Arbitral Proceedings, you provide any personal data relating to individuals with whom I or the person to whom such data is submitted has no direct relationship, it is your duty to provide the individual data subject with adequate notice that their data is being processed for this purpose and to comply with your other applicable data protection obligations.

This Privacy Notice is in effect as of the date indicated at the end of this Privacy Notice. A link to this Privacy Notice is found under the signature line of my emails. If I make material changes to this Privacy Notice, I will update this Privacy Notice on my website with a changed date at: [[Link](#)].

If you have any questions about this Privacy Notice or how I treat your personal data in the context of Arbitral Proceedings, or if you wish to exercise any of your data subject rights, please refer to the details found at the end of this Privacy Notice.

What personal data do I collect and how do I collect it?

Depending on the circumstances, I may obtain the following personal data about you in the context of Arbitral Proceedings in which I serve as arbitrator:

Institutional Representatives

- Your name, contact details and other information you may provide to me during the appointment process or in the context of Arbitral Proceedings, including any challenge proceedings, in which I serve as an arbitrator.

Neutrals

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator;

– Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
<i>Tribunal Secretaries</i>
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party’s authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
<i>Individual Parties/Party’s Authorised Representatives and Legal Counsel</i>
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party’s authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
<i>Fact and Expert Witnesses</i>
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party’s authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment; – Personal data you choose to include in your witness statement or expert report and any oral testimony you may give (which may be transcribed), as

submitted to me during Arbitral Proceedings in which you provide written or oral evidence; – Any other personal data of yours submitted to me by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator.
<i>Other Individuals</i>
– Personal data of yours submitted to me by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context Arbitral Proceedings in which I serve as an arbitrator.
How do I use your personal information and on what legal basis?
In the context of Arbitral Proceedings in which I serve as an arbitrator, and depending on the circumstances, I may use your personal data in the following ways and on the legal bases described below:
<i>Other Neutrals and Tribunal Secretaries</i>
– To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in Arbitral Proceedings, as necessary to further the parties' and my legitimate interests⁴ in ensuring that only suitable candidates are appointed and that conflicts of interest do not arise that could undermine the actual or perceived integrity of the Arbitral Proceedings; – To maintain an informal database of potential Neutrals and tribunal secretaries as necessary to further both my and potential parties' legitimate interests in identifying and appointing suitable chair persons and tribunal secretaries; – To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of Arbitral Proceedings, as necessary for the performance of any agreement we may have entered into and my duties under them;

4. Any time legitimate interests are relied on in the EU, consideration should be given to undertaking a documented Legitimate Interests Assessment (see [Annex 5](#)).

- To facilitate the general conduct of Arbitral Proceedings, including to communicate with you, facilitate communications between the tribunal and the arbitral participants more broadly, and to fulfil other administrative tasks in relation to Arbitral Proceedings, as necessary for furthering the parties’ and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected;
- Where necessary to meet my legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering (“**Legal Compliance Obligations**”).

Individual Parties/Party’s Authorised Representatives and Legal Counsel

- To facilitate the general conduct of Arbitral Proceedings, including to communicate with you, facilitate communications between the tribunal and the arbitral participants, and to fulfil other administrative tasks in relation to Arbitral Proceedings, as necessary for furthering the parties’ and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected;
- Where we have entered into an agreement for me to provide services to you as an individual in connection with Arbitral Proceedings (for example, claims brought by individuals), I may process your personal data (only) as necessary to perform my obligations and duties under that agreement;
- Where necessary to meet my Legal Compliance Obligations.

Expert and Fact Witnesses

- To facilitate your giving of evidence in Arbitral Proceedings, and the examination of such evidence, as necessary for furthering the parties’ and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected;
- Where necessary to meet my Legal Compliance Obligations.

Other Individuals

- As necessary for furthering the parties’ and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected;
- Where necessary to meet my Legal Compliance Obligations.

How do I share your personal information?

Depending on the circumstances in which I process your personal data, I may share it with the following people as necessary for furthering the parties' and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected, or as otherwise set out below:

- Arbitral Participants and others involved in Arbitral Proceedings in which you are also involved;
- My service providers such as third-party data hosting providers in order for me to provide services in connection with Arbitral Proceedings;
- Third parties including my professional advisors, financial institutions, or law enforcement agencies, where necessary to comply with my Legal Compliance Obligations, or where it is otherwise in my or another Arbitral Participant's legitimate interests to do so.

Where do I transfer your personal data?

From time to time I transfer personal data to third countries in connection with the Arbitral Proceedings in which I serve as an arbitrator, or as may otherwise become necessary in the course of my operations. I make such transfers where there is a lawful basis for doing so.⁵

How long do I retain your personal information?

I will only keep your personal data for as long as is reasonably necessary in the circumstances. Retention periods vary depending on the category of data, taking into account legal and regulatory requirements, limitation periods for taking legal action, good practice and the lawful basis on which I process your personal data.

-
5. Where the GDPR applies, consideration should be given to the following language:
- If the recipient is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Union, such transfers are made in accordance with our legal obligations, including entering into the standard contractual clauses or another adequacy mechanism promulgated by the European Union where feasible and if this is not feasible, in accordance with a derogation, for example where the transfers are necessary to establish, exercise or defend legal claims, or where there is another lawful basis to do so.

What rights do you have over your personal data?

Depending on the circumstances, you may have a number of rights over the personal data that I process about you. These may include the right to:

- Request access to your personal data and obtain a copy of it from me, where this would not adversely affect the rights and freedoms of others;
- Correct your personal data that I hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for me continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defence;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defence;
- Request me to stop processing your personal data when it is being processed based on your consent;
- Object to your personal data being processed if the lawful basis for processing it is either my or a third party's legitimate interests unless there are overriding legitimate grounds for the processing;
- Require certain of your personal data to be transferred to you or a third party to the extent that I collected the data directly from you;
- Lodge a complaint with the relevant data protection authority.

If you wish to exercise any of these rights, or if you have any questions about this notice or how I treat your personal data, you can contact me:

- By email: **[TO BE ADDED]**
- By post: **[TO BE ADDED]**

Please note that if you are an employee of, nominated or engaged by, or otherwise affiliated with a party to an Arbitral Proceeding in which I am appointed as an arbitrator, I suggest that you raise your concerns with that party first before contacting me regarding the processing of your personal data in the context of Arbitral Proceedings.

Date: **[dd mm year]**

ANNEX 9C

Data Privacy Notice for Legal Counsel

SAMPLE ONLY

SAMPLE DATA PRIVACY NOTICE FOR LEGAL COUNSEL
Last Updated: [●]
Purpose of this Privacy Notice
[Name of Legal Counsel or the law firm] [“I”, “me,” “we” or the firm] act(s) as a legal counsel and [carry/carries] out other activities in relation to disputes or potential disputes that are submitted to arbitration and other dispute resolution mechanisms, both during their pendency and after their conclusion. (“Dispute Resolution Proceedings”) This Privacy Notice describes how [I/we/the firm] collect and process personal data in the context of those services and activities. [My/ the firm’s] General Privacy Notice can be found here. [Link] Dispute Resolution Proceedings may finally determine the rights and interests of persons (both individuals and legal entities) and must therefore be undertaken fairly and impartially, which requires that the parties’ fundamental due process rights, rights to equal treatment and their right to present their case and to be heard are protected. [My/The firm’s] activities as a legal counsel during Dispute Resolution Proceedings may require [me/us/the firm] to process personal data that relates to arbitrators, mediators, adjudicators, experts, and others acting or potentially acting in similar roles (“Neutrals”), as well as tribunal secretaries, employees of arbitral institutions, parties, their authorised and legal counsel, witnesses, and other individuals that may be identified or identifiable in any information that is processed during the Dispute Resolution Proceedings. [I/we/the firm] acts as a controller of personal data for some of [my/our] activities as legal counsel. You should be aware that others may also act as data controllers during a Dispute Resolution Proceeding, for example, the parties, their authorised representatives, other legal counsel, the arbitral institution, and Neutrals. When I act

as a legal counsel, I am responsible for the data processing activities that I undertake in that function, but not for the activities undertaken by other data controllers acting in the context of Dispute Resolution Proceedings. Their activities are not the subject of this Privacy Notice.

Please note that when, in the context of Dispute Resolution Proceedings, you provide me with any personal data relating to individuals with whom I have no direct relationship, it is your duty to provide the individual data subject with adequate notice that their data is being processed for this purpose and to comply with your other applicable data protection obligations.

This Privacy Notice is in effect as of the date indicated at the end of this Privacy Notice. A link to the Privacy Notice is found under the signature line of **[my/our/the firm's]** emails. If **[I/we]** make material changes to this Privacy Notice, **[I/we]** will update this Privacy Notice on the website with a changed date at: **[Link]**.

If you have any questions about this Privacy Notice, or how **[I/we/the firm]** treat your personal data in the context of Dispute Resolution Proceedings or wish to exercise any of your data subject rights, please refer to the details found at the end of this Privacy Notice.

What personal data do I collect and how do I collect it?

Depending on the circumstances, **[I/we/the firm]** may obtain the following personal data about you in the context of Dispute Resolution Proceedings in which **[I/we/the firm]** act as a legal counsel:

Institutional Representatives

- Your name, contact details, and other information you may provide to **[me/us/the firm]** in the context of Dispute Resolution Proceedings in which **[I/we/the firm]** act[s] as legal counsel.

Neutrals

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to **[me/us/the firm]** by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, **[me/us/the firm]** from third parties or publicly available resources

in the context of Dispute Resolution Proceedings in which [I/we/the firm] act[s] as legal counsel; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
<i>Tribunal Secretaries</i>
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [me/us/the firm] by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, a representative of the institution, or otherwise disclosed to, or collected by [me/us/the firm] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [I/we/the firm] act[s] as legal counsel; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
<i>Individual Parties/Party's Authorised and Legal Counsels</i>
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [me/us/the firm] by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [me/us/the firm] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [I/we/the firm] act as a legal counsel; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
<i>Fact and Expert Witnesses</i>
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [me/us/the firm] by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [me/us/the firm] from third parties or publicly available

resources in the context of Dispute Resolution Proceedings in which [I/we/the firm] act as a legal counsel; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment; – Personal data you choose to include in your witness statement or expert report and any oral testimony you may give (which may be transcribed), as submitted to [me/us/the firm] during Dispute Resolution Proceedings in which you provide written or oral evidence; – Any other personal data of yours submitted to [me/us/the firm] by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [me/us/the firm] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [I/we/the firm] act as a legal counsel.
<i>Other Individuals</i>
– Personal data of yours submitted to [me/us/the firm] by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [me/us/the firm] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [I/we/the firm] act as a legal counsel.
How do [I/we/the firm] use your personal information and on what legal basis?
In the context of Dispute Resolution Proceedings in which [I/we/the firm] act as a legal counsel, depending on the circumstances, [I/we/the firm] may use your personal data in the following ways and on the legal bases described below:
<i>Neutrals and Tribunal Secretaries</i>
– To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in Dispute Resolution Proceedings, as necessary for furthering [my/our/the firm's] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;⁶

6. Any time legitimate interests are relied on in the EU, relevant EU guidance suggests that consideration should be given to undertaking a documented Legitimate Interests Assessment (*see*

- To maintain an informal database of potential Neutrals and tribunal secretaries as necessary to further **[my/our/the firm’s]** and potential parties’ legitimate interests in identifying and appointing suitable Neutrals and tribunal secretaries;
- To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of Dispute Resolution Proceedings, as necessary for the performance of any agreement we may have entered into and **[my/our/the firm’s]** duties under it;
- To facilitate the general conduct of Dispute Resolution Proceedings, as necessary for furthering **[my/our/the firm’s]** and our client’s legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client’s rights are respected;
- Where necessary to meet **[my/our/the firm’s]** legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering (“**Legal Compliance Obligations**”).

Legal Counsel of Other Parties

- To facilitate the general conduct of Dispute Resolution Proceedings, as necessary for furthering **[my/our/the firm’s]** and our client’s legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client’s rights are respected;
- Where we have entered into an agreement for me to provide services to you as an individual in connection with Dispute Resolution Proceedings (for example, claims brought by individuals), **[I/we/the firm]** may process your personal data (only) as necessary to perform **[my/our/the firm’s]** obligations and duties under that agreement;
- Where necessary to meet **[my/our/the firm’s]** Legal Compliance Obligations.

Expert and Fact Witnesses

- To facilitate your giving evidence in Dispute Resolution Proceedings and the examination of such evidence, as necessary for furthering **[my/our/the firm’s]** and our client’s legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client’s rights are respected;
- Where necessary to meet **[my/our/the firm’s]** Legal Compliance Obligations.

Other Individuals

- As necessary for furthering **[my/our/the firm’s]** and our client’s legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client’s rights are respected;
- Where necessary to meet **[my/our/the firm’s]** Legal Compliance Obligations.

How do share your personal information?

Depending on the circumstances in which **[I/we/the firm]** process your personal data, **[I/we/the firm]** may share it with the following people, as necessary for furthering **[my/our/the firm’s]** and our client’s legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client’s rights are respected:

- Participants involved in Dispute Resolution Proceedings in which our client is also involved;
- **[My/Our/The firm’s]** service providers such as third-party data hosting providers in order for **[me/us/the firm]** to provide services in connection with Dispute Resolution Proceedings;
- Third parties, including my colleagues, professional advisors, financial institutions, or law enforcement agencies, where necessary to perform conflict checks, to comply with **[my/our/the firm’s]** Legal Compliance Obligations, or where it is otherwise in **[my/our/the firm’s]** or another Arbitral Participant’s or third party’s legitimate interests to do so.

Where do I transfer your personal data?

From time to time **[I/we/the firm]** transfer personal data to third countries in connection with the services **[I/we/the firm]** perform for the Dispute Resolution Proceedings in which **[I/we/the firm]** serve as a legal counsel, or as may otherwise become necessary in the course of **[my/our/the firm’s]** operations. **[I/we/the firm]** make such transfers where there is a lawful basis for doing so.⁷

7. Where the GDPR applies, consideration should consider the following language:

If the recipient is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Union, such transfers are made in accordance with our legal obligations, including entering into the standard contractual clauses or another adequacy mechanism promulgated by the European Union where feasible and if this is not feasible, in accordance with a derogation, for example where the transfers are necessary to establish, exercise or defend legal claims, or where there is another lawful basis to do so.

How long do [I/we/the firm] retain your personal information?

[I/we/the firm] will only keep your personal data for as long as is reasonably necessary in the circumstances. Retention periods vary depending on the category of data, taking into account legal and regulatory requirements, limitation periods for taking legal action, good practice and the lawful basis on which [I/we/the firm] process it.

What rights do you have over your personal data?

Depending on the circumstances, you may have a number of rights over the personal data that [I/we/the firm] process about you. These may include the right to:

- Request access to your personal data and obtain a copy of it from [me/us/the firm], where this would not adversely affect the rights and freedoms of others;
- Correct your personal data that [I/we/the firm] hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for [me/us/the firm] continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defence;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defence;
- Request [me/us/the firm] to stop processing your personal data when it is being processed based on your consent;
- Object to your personal data being processed if the lawful basis for processing it is either [my/our/the firm's] or a third party's legitimate interests unless there are overriding legitimate grounds for the processing;
- Require certain of your personal data to be transferred to you or a third party to the extent that [I/we/the firm] collected the data directly from you; and
- Lodge a complaint with the relevant data protection authority.

If you wish to exercise any of these rights, or if you have any questions about this notice or how [I/we/the firm] treat your personal data, you can contact [me/us/the firm] as follows:

- By email: [TO BE ADDED]
- By post: [TO BE ADDED]

Please note that if you are an employee of, nominated or engaged by, or otherwise affiliated with a party to an Dispute Resolution Proceeding in which [I/we/the firm]

THE ICCA REPORTS

act as a legal counsel, [**I/we/the firm**] suggest that you raise your concerns with that party first before contacting [**me/us/the firm**] regarding the processing of your personal data in the context of Dispute Resolution Proceedings.

Date: [**dd mm year**]

ANNEX 10

List of Sources by Category

Data Protection Related Materials

Application of Data Protection Directive to Discovery

1. *Working Document on Pre-trial Discovery for Cross Border Civil Litigation*, EU Working Party, 00339/09/EN WP 158, 2009 (endorsed by the EPDB) (referred to as “**Document Disclosure Guidance**”)
2. *The Sedona Conference: International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, App. D: Cross-Border Data Safeguarding Process + Transfer Protocol, Sedona Conference Working Group (2017)
3. *E-Discovery and Data Privacy: A Practical Guide*, Catrien Noorda & Stefan Hanlose eds., 2011

Consent

4. *Guidelines on Consent under Regulation 2016/679*, EU Working Party, 17/EN WP259 rev.01, as revised and adopted on 10 April 2018 (endorsed by the EPDB)

Controller versus Processor

5. *Opinion 1/2010 on the Concepts of “Controller” and “Processor”*, EU Working Party, 00264/10/EN WP 169, 2010 (“**Controller/Processor Opinion**”)

Data Breach

6. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification*, EU Working Party, Version 2.0, adopted on 14 December 2021
7. *Guidelines on Personal data breach notification under Regulation 2016/679*, endorsed by the EDPB, G29 WP250 rev.1, 6 February 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Data Processing

8. *What Constitutes Data Processing?*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [<https://perma.cc/Q85B-NJ33>] (archived 19 March 2018)

Data Transfers

9. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, EDPB, Version for Public Comment, 18 November 2021
10. *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* (Text with EEA relevance) C/2021/3972 OJ L 199, 7.6.2021, p. 31–61. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en (referred to as “**standard contractual clauses**”)
11. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, EDPB, 2018 (referred to as “**Data Transfer Guidance**”)
12. *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, EU Working Party, 2093/05/EN WP 114, 2005
13. *Adequacy of the protection of personal data in non-EU countries*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

General Materials

14. Daniel Cooper and Christopher Kuner, *Data Protection Law and International Dispute Resolution*, 32 *Recueil des cours/ Collected Courses of the Hague Academy of International Law* 9-174 (2017)
15. *Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulations as of 25 May 2018*, Communication from the Commission to the European Parliament and the Council, COM (2018) 43 (24 January 2018)
16. *Handbook on European Data Protection Law*, European Union Agency for Fundamental Rights (2018)

Joint Controller

17. Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* C210/16, EU:C:2018:388
18. Judgment of 10 July 2018, *Tietosuojavaltuutettu*, C25/17, EU:C:2018:551 Case C-25/17
19. *CJEU rules on joint controllership – what does this mean for companies?*, <https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies> (August 2018)

Legitimate Interests

20. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, EU Working Party, 844/14/EN, WP 217, 9 April 2014
21. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, EDPB, 8 October 2019

Lead Supervisory Authority

22. *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority*, EU Working Party, 16/EN WP 244 rev. 01, 2017

Personal Data

23. *What is Personal Data?*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [<https://perma.cc/CJ52-ZQVB>] (archived 31 May 2018)

Proportionality

24. *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (19 December 2019)

Risk-Based Approach

25. *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks 3*, EU Working Party, 14/EN 218 WP 169, 2014

Territorial Scope

26. *Guidelines 3/2018 on the Territorial Scope of the GDPR*, EDPB, 12 November 2019

Transparency

27. *Guidelines on Transparency under Regulation 2016/679*, EU Working Party, 17/EN WP 260, 2018

Arbitration-related Data Protection Materials

28. *Protocol for Online Case Management in International Arbitration*, Working Group on LegalTech Adoption in International Arbitration (2020) (referred to as “**Online Platform Protocol**”)
29. *Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration*, International Chamber of Commerce (1 January 2021)
30. *It’s All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, Kathleen Paisley, 41 Fordham Int’l L.J. 840 (2017)
31. *IBA Rules on the Taking of Evidence in International Arbitration* (International Bar Association, revised in 2020) (referred to as “**IBA Rules**”)
32. *Commentary on the Revised Text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration* (2020)

Cybersecurity Materials

33. *ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitration* (2022 Edition) (referred to as “**Cybersecurity Protocol**”)
34. *Cybersecurity Guidelines*, IBA Presidential Task Force on Cybersecurity (2018)
35. *A Call to Cyberarms: The International Arbitrator’s Duty to Avoid Digital Intrusion*, Stephanie Cohen and Mark Morril, 40 Fordham Int’l L.J. 981 (2017)

36. *Debevoise & Plimpton Protocol to Promote Cybersecurity in International Arbitration* https://www.debevoise.com/~media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf. (2017)

Applicable Law to Data Protection

37. *Cross-Border Application of EU's General Data Protection Regulation (GDPR)- A private international law study on third state implications*, Anni-Maria Taka (2017)
38. *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*, Jiahong Chen, *International Data Privacy Law* 6.4 (2016): 310-323.
39. *Data protection and conflict-of-laws: a challenging relationship*, Maja Brkan, *Eur. Data Prot. L. Rev.* 2 (2016): 324
40. *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, Christian Kohler, *Rivista di diritto internazionale privato e processuale* (2016): 653
41. *Protection of Privacy in Private International and Procedural Law: Interim Report and Commentary*, International Law Association Sydney Conference (2018)

ANNEX 11

Compendium of Selected Data Protection Laws

The Task Force has compiled this compendium from publicly available sources and has undertaken reasonable efforts to ensure that it is current as of the date of publication of the Roadmap. It should not be relied on without independent confirmation of the current law.

Jurisdictions with EU Adequacy Decisions				
No.	Country	Supervisory Authority	Implementing Legislation	Adequacy Decision
1	Andorra	l'Agència Andorrana de Protecció de Dades (APDA) https://www.apda.ad/	Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades (LQPD)	Commission Decision 2010/625/EU
2	Argentina	Agencia de Acceso a la Información Pública https://www.argentina.gob.ar/aaip	Ley de Protección de Datos Personales 25.326	Commission Decision 2003/490/EC
3	Canada (commercial organisations)	Office of the Privacy Commissioner of Canada ("PIPEDA") Office of the Information and Privacy Commissioner of Alberta ("PIPA Alberta") Office of the Information and Privacy Commissioner for British Columbia ("PIPA BC"), and Commission d'accès à l'information du Québec ("Quebec Privacy Act")	In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Canada's private sector privacy statutes: Personal Information Protection and Electronic Documents Act ("PIPEDA") Personal Information Protection Act ("PIPA Alberta") Personal Information Protection Act ("PIPA BC"), Personal Information Protection and Identity Theft Prevention Act ("PIPIITA") (not yet in force), and An Act Respecting the Protection of Personal Information in the Private Sector ("Quebec Privacy Act")	Commission Decision 2002/2/EC
4	Faroe Islands			Commission Decision 2010/146/EU

No.	Country	Supervisory Authority	Implementing Legislation	Adequacy Decision
5	Guernsey	Data Protection Authority Office of the Data Protection Authority	Data Protection (Bailiwick of Guernsey) Law 2017 (DPL 2017) (came into force on 25 May 2018 to coincide with the GDPR)	Commission Decision 2003/821/EC
6	Israel	The Israel Privacy Protection Authority (PPA)	Human Dignity and Liberty, 5752 – 1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the PPL); and the guidelines of the Israel Privacy Protection Authority.	Commission Decision 2011/61/EU
7	Isle of Man			Commission Decision 2004/411/EC
8	Japan	Personal Information Protection Commission	Act on the Protection of Personal Information, as amended on 30 May 2017	EU Japan Adequacy Decision, January 2019
9	Jersey	Data Protection Authority Information Commissioner	Data Protection (Jersey) Law, 2018 (DPJL) and the Data Protection Authority (Jersey) Law, 2018 (DPAJL) came into force on May 25, 2018. These laws superseded the Data Protection (Jersey) Law 2005, which had been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC). This decision continues to apply pending a review of Jersey's adequacy (to be conducted under Article 45 of the European General Data Protection Regulation (GDPR)), which is expected to take place in 2020. The DPJL and DPAJL provide a broadly equivalent regime to that under the GDPR.	Commission Decision 2008/393/EC

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

No.	Country	Supervisory Authority	Implementing Legislation	Adequacy Decision
10	New Zealand	Privacy Commissioner's Office	The Privacy Act 1993 (Act) A Privacy Amendment Bill was introduced to New Zealand's parliament in 2018	Commission Implementing Decision 2013/65/EU
11	Republic of Korea	Personal Information Protection Commission (PIPC)	Personal Information Protection Act (PIPA), as amended on 4 February 2020	Commission Implementing Decision of 17.12.2021
12	Switzerland	Federal Data Protection and Information Commissioner (FDPIC)	<i>See below (subject to a new decision on adequacy in view of regulatory changes since 2000)</i>	Commission Decision 2000/518/EC
13	Uruguay	Unidad Reguladora y de Control de Datos Personales (URCDP or Data Protection Authority) https://www.gub.uy/unidad-reguladora-control-datos-personales/	Data Protection Act Law No. 18.331 (August 11, 2008) Decree No. 414/009 (August 31, 2009)	Commission Implementing Decision 2012/484/EU
14	United Kingdom	Information Commissioner's Office https://ico.org.uk/	Data Protection Act 2018	Commission Implementing Decision of 28.6.2021

Selected Data Protection Laws of Non-EEA Jurisdictions		
	Country	Supervising Authority(ies)
1	Brazil	National Data Protection Authority (ANPD) https://www.gov.br/anpd/pt-br
		National Law(s) Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018, published on August 15, 2018. Largely aligned to the EU General Data Protection Act (GDPR)
2	Canada	Office of the Privacy Commissioner of Canada ("PIPEDA") Office of the Information and Privacy Commissioner of Alberta ("PIPA Alberta") Office of the Information and Privacy Commissioner for British Columbia ("PIPA BC"), and Commission d'accès à l'information du Québec ("Quebec Privacy Act")
		National Law(s) In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Canada's private sector privacy statutes: Personal Information Protection and Electronic Documents Act ("PIPEDA") Personal Information Protection Act ("PIPA Alberta") Personal Information Protection Act ("PIPA BC"), Personal Information Protection and Identity Theft Prevention Act ("PIPI-ITPA") (not yet in force), and An Act Respecting the Protection of Personal Information in the Private Sector ("Quebec Privacy Act")
3	China	Cyberspace Administration of China (CAC) Ministry of Public Security
		National Law(s) There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal data protection and data security are part of a complex framework and are found across various laws and regulations. PRC Cybersecurity Law came into effect on June 1, 2017 and became the first national-level law to address cybersecurity and data privacy protection. However, there remains uncertainty as to how it will be applied.
4	Hong Kong	The Office of the Privacy Commissioner for Personal Data
		National Law(s) The Personal Data (Privacy) Ordinance (Cap. 486) – in force since 1996, significantly amended in 2012/2013
5	India	[No authority]
		National Law(s) Personal Data Protection Bill 2018 – [withdrawn] Information Technology Act, 2000 India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

	Country	Supervising Authority(ies)	National Law(s)
6	Mexico	National Institute of Transparency for Access to Information and Personal Data Protection Ministry of Economy	Federal Law on the Protection of Personal Data held by Private Parties (July 6, 2010), supplemented by further regulations: The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (December 22, 2011) The Privacy Notice Guidelines (April 18, 2013) The Recommendations on Personal Data Security (November 30, 2013) The Parameters for Self-Regulation regarding personal data (May 30, 2014) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (January 27, 2017)
7	Russia	Federal Service for Supervision of Communications, Information Technologies and Mass Media (“Roscomnadzor”)	Russian Constitution establishes the right to privacy of each individual (arts. 23-24) Data Protection Act No. 152 FZ dated 27 July 2006 (DPA), amended on 22 July 2014
8	Singapore	Personal Data Protection Commission	Personal Data Protection Act No. 26 of 2012, enacted on October 15, 2012
9	Switzerland	Federal Data Protection and Information Commissioner (FDPIIC)	Federal Act on Data Protection of June 19, 1992 (DPA), together with Ordinance to the Federal Act on Data Protection (DPO) and the Ordinance on Data Protection Certification (ODPC). After substantial revision, a new Federal Act on Data Protection was adopted on September 25, 2020 and should come into force on September 1, 2023 (the new Act aims to align the DPA with the GDPR).
10	United Kingdom	Information Commissioner’s Office https://ico.org.uk/	Data Protection Act 2018
11	USA¹	No single national authority The Federal Trade Commission has authority to issue and enforce privacy regulations in specific areas	

1. The list of states with data protection frameworks is not exhaustive. We refer to a select few, deemed especially relevant in arbitration.

	Country	Supervising Authority(ies)	National Law(s)
12	California		More than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020 and the California Privacy Rights Act (CPRA) – the majority of the CPRA's provisions will enter into force on Jan. 1, 2023
13	Florida		Fl Stat § 282.318 Information Technology Security Act Fl Stat § 408.051 Florida Electronic Health Records Exchange Act Fl Stat § 501.171 Security of Confidential Personal Information
14	New York		Ny Gen. Bus. Law § 899-Aa <i>Notification; Person Without Valid Authorization Has Acquired Private Information</i> Ny Gen. Bus. Law §§ 899-Aaa – 899-Bbb <i>Document Destruction Contractors</i> Ny Gen. Bus. Law § 399-Ddd <i>Confidentiality of Social Security Account Number</i> Ny Gen. Bus. Laws § 399-Ddd*2 <i>Disclosure of Social Security Number</i> Ny Gen. Bus. Law § 399-H <i>Disposal of Records Containing Personal Identifying Information</i> 23 Nycrr 500 §§ 500.00 – 500.23 <i>Cybersecurity Requirements for Financial Services Companies</i>
15	Texas		Tx Business and Commerce Code §§ 521.001 – 521.002 <i>Identity Theft Enforcement and Protection Act</i> Tx Business and Commerce Code § 521.051 <i>Unauthorized Use or Possession of Personal Identifying Information</i> Tx Business and Commerce Code § 521.052 <i>Business Duty to Protect Sensitive Personal Information</i> Tx Business and Commerce Code § 521.053 <i>Notification Required Following Breach of Security of Computerized Data</i> Tx Business and Commerce Code § 521.151 <i>Civil Penalty; Injunction</i> Tx Business and Commerce Code §§ 72.001 – 72.004 <i>Disposal of Certain Business Records</i>

	Country	Supervising Authority(ies)	National Law(s)
16	Washington DC		D.C. Code §§ 28-3851 – 3853 Consumer Security Breach Notification D.C. Code §§ 47-3151 – 3154 Use of Consumer Identification Information D.C. Code §§ 38-831.01 – 38-831.06 Protection of Students Digital Privacy D.C. Code §§ 7-241 – 7-248 Human Health Care and Safety/Data Sharing D.C. Code § 38-607 Student Health Files
EU/EEA Member State Data Protection Laws			
	Country	Supervising Authority	Implementing Law(s)
1	Austria	Österreichische Datenschutzbehörde http://www.dsb.gv.at/	Federal Act Amending the Data Protection Act 2000 (Data Protection Adaptation Act) 2018 Federal Law 23 Federal Law 24
2	Belgium	Autorité de la protection des données/ Gegevensbeschermingsautoriteit (APD-GBA) https://www.autoriteprotectiondonnees.be/ https://www.gegevensbeschermingsautoriteit.be/	Law of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data Law of 3 December 2017 establishing the Data Protection Authority
3	Bulgaria	Commission for Personal Data Protection https://www.cdpd.bg/	Personal Data Protection Act
4	Croatia	Croatian Personal Data Protection Agency http://www.azop.hr/	Law on Implementation of the General Data Protection Agreement
5	Cyprus	Office of the Commissioner for Personal Data Protection http://www.dataprotection.gov.cy/	Law Providing Protection of Natural Persons against the Processing of Personal Data and the Free Movement of this Data

	Country	Supervising Authority	Implementing Law(s)
6	Czech Republic²	Office for Personal Data Protection http://www.uouu.cz/	Act No. 110/2019 Coll., on processing of personal data
7	Denmark	Datatilsynet http://www.datatilsynet.dk/	Law No. 502 of 23 May 2018 on Supplementary Provisions to the Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Exchange of Such Information (Data Protection Act) https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf
8	Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) http://www.aki.ee/	Personal Data Protection Act 616 SE
9	Finland	Office of the Data Protection Ombudsman http://www.tietosuojafi.fi/en/	Data Protection Act (Fi: Tietosuojalaki, 1050/2018)
10	France	Commission Nationale de l'Informatique et des Libertés – CNIL http://www.cnil.fr/	Law No. 78-17 dated 6 January 1978 on information technology, files and freedoms, as amended by: - Law No. 2018-493 dated 20 June 2018 on the protection of personal data; and - Ordinance No. 2018-1125 dated 12 December 2018 implementing Article 32 of Law No. 2018-493. - Law No. 78-17 has been implemented by Decree No. 2005-1309 dated 20 October 2005 as amended by Decree No. 2018-687 dated 1 August 2018 - Law No. 78-17 is implemented by Decree No. 2019-536 dated 29 May 2019

2. In the Czech Republic, Act No. 216/1994 Coll., on Arbitration and Enforcement of Arbitral Awards, governs the conditions under which the state delegates its jurisdiction to private subjects – the arbitrators – the substantive and procedural framework of arbitration with regard to both *ad hoc* arbitrators and permanent arbitration courts as well as conditions under which the latter category can be established. Unlike in other Member States of the European Union, permanent arbitration courts in the Czech Republic can only be established by special legal act, or only if their establishment is expressly permitted by such special legal act..

	Country	Supervising Authority	Implementing Law(s)
11	Germany – Federal	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit https://www.bfdi.bund.de/DE/Home/home_node.html	German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680
	Baden-Württemberg	Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg https://www.baden-wuerttemberg.datenschutz.de/	Act to Adapt Data Protection Law to Regulation (EU) 2016/679 (Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679) dated 12 June 2018
	Bavaria	Bavarian Data Protection Commissioner https://www.datenschutz-bayern.de/	Bavarian Data Protection Act (Bayerisches Datenschutzgesetz) dated 15 May 2018
	Berlin	Berliner Beauftragte für Datenschutz und Informationsfreiheit https://www.datenschutz-berlin.de/	Berlin Data Protection Act (Berliner Datenschutzgesetz) dated 13 June 2018
	Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg https://www.la.brandenburg.de/cms/detail.php?gsid=bb1.c.233960.de	Brandenburg Data Protection Act (Brandenburgisches Datenschutzgesetz) dated 8 May 2018 [German]
	Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit https://www.datenschutz.bremen.de/	Bremen Act on implementation of the General Data Protection Regulation (Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung) dated 8 May 2018
	Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz-hamburg.de/	Hamburg Data Protection Act (Hamburgisches Datenschutzgesetz) dated 18 May 2018
	Hesse	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz.hessen.de/	Hessian Data Protection Act and Freedom of Information Act (Hessisches Datenschutz- und Informationsfreiheitsgesetz) dated 3 May 2018

Country	Supervising Authority	Implementing Law(s)
Mecklen-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklen-Vorpommern https://www.datenschutz-mv.de/	Law on the Adaptation of the State Data Protection Act and other data protection regulations within the area of responsibility of the Ministry of the Interior and Europe Mecklenburg-Vorpommern to the Regulation (EU) 2016/679 and the implementation of the Directive (EU) 2016/680 (Gesetz zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 22 May 2018
Lower Saxony	Die Landesbeauftragte für den Datenschutz Niedersachsen https://www.lfd.niedersachsen.de/startseite/	Lower Saxony Data Protection Act (Niedersächsisches Datenschutzgesetzes) dated 16 May 2018
North Rhine-Westphalia	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen https://www.lfdi.nrw.de/	North Rhine Westphalia Data Protection Act (Datenschutzgesetz Nordrhein-Westfalen) dated 17 May 2018 (Datenschutzgesetz Nordrhein-Westfalen) dated 17 May 2018
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz https://www.datenschutz.rlp.de/de/startseite/	State Data Protection Law (Landesdatenschutzgesetz) dated 8 May 2018
Saarland	Unabhängiges Datenschutz Zentrum Saarland https://datenschutz.saarland.de/	Saarland Data Protection Act (Saarländisches Datenschutzgesetz) dated 16 May 2018
Saxony	Sächsischer Datenschutzbeauftragter https://www.saechdsb.de/	Saxony Data Protection Act (Sächsisches Datenschutzgesetz) dated 25 August 2003 (last amended on 22 August 2019)

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

	Country	Supervising Authority	Implementing Law(s)
	Saxony-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt https://datenschutz.sachsen-anhalt.de/nc/datenschutz-sachsen-anhalt/	Saxony-Anhalt General Data Protection Regulation Implementation Act (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt) dated 18 February 2020 Saxony-Anhalt Data Protection Directive Implementation Act (Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt) dated 2 August 2019
	Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz https://www.datenschutzzentrum.de/	State Data Protection Law (Landesdatenschutzgesetz) dated 2 May 2018
	Thuringia	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit https://www.tlfdi.de/	Thuringia Data Protection Act (Thüringer Datenschutzgesetz) dated 6 June 2018 [German]
12	Greece	Hellenic Data Protection Authority http://www.dpa.gr/	Law No. 4624/2019
13	Hungary	Hungarian National Authority for Data Protection and Freedom of Information http://www.naih.hu/	Act on the Right to Information Self-Determination and Freedom of Information 2011 CXII. law for legal harmonisation
14	Iceland	Persónuvernd https://www.personuvernd.is/	Law no. 90/2018 on personal protection and processing of personal information
15	Ireland	Irish Data Protection Commission https://www.dataprotection.ie/	Data Protection Act 2018
16	Italy	Garante per la protezione dei dati personali (“Garante Privacy”) https://www.garanteprivacy.it/	Provisions for the adaptation of national legislation to the provisions of the GDPR, in particular Legislative Decree No. 101 of 10 August 2018, which amended the “Privacy Code” (Legislative Decree No. 196 of 30 June 2003)
17	Latvia	Data State Inspectorate http://www.dvi.gov.lv/lv/	Personal Data Processing Law

	Country	Supervising Authority	Implementing Law(s)
18	Liechtenstein	Data Protection Office, Principality of Liechtenstein https://www.datenschutzstelle.li	Liechtenstein Data Protection Law, 4 October 2018
19	Lithuania	State Data Protection Inspectorate https://www.ada.lt/	Law on the Protection of Personal Data
20	Luxembourg	Commission Nationale pour la protection des données http://www.cnpd.lu/	Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the General Scheme on Data Protection
21	Malta	Office of the Information and Data Protection Commissioner https://idpc.org.mt/en/Pages/Home.aspx	Data Protection Act (CAP 586) Other Subsidiary Legislation, including: Subsidiary Legislation 586.09 Restrictions of the Data Protection (Obligations and Rights) Regulations
22	The Netherlands	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/nl	Law Implementing the General Data Protection Regulation
23	Norway	Datatilsynet www.datatilsynet.no	The Personal Data Act
24	Poland	Personal Data Protection Office (Urząd Ochrony Danych Osobowych) https://uodo.gov.pl/	Act of 10 May 2018 on the Protection of Personal Data Act of 26 May 1982, Law on Advocates (Polish: Prawo o adwokaturze) Act of 6 July 1982 on Attorneys-at-law (Polish: Ustawa o radcach prawnych)
25	Portugal	Comissão Nacional de Protecção de Dados – CNPD https://www.cnpd.pt/	Law no. 58/2019 of 8 August 2019

	Country	Supervising Authority	Implementing Law(s)
26	Romania	The National Supervisory Authority for Personal Data Processing http://www.dataprotection.ro/	Law 190/2018 on measures to implement regulations of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the EU Directive 95/46 https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf [unofficial translation] Law 129/2018 amending Law 102/2005 on the creation, organization and functioning of the National Supervisory Authority for Personal Data Processing, and repealing Law 677/2001 for the protection of individuals regarding personal data processing and the free circulation of such data
27	Slovakia	Office for Personal Data Protection of the Slovak Republic http://www.dataprotection.gov.sk/	Act No. 18/2018 Coll., on Protection of Personal Data and on Changing and Amending of Other Acts (the “ <i>Slovak Data Protection Act</i> ”)
28	Slovenia	Information Commissioner of the Republic of Slovenia https://www.ip-rs.si/	[legislation implementing the GDPR in draft]
29	Spain	Agencia Española de Protección de Datos (AEPD) https://www.aepd.es/es	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
30	Sweden	Datainspektionen http://www.datainspektionen.se/	Law (2018:218) with additional provisions to the EU Data Protection Ordinance Regulation (2018: 219) with additional provisions to the EU Data Protection Ordinance

Roadmap to Data Protection in International Arbitration

Data protection laws prescribe the rules applicable to personal data processing, including when, where and how personal data may be processed. However, they do not address how they should be applied in specific contexts, including arbitration. This ICCA-IBA Roadmap to Data Protection in International Arbitration ("Roadmap") has therefore been developed by the ICCA-IBA Task Force as a tool to assist arbitration professionals in understanding how the data protection laws may apply during international arbitration proceedings.

When an arbitral participant is subject to a data protection law, compliance is legally required. As a result, data protection principles will need to be applied to supplement the applicable laws, arbitration rules, and soft law instruments (including the IBA Rules). By reference to general data protection principles, the Roadmap aims to assist arbitral participants in identifying and addressing data protection issues, and proposes that arbitration proceedings benefit when data protection compliance is addressed early in the process and a reasonable, cooperative, and proportionate approach is adopted and documented. The Annexes provide practical guidance in the form of practice tips, check lists, references, and sample text for data protection directions/protocols, standard contractual clauses, and privacy notices.

The ICCA Reports No. 7



December 2021

Volume 27, Number 3

GEORGIA BAR JOURNAL

COVID-19-Induced
Courthouse Workarounds:
Adopting Temporary
Changes for the Permanent
Good—Virtual Voir Dire

From the YLD President:
It's OK to Not Be OK

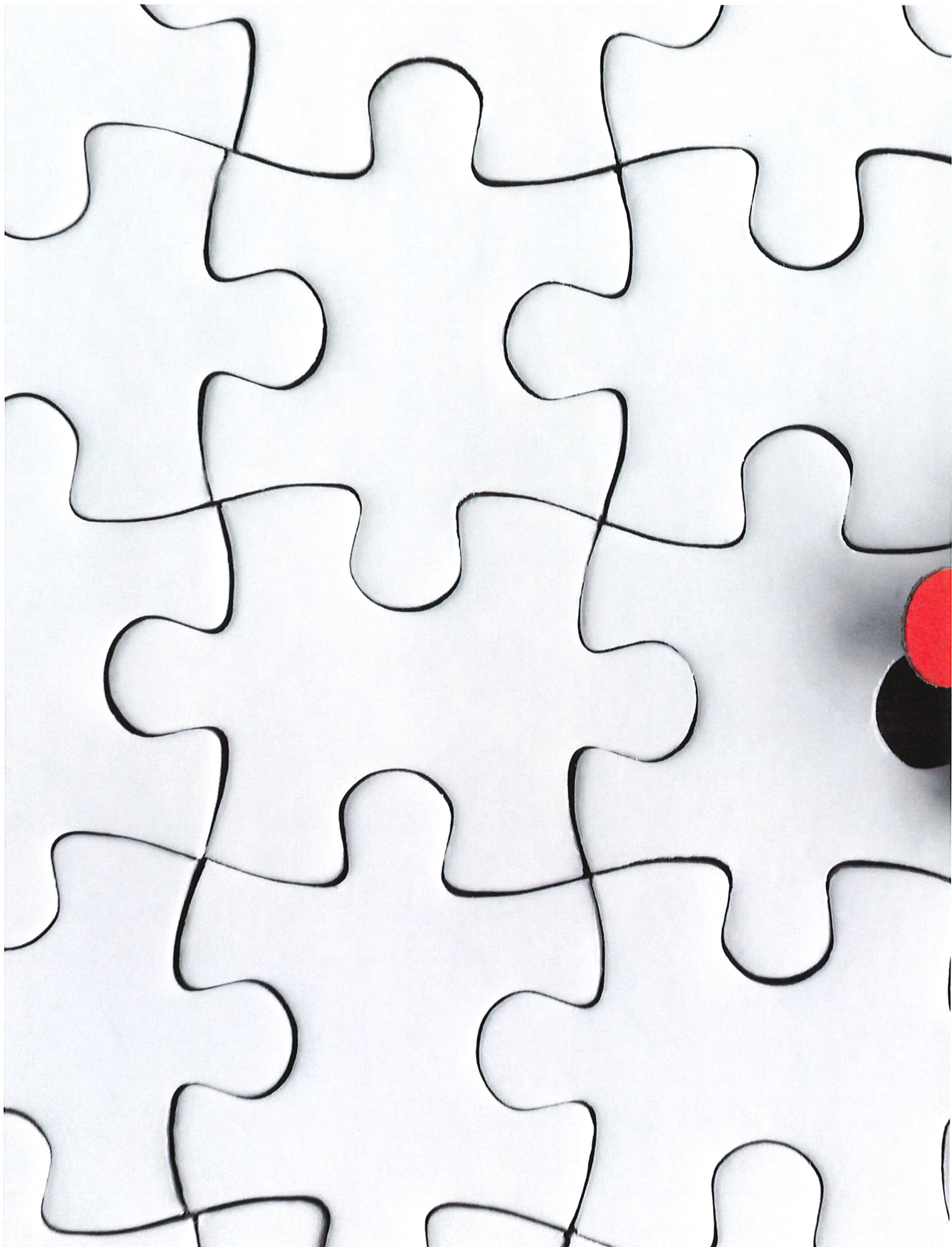
A Conversation with
Douglas Burrell

A New Resolve on
New Year's Resolutions



THE LEGAL

Georgia's New Mediation Law: Harmonization and Innovation



Georgia's New Mediation Law: Harmonization and Innovation

This article explains the genesis of the new Georgia Uniform Mediation Act, outlines its scope and function and discusses some important practice points for attorneys and mediators.

BY SHELBY S. GUILBERT JR., TRACY JOHNSON,
STEPHEN F. MCKINNEY AND DOUGLAS H. YARN

Each year, thousands of mediations take place in Georgia.¹ Some are court-ordered, many are administered privately pursuant to voluntary agreements by the parties and an increasing number involve parties in international disputes arising from business activities in Georgia. Although reliable statistics are hard to come by given the proliferation of voluntary mediations and the growth in mediations in which the parties are unrepresented, most practitioners would agree that, over the last two decades in Georgia, far more civil disputes have been resolved through mediation than jury verdicts. Given the current backlog in the courts due to the COVID-19 pandemic, and the escalating costs associated with civil litigation, this trend will likely continue in the years ahead, not only in Georgia but around the country.

In most mediations, the decisive factor in whether the mediation will prove successful is the parties' willingness to be open and candid with each other and the mediator about their underlying interests and the strengths and weaknesses of their respective claims and defenses. And the willingness to be candid depends on assurances by the parties and the mediator that what happens in mediation stays in mediation.²

Most Georgia lawyers are familiar with the assurances of confidentiality that mediators give in their introducto-



MEDIATION

ry statements at the outset of a mediation. But does the law back up these assurances? Until recently, the answer to this question was uncertain and depended in part on whether the mediation was court-connected, and thus subject to the Alternative Dispute Resolution Rules (Georgia ADR Rules) promulgated by the Supreme Court of Georgia,³ or whether the parties were conducting a voluntary mediation, where parties are free to express in writing (or not) their agreement to keep mediation communications confidential. This uncertainty created confusion in Georgia case law⁴ and has contributed to a reluctance on the part of some parties, particularly those from outside the United States who are increasingly engaged in international trade and investment activities in Georgia, to conduct mediations in this state.

The new Georgia Uniform Mediation Act (GUMA),⁵ which became effective on July 1, 2021, was drafted to address these issues by creating a well-defined statutory privilege for mediation communications and requiring all mediators to disclose potential conflicts of interest before a mediation, regardless of whether the mediation is court-connected or voluntary. The GUMA also contains a specific section that is designed to promote international mediation in Georgia, which will enhance Georgia's position as a leading hub for the resolution of international business disputes.⁶

This article explains the genesis of GUMA, outlines its scope and function

and discusses some important practice points for attorneys and mediators.

Background and Objectives

Generally, there are three mechanisms available to help keep mediation communications confidential: (1) confidentiality agreements, (2) evidentiary exclusion and (3) evidentiary privilege. With respect to confidentiality agreements, it is common practice to include confidentiality provisions in an agreement to mediate, at least when the parties are represented by lawyers, which is not always the case. A confidentiality agreement may bind the parties with a duty to maintain secrecy and restricts what they can reveal to the public or others about the mediation. A confidentiality agreement cannot, however, bind non-signatories, and the mediator may or may not be a signatory.⁷ A confidentiality agreement also cannot insulate mediation communications from being introduced in court proceedings unless a court chooses to recognize and enforce the agreement.⁸

With respect to evidentiary exclusion, Section 408 of Georgia's evidence code makes "[e]vidence of conduct or statements made in compromise negotiations or mediation" inadmissible.⁹ But Section 408 applies only to proceedings governed by Georgia's evidence code. It does not protect mediation communications from discovery, and it contains loopholes that allow mediation communications to be offered as evidence for "another purpose," such as "proving bias or prejudice of a witness, negating a contention of undue delay or abuse of process, or proving an effort to obstruct a criminal investigation or prosecution."¹⁰ Moreover, only parties to the litigation may invoke Section 408, which does little to protect a non-party mediator-witness who feels ethically bound not to disclose what occurred in the mediation.

In contrast to confidentiality agreements and evidentiary exclusion, evidentiary privilege provides more protection from disclosure because it creates (1) a right not to disclose, and (2) a right to keep others from disclosing mediation communications, in both discovery and

"Generally, there are three mechanisms available to help keep mediation communications confidential: (1) confidentiality agreements, (2) evidentiary exclusion and (3) evidentiary privilege. lawyers, which is not always the case."

at trial. Prior to the GUMA, the law on the existence of an evidentiary privilege for mediation in Georgia was murky and inconsistent at best. Murky, because the Georgia ADR Rules, which regulate court-connected mediation in Georgia,¹¹ indirectly establish a hybrid rule of evidentiary exclusion and privilege that insulates court-connected mediation communications from discovery and protects the mediator from subpoenas. Inconsistent, because the ADR Rules do not apply to private, voluntary mediations, which are thus denied the same protections.¹² The resulting confusion came to a head in *Wilson v. Wilson*,¹³ where the Supreme Court of Georgia confronted a mediation that may or may not have been court-connected and raised significant questions about the admissibility of the mediator's voluntary testimony in a subsequent trial. In light of the murky and inconsistent state of the law on mediation confidentiality, the Court justified its decision to allow the evidence by citing the Uniform Mediation Act (UMA), which was not Georgia law at the time.¹⁴

Naturally, the Court's policy-making body for court-connected mediation, the Georgia Commission on Dispute Resolution (GCDR), became interested in a Georgia version of the UMA to fill the gaps left open by confidentiality agreements and evidentiary exclusion and to

provide more clarity and consistency to the law governing confidentiality in mediation. The Uniform Law Commission promulgated and approved the UMA in 2001,¹⁵ in collaboration with the American Bar Association's Section on Dispute Resolution. The ABA approved the UMA the following year, and all the major national providers of dispute resolution services have endorsed it. Twelve other states have passed versions of the UMA, and other states currently have it under consideration. Other states, such as Florida, have drawn on the UMA's principles when devising or revising their mediation confidentiality schemes.¹⁶ The UMA is remarkably stable having generated very little case law over its meaning and application.

In 2017, the Atlanta International Arbitration Society (AtlAS) began exploring draft legislation on confidentiality in international mediations. The primary goal of AtlAS is to promote Georgia as a venue for international dispute resolution.¹⁷ One way to achieve this goal is to create an attractive legal environment for the resolution of international disputes by promoting legislation familiar to international practitioners. One obvious candidate was the United Nations Commission on International Trade Law (UNCITRAL) Model Law on International Commercial

Conciliation, which was promulgated in 2002 to serve as a model law for international mediation.¹⁸ But adopting this legislation would not have solved Georgia's problems with confidentiality in domestic mediations.

A 2003 amendment of the UMA incorporated the UNCITRAL Model Law on International Commercial Conciliation.¹⁹ Adopting the UMA in Georgia would therefore allow the GCDR and AtlAS to kill two birds with one stone. Thus, representatives of both bodies formed a joint working group to study and report on the efficacy of the UMA for both domestic and international mediations in Georgia. After several months of study, discussion and revision, the working group recommended adopting a version of the UMA. Since 2018, GCDR, AtlAS and the Dispute Resolution Section of the State Bar of Georgia worked with other stakeholders to garner support for the Act. This group effort ultimately obtained the support of the Judicial Council of Georgia, the Atlanta Chamber of Commerce, numerous sections of the State Bar and the Atlanta Bar Association, the State Bar's Board of Governors and the Association of Conflict Resolution's Georgia Chapter, as well as important input from the Georgia Trial Lawyers Association. The State Bar of Georgia voted to include the GUMA in its



BEN PARKS

OUTSTANDING RATES & SERVICE

“

Outstanding rates and service. Even more importantly, Ben Parks is why we are with ALPS—Ben explains all to lawyers in an easy to understand manner—a fleeting art in our profession.

”

▶ Randall Fry, The Fry Law Firm, Atlanta, GA

Learn how ALPS can benefit your firm at:

www.alpsinsurance.com/georgia

◀ Ben is located right here in Georgia. Get in touch with him today!

● bparks@alpsinsurance.com ● (470) 946-0819



ALPS

LEGAL MALPRACTICE INSURANCE MADE EASY

★ Trustpilot

★
★
★
★
★

Our Policyholders Love Us!

legislative package in 2019 and 2021. The General Assembly passed the GUMA on March 25, 2021, and the governor signed it into law on May 10, 2021.²⁰

Scope of the GUMA

The GUMA covers “mediation communications,” including verbal and non-verbal statements made during a mediation or for the purposes of mediating.²¹ “Mediation communications” also includes documents and other materials created for purposes of the mediation.²² Consistent with the evidentiary exclusion rule, the privilege created by the GUMA does not extend to the underlying facts of the dispute, and otherwise discoverable or admissible information and evidence does not become privileged merely because it was disclosed in mediation.²³

While the GUMA broadly defines the term “mediation,” it applies only to formal mediations such as:

- mediations required by statute or rule or referred by an adjudicative body or administrative agency;
- private, voluntary mediations where the parties and mediator agree to mediate in a record that demonstrates an expectation that mediation communications will be privileged; or
- any mediation conducted by someone who holds themselves out as a mediator or provider of mediation.²⁴

The GUMA does not cover mediations involving collective bargaining, programs for minors in primary and secondary schools, programs in prisons for inmates and judicial settlement conferences conducted by a judge who may make a ruling on the dispute.²⁵ Consistent with mediation’s core principle of party autonomy, parties can opt out of the GUMA’s coverage.²⁶

Operation of the Mediation Privilege

The GUMA creates a mediation privilege by providing that mediation communications are neither subject to discovery nor admissible in evidence in any adjudicative or legislative process.²⁷ Fur-

ther, all the participants in a mediation can invoke the privilege²⁸ in ways limited to their status as parties in the dispute and process. For example, “mediation parties” (actual disputants) may use the privilege to protect mediation communications from disclosure by themselves or by others.²⁹ A “mediator” may use the privilege to refuse to disclose a mediation communication or to keep others from disclosing the mediator’s communication.³⁰ “Non-party participants” (including an attorney) may use the privilege to refuse to disclose a mediation communication or keep others from disclosing their communication.³¹

The GUMA also provides that holders of the mediation privilege can explicitly waive it.³² Waivers operate as follows:

- For testimony about a party’s mediation communications, all parties hold the privilege, and therefore all parties must waive the privilege before a party or nonparty participant may testify or provide evidence about a party’s mediation communication. If a mediator seeks to provide that testimony, then all parties and the mediator must waive the privilege.³³
- For testimony about a mediator’s mediation communications, both the parties and the mediator hold the privilege, and therefore both the parties and the mediator must waive the privilege before a party, mediator or nonparty participant may testify or provide evidence of a mediator’s mediation communications.³⁴
- For testimony about a nonparty’s mediation communications, both the parties and the nonparty participants hold the privilege, and therefore both the parties and the nonparty participant must waive the privilege before a party or nonparty participant may testify. If that testimony is to be offered through the mediator, then the mediator must also agree to waive the privilege.³⁵

Finally, if a person makes a disclosure that prejudices another, that person is precluded from asserting a privilege to the extent necessary for the prejudiced person to respond.³⁶ Similarly, a person who uses a mediation in furtherance

of a crime is precluded from asserting the privilege.³⁷

Exceptions to the Privilege and Confidentiality

The GUMA sets out a limited number of categorical exceptions to the mediation privilege for situations where society’s interest in the information outweighs the parties’ interest in maintaining confidentiality.³⁸ These include: (1) signed agreements relating to the conduct of the mediation or the resolution of the dispute; (2) communications covered by the open records or open meetings laws; (3) communications involving threats of violence; (4) communications in furtherance of crimes; (5) communications relating to a professional malpractice claim against a mediator; (6) communications relating to a professional malpractice claim against a participant; and (7) information necessary to protect children or vulnerable elders.³⁹

Moreover, a party can seek a limited exception to the privilege in a court proceeding involving a felony or to contest a mediated settlement agreement.⁴⁰ In a hearing *in camera*, the party must convince the adjudicator that the evidence is not available otherwise and that the need for it outweighs the parties’ interest in protecting confidentiality.⁴¹

Despite these exceptions, mediators cannot be compelled to reveal mediation communications related to contested mediated agreements or ethics or malpractice claims against other participants in the mediation.⁴² If a mediation communication is excepted from the privilege, only the portion necessary for the excepted purpose can be admitted, and the communication does not become discoverable or admissible for any other purpose.⁴³

Mediators’ Responsibilities

In addition to the privilege, which confers a right upon the mediator to refuse to disclose evidence in a subsequent proceeding, the GUMA imposes certain responsibilities upon mediators. Like the current ADR Rules,⁴⁴ the GUMA prohibits communications between mediators and courts or

other adjudicative bodies that may rule on the matter.⁴⁵ This rule is designed to reinforce party confidence in the neutrality of both the mediator and any subsequent adjudicator. This rule insulates the adjudicator from information that might prejudice their subsequent judgment. Specifically, mediators cannot “make a report, assessment, evaluation, recommendation, finding, or other communication” to an adjudicator;⁴⁶ however, a mediator can disclose information necessary for administrative purposes, such as whether the mediation occurred, who attended, and whether a settlement occurred.⁴⁷ Of course, the mediator is allowed to disclose the exceptions discussed above and report evidence of neglect, abuse or abandonment to an agency responsible for protecting vulnerable individuals.⁴⁸

The GUMA also includes a consumer protection element by imposing on a mediator the responsibility to disclose any existing or potential conflicts of interest that may cast doubt on the fairness of the proceeding.⁴⁹ Before accepting a mediation, the mediator has a duty to make a reasonable inquiry to determine whether there is a past or existing relationship or some other fact that would lead a reasonable person to believe that the mediator may have an interest in the outcome.⁵⁰ After accepting a mediation, the mediator has a continuing duty to disclose any such facts that may come to the mediator’s attention.⁵¹ This rule is consistent with mediation’s core values of promoting party autonomy and informed consent. Mediators who fail to make timely disclosures waive their right to assert the privilege in that case.⁵²

Finally, mediators must disclose their qualifications to serve upon request by a mediation party.⁵³ This allows parties to make informed decisions about the person they select to help them resolve their dispute. Importantly, the GUMA does not impose any special qualifications upon mediators.⁵⁴ As long as the parties are informed, they may select lawyers or non-lawyers, experienced or inexperienced mediators, and mediators who use different styles. Mediators in court-connected programs, however, are still required to meet the qualification standards under the ADR Rules.⁵⁵

Promoting International Mediation in Georgia

A key feature of the GUMA that sets Georgia apart from other states that have adopted the Uniform Mediation Act is its express incorporation of the United Nations Commission on International Trade Law’s (UNCITRAL)⁵⁶ 2018 Model Law on International Commercial Mediation and Settlement Agreements Resulting from Mediation (the Model Law).⁵⁷ The Model Law amended and modernized UNCITRAL’s earlier 2002 Model Law on International Commercial Conciliation to reflect recent innovations in international dispute resolution and to address issues surrounding the enforcement of international mediated settlement agreements. Section 10 of the GUMA expressly provides that if a mediation is an “international commercial mediation” as defined by Article 2 of the Model Law,⁵⁸ then the mediation is governed by the Model Law unless the parties agree in advance that all or part of the mediation is not privileged,⁵⁹ or the parties otherwise agree that the Model Law shall not apply, in which case the rest of the provisions in Chapter 17 shall apply.⁶⁰ Georgia is the first state in the United States to enact the Model Law.

The Model Law represents a significant innovation in the field of international commercial dispute resolution. Mediation is increasingly seen as a cost-effective mechanism for resolving cross-border business disputes, but the use of mediation around the globe is uneven. For a mediation to be successful, the parties must understand and trust the process and also know that what they say in the mediation may not be used against them, whether in the actual dispute being mediated, or in a collateral proceeding that may take place halfway around the globe at some point in the future. Further, parties from different countries may agree conceptually with the idea of using a neutral party to facilitate a settlement discussion, but because they come from different legal traditions, they may disagree about the ground rules that should govern the mediation. Finally, the goal of mediation is to produce a settlement, but if the mediation results in a settlement agree-

ment that is difficult to enforce across international boundaries, there may be little incentive to mediate in the first place. The Model Law attempts to address these issues in several ways.

First, the Model Law addresses numerous procedural aspects pertaining to international mediation, such as the process for commencing a mediation,⁶¹ the appointment of the mediator,⁶² the conduct of the mediation⁶³ and the termination of the mediation.⁶⁴ Because foreign parties may have less familiarity with mediators outside their home jurisdiction, the Model Law provides that “[w]hen a person is approached in connection with his or her possible appointment as mediator, he or she shall disclose any circumstances likely to give rise to justifiable doubts as to his or her impartiality or independence.”⁶⁵ While the Model Law allows parties to agree to conduct the mediation by reference to the rules of a particular institution,⁶⁶ in the absence of such an agreement, the mediator “may conduct the mediation proceedings in such a manner as the mediator considers appropriate, taking into account the circumstances of the case, [and] any wishes that the parties express and the need for a speedy settlement of the dispute,”⁶⁷ as long as the mediator seeks “to maintain fair treatment of the parties” in so doing.⁶⁸ The mediator also is empowered to make “mediator’s proposals” for a settlement at any stage of the mediation,⁶⁹ a tool that U.S.-based mediators frequently use in domestic mediations.

Second, the Model Law addresses confidentiality concerns by providing that, unless the parties otherwise agree, “all information relating to the mediation proceedings shall be kept confidential.”⁷⁰ In addition, the Model Law prohibits parties, the mediator and any third persons involved in the administration of the mediation proceedings from relying on, introducing as evidence or giving testimony or evidence in another arbitral or judicial proceeding about an invitation to mediate, views expressed in the mediation about settlement, statements or admissions made during the mediation, mediator proposals and documents prepared solely for purposes of mediation.⁷¹

GEORGIA BAR

JOURNAL

Get published.
Earn CLE credit.

The Editorial Board of the *Georgia Bar Journal* is in regular need of scholarly legal articles to print in the *Journal*. Earn CLE credit, see your name in print and help the legal community by submitting an article today.

Submit articles to Jennifer R. Mason:
Director of Communications
jenniferm@gabar.org | 404-527-8761
104 Marietta St. NW, Suite 100, Atlanta 30303



Third, Section 3 of the Model Law provides mechanisms for the enforcement of international commercial settlement agreements resulting from a mediation.⁷² For example, Article 18 sets forth a non-exhaustive list of criteria that courts may rely upon to determine whether to enforce an international settlement agreement governed by the Model Law.⁷³ Article 19 then enumerates a limited set of factors that courts may consider when asked to refuse enforcement of an international settlement agreement governed by the Model Law, such as the incapacity of a party to the settlement agreement; evidence that the settlement agreement is null and void, not final and binding, or has subsequently been modified; evidence that the obligations in the settlement agreement have been performed or are not clear and comprehensible; evidence of mediator misconduct or a failure of the mediator to disclose conflicts of interest; or public policy.⁷⁴ These enforcement mechanisms for mediated international settlement agreements that can now be used in Georgia courts go hand in hand with the 2018 United Nations Convention on International Settlement Agreements Resulting from Mediation (the Singapore Convention on Mediation).⁷⁵ The Singapore Convention on Mediation established a legal framework for the enforcement of mediated international settlement agreements across jurisdictions, in much the same way that international arbitral awards are now enforceable in most countries pursuant to the 1958 Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the New York Convention).⁷⁶ In the two and half years since the General Assembly adopted the Singapore Convention, 54 countries have signed the Convention, including leading trading powers like the United States, Brazil, China, India, Nigeria, the Republic of Korea, Singapore and Saudi Arabia.⁷⁷ Although the United States has not yet ratified the Convention, and most European countries have not yet signed it, the Singapore Convention is now in force in the countries that have ratified it, and the Convention is expected to promote international mediation in

much the same way that the New York Convention fostered an explosion in the use of international commercial arbitration in the decades following its adoption in 1958.

Georgia has long been one of the leading jurisdictions in the United States for the resolution of international business disputes⁷⁸ due to its incorporation of the UNCITRAL Model Law on International Commercial Arbitration into its international arbitration code,⁷⁹ Georgia's strong public policy in favor of international arbitration,⁸⁰ pro-international arbitration decisions from the Eleventh Circuit,⁸¹ and the State Bar's adoption of inclusive rules that allow foreign lawyers to practice in Georgia.⁸² Georgia's enactment of the Model Law continues that trend and places Georgia on the leading edge of international dispute resolution. Global businesses that operate in Georgia can now be confident that the international mediations they conduct in Georgia will be confidential, governed by well-recognized, streamlined international standards that now represent best-practice in international dispute resolution, and that Georgia courts will enforce mediated settlement agreements in much the same way that arbitration awards are enforced under the New York Convention.

Important Practice Pointers for Lawyers and Mediators Operating Under the GUMA

For attorneys, the GUMA should not have an appreciable effect on best practices in mediation representation. The Act specifically recognizes the right of parties to have their attorneys participate in a mediation.⁸³ Although parties might consider opting out of the statutory protections afforded under the Act, there seems little reason to do so. The biggest question for attorneys is how best to manage the three confidentiality mechanisms now available. Under the GUMA, the mediation privilege does not supplant traditional confidentiality agreements or existing rules of evidentiary exclusion.⁸⁴ This allows all three confidentiality mechanisms to come into play as needed. Attorneys can continue to use and enforce confidentiality provisions in me-

diation agreements. Such agreements are particularly important if subsequent related litigation might occur outside Georgia or in federal courts, though parties may wish to provide expressly that the GUMA governs their mediations, which may trigger enforcement of the GUMA in non-Georgia jurisdictions. Further, attorneys can continue to invoke O.C.G.A. § 24-4-408 at trial to exclude evidence of conduct and statements made in mediation. Moreover, there may be other statutes,⁸⁵ court rules⁸⁶ or agency rules⁸⁷ that provide for confidentiality in particular circumstances.

For mediators, the Act simply encourages what should already be accepted best practices for conflicts and qualifications disclosures. The GCDR has formed a working group to review the ADR Rules to ensure conformity with the GUMA; however, the GCDR remains free to impose additional provisions on confidentiality, disclosure and qualifications. Georgia courts with mediation programs can do likewise through their local rules in conformity with the ADR Rules.

Conclusion

Practitioners are increasingly comfortable using mediation as a mechanism for resolving disputes. The GUMA harmonizes the law governing court-connected and voluntary mediations in Georgia, thereby creating greater protections for party-participants, lawyers and mediators alike. It promotes uniformity of the law across state boundaries given the growing acceptance of the GUMA around the country. It also further solidifies Georgia's position as a leading innovator in the field of international dispute resolution and should benefit all members of the Bar, as well as the state's economy, by encouraging more foreign businesses to keep Georgia on their mind when deciding where to conduct trade and resolve international business disputes. ●



Shelby S. Guilbert Jr. is a partner in the Complex Commercial Litigation Group at McGuireWoods LLP and the president-elect of the Atlanta International Arbitration Society (AtIAS).



Tracy Johnson is the Executive Director of the Georgia Office of Dispute Resolution and the immediate past president of the Georgia Council of Court Administrators.



Stephen F. McKinney is an arbitrator and mediator and is the managing director of Dispute Management Services, LLC. He is the immediate past chair of the Dispute Resolution Section of the State Bar of Georgia.



Douglas H. Yarn is a professor of law emeritus, Georgia State University College of Law, and a former ATLAS board member. He co-drafted Georgia's domestic and international arbitration codes and served as an advisor on the adoption of the Uniform Mediation Act.

Endnotes

1. Georgia courts that reported their activity referred 31,228 cases to mediation in 2019. *See Georgia Administrative Office of the Courts, Georgia Office of Dispute Resolution 2019 Caseload Data 2* (2020). This total excludes private voluntary mediations for which there is no reliable data available.
2. DOUGLAS H. YARN, *GEORGIA ALTERNATIVE DISPUTE RESOLUTION* § 7:30 (2021).
3. Ga. Alt. Dispute Resolution R. 7.
4. *See, e.g., Wilson v. Wilson*, 282 Ga. 728, 653 S.E.2d 702 (2007).
5. Georgia Uniform Mediation Act ("GUMA"), O.C.G.A. §§ 9-17-1 to 9-17-17.
6. O.C.G.A. § 9-17-10.
7. *See generally* YARN, *supra* note 3, at § 6:56.
8. *Barger v. Garden Way*, 231 Ga. App. 723, 726, 499 S.E.2d 737, 741 (1998) (disclosure of parties to confidential settlement agreement required because it is implicit in such agreements that parties may nevertheless comply with subpoenas, court orders, and applicable laws).
9. *See Georgia Evidence Code*, O.C.G.A. § 24-4-408(b).
10. For example, offers to compromise are admissible in claims for litigation expenses based on bad faith, stubborn litigiousness and abuse of process against defendants under O.C.G.A. §§ 13-6-11, 24-4-408. *See Christie v. Rainmaster Irr., Inc.*, 299 Ga. App. 383, 390, 682 S.E.2d 687, 693 (2009) (plaintiff's statement allegedly made in the course of settlement correspondence and subsequently elicited during cross-examination admissible to support defendant's claim for attorney's fees); *see also Reid v. Reid*, 348 Ga. App. 550, 556, 823 S.E.2d 860, 866 (2020) (settlement offers were admissible for the purpose of determining whether husband's actions constituted delay or abuse of process). An example of "other purpose" can be found in *Agio Corp. v. Coosawattee River Resort Ass'n, Inc.*, 328 Ga. App. 642, 646, 760 S.E.2d 691, 695 (2014), where evidence of discussions about installing a firewall to settle a claim was admissible because the court did not consider the evidence as an admission, but as evidence that the installation of the firewall might result in corruption of the shared server. *See also Rogers v. Dupree*, 340 Ga. App. 811, 820, 799 S.E.2d 1, 9 (2017) (allegedly extortionist demand letter made by attorney in sexual harassment claim not protected by exclusionary rule nor was the amount of money demanded by that attorney's client during the mediation). The 2017 *Rogers* decision was vacated and remanded on other grounds and in light of *State v. Cohen*, 302 Ga. 616, 807 S.E.2d 861 (2017), and *Cohen v. Rogers* (Case Nos. S17C1376–S17C1380) (April 16, 2018) (order), but on remand the Court of Appeals of Georgia did not revisit the evidentiary issues because the Supreme Court of Georgia had ruled that the demand letter did not constitute evidence of extortion.
11. *See* Ga. Alt. Dispute Resolution R. (2016). The Georgia Court-Connected Alternative Dispute Resolution (ADR) Act, O.C.G.A. § 15-23-1 *et seq.*, outlines how to fund court-connected mediation programs. The ADR Act does not discuss mediation confidentiality or privilege, but those topics are addressed in the ADR Rules.
12. Ga. Alt. Dispute Resolution R. VII.
13. 282 Ga. 728, 653 S.E.2d 702 (2007).
14. *Id.* at 733.
15. Details relating to the Uniform Law Commission's drafting history of the UMA and an annotated version of the UMA are available on the ULC's website at <https://www.uniformlaws.org> (last visited Aug. 1, 2021).
16. *See, e.g., FLA. STAT. ANN.* §§ 44.401 *et seq.* (LexisNexis 2021), and *Me. R. Evid.* 514.
17. *See* ATLAS Mission Statement, available at <http://arbitrateatlanta.org/atlas-mission-vision-values> (last visited Aug. 1, 2021).
18. *Model Law on International Commercial Conciliation*, United Nations Commission on International Trade Law (UNCITRAL), 57th Sess., Supp. No. 17, U.N. Doc. A/57/17, annex I (2002).
19. Uniform Mediation Act, § 11 (2003).
20. 2021 Ga. Laws 268.
21. O.C.G.A. § 9-17-1(2).
22. *Id.*
23. O.C.G.A. § 9-17-3(c).
24. O.C.G.A. § 9-17-2(a).
25. O.C.G.A. § 9-17-2(b).
26. O.C.G.A. § 9-17-2(c).
27. O.C.G.A. § 9-17-3 (a). *See also* O.C.G.A. § 9-17-1(7) (defining "proceeding").
28. *See* O.C.G.A. § 9-17-3. O.C.G.A. § 9-17-1 defines the participants as either a "mediator," a "mediation party" or a "nonparty participant." In somewhat of a redundancy, Georgia's version of the UMA expressly includes mediators in court-connected mediations to emphasize coverage of the Act over those mediations. In another redundant but useful clarification, the GUMA expressly includes lawyers, in their representative capacity, as nonparty participants. *See* O.C.G.A. § 9-17-1(5).
29. O.C.G.A. § 9-17-3(b).
30. *Id.*
31. *Id.*
32. O.C.G.A. § 9-17-4(a).
33. *Id.*
34. *Id.*
35. *Id.*
36. O.C.G.A. § 9-17-4(b).
37. O.C.G.A. § 9-17-4(c).
38. O.C.G.A. § 9-17-5.

39. O.C.G.A. § 9-17-5(a).
40. O.C.G.A. § 9-17-5(b).
41. *Id.* This is equivalent to the UMA section that the Georgia Supreme Court specifically approved of and referenced in *Wilson v. Wilson*, 282 Ga. 728, 733 (2007).
42. O.C.G.A. § 9-17-5(c).
43. O.C.G.A. § 9-17-5(d).
44. Ga. Alt. Dispute Resolution R., App. C, Ch. 1, III(C)(b).
45. O.C.G.A. § 9-17-6(c).
46. O.C.G.A. § 9-17-6 (a).
47. O.C.G.A. § 9-17-6(b).
48. *Id.*
49. O.C.G.A. § 9-17-8(a)(1).
50. O.C.G.A. § 9-17-8(a).
51. O.C.G.A. § 9-17-8(b).
52. O.C.G.A. § 9-17-8(d).
53. O.C.G.A. § 9-17-8(c).
54. O.C.G.A. § 9-17-8(f).
55. Ga. Alt. Dispute Resolution R. V.
56. *Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation*, UNCITRAL, U.N. Doc. A/73/17, Annex II (2018) (the “Model Law”). The United Nations General Assembly established UNCITRAL in 1966 to promote the harmonization and modernization of the law of international trade. *See* GA Res 2205, UNGAOR, 21st Sess, Annex II, U.N. Doc A/6394. Over the last 55 years, UNCITRAL has worked with member states of the United Nations, non-member states, and intergovernmental and nongovernmental organizations to negotiate and prepare model laws, international treaties and other legal instruments regarding numerous aspects of international commercial law, including international dispute resolution, the international sale of goods, international contracting, international transport, electronic commerce and international transport. *See* A GUIDE TO UNCITRAL: BASIC FACTS ABOUT THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (2013), at 1. UNCITRAL’s model laws and instruments have been widely adopted across the globe in part because they can help countries accommodate differences and resolve disputes that sometimes arise when countries from different legal traditions and in different stages of economic development engage in international commerce.
57. O.C.G.A. § 9-17-10(a)–(b).
58. Under Article 2 of the Model Law, a mediation is “international” if: (a) the parties to an agreement to mediate have, at the time of the conclusion of that agreement, their places of business in different States; or (b) the State in which the parties have their places of business is different from either: (i) the State in which a substantial part of the obligations of the commercial relationship is to be performed; or (ii) the State with which the subject matter of the dispute is most closely connected.
59. O.C.G.A. § 9-17-10(c).
60. O.C.G.A. § 9-17-10(d).
61. Model Law, Art. 5.
62. Model Law, Art. 6.
63. Model Law, Art. 7.
64. Model Law, Art. 18.
65. Model Law, Art. 6(5).
66. Model Law, Art. 7(1).
67. Model Law, Art. 7(2).
68. Model Law, Art. 7(3).
69. Model Law, Art. 7(4).
70. Model Law, Art. 10.
71. Model Law, Art. 11(1).
72. *See generally* Model Law, § 3. Section 3 on International settlement agreements expressly does not apply to certain categories of settlement agreements involving consumer transactions, “family, inheritance or employment law,” court approved settlements or settlement agreements that are enforceable as an arbitral award. *See* Model Law Art. 16(2)–(4).
73. Model Law, Art. 19 (listing factors).
74. Model Law, Art. 19.
75. United Nations Convention on International Settlement Agreements Resulting from Mediation, Dec. 20, 2018.
76. Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21.3 U.S.T. 2517.
77. *See* STATUS: UNITED NATIONS CONVENTION ON INTERNATIONAL SETTLEMENT AGREEMENTS RESULTING FROM MEDIATION, available at https://uncitral.un.org/en/texts/mediation/conventions/international_settlement_agreements/status (last visited, Aug. 1, 2021).
78. For a discussion of the Georgia International Arbitration Code and other innovations in Georgia designed to facilitate international commercial dispute resolution in Georgia, *see generally*, Stephen L. Wright & Shelby S. Guilbert Jr., *Recent Advances in International Arbitration in Georgia: Winning the Race to the Top*, Ga.St.B.J., June 2013, at 18.
79. *See* O.C.G.A. § 9-9-20, *et seq.*
80. *See* O.C.G.A. § 9-9-20(b) (stating that the purpose of the international arbitration code is “to encourage international commercial arbitration in the state, to enforce arbitration agreements and arbitration awards, to facilitate prompt and efficient arbitration proceedings . . . and to provide a conducive environment for international business and trade”).
81. *Indus. Risk Insurers v. M.A.N. Gutehoffnungshutte GmbH*, 141 F.3d 1434, 1445 (11th Cir. 1998) (holding that an international arbitration award issued in a U.S. proceeding is subject to vacatur only on the grounds set forth in Article V of the New York Convention); *Bautista v. Star Cruises*, 396 F.3d 1289, 1302 (11th Cir. 2005) (eliminating domestic arbitration law as a basis for vacating international arbitration awards).
82. *See, e.g.*, Ga. Super. Ct. R. 4.4 (authorizing *pro hac vice* admission of foreign lawyers) and Ga. R. Prof. Cond. 5.5(e) (authorizing temporary practice of law by foreign lawyers).
83. O.C.G.A. § 9-17-9.
84. O.C.G.A. § 9-17-7.
85. *See, e.g.*, O.C.G.A. § 12-10-100 (confidentiality of mediation under the Apalachicola-Chattahoochee-Flint River Basin Compact, Art. XIII (a) (8) & (9)), and O.C.G.A. § 12-10-110 (confidentiality of mediation under the Alabama-Coosa-Tallapoosa River Basin Compact, Art. XIII (a)(8)&(9)).
86. *See, e.g.*, ADR Rule VII. B.
87. *See, e.g.*, Rule 100 of the Board of Workers’ Compensation (confidentiality of mediation of workers; compensation claims).

Arbital Foresight: The Arbitrator's Untapped Superpower

Christopher M. Campbell*

- I Introduction
- II The Problem: The Financial and Temporal Costs
- III The Concept of Arbital Foresight
- IV Arbital Foresight in Practice
- V Conclusion

I Introduction

There are several scenes in the Joel Silver-directed movies *Sherlock Holmes* and *Sherlock Holmes: Game of Shadows*, whereby Sherlock Holmes (portrayed by Robert Downey Jr.) uses the information and/or clues before him to foresee how a scuffle or a particular scene will play out. The screen fades to a dreamy-like sequence, and the scene plays out in slow motion with how Holmes imagines the events will unfold. Once that sequence concludes, the scene then plays out in real-time, often exactly as Holmes foresaw, but not always.

There is a moment at the end of an arbitral proceeding where the parties and arbitrators alike look back and wonder “what could have been,” and where were the missed moments or pieces of information that could have brought these two sides to resolution sooner. They were likely there, but for whatever reason they were missed. From the parties’ perspective, had they known that the tribunal would have ruled a certain way on a given issue earlier in the proceedings, perhaps there could have been an opportunity for resolution. If clients and counsel had the opportunity to peer into the mind of the tribunal at a pivotal moment in the case, perhaps they could have cracked the case; it would “be elementary, my dear reader.” But alas, no such opportunity materializes, and both sides will instead spend months if not years and likely millions of dollars in fielding their cases.

But what if the parties, already at the mercy of the tribunal, bestowed a further power to the tribunal? Not one that materially changes arbitral process or limits the power for the parties to

* Christopher (“Chris”) M. Campbell is a Florence, IT based Senior Counsel—Litigation at Baker Hughes. He is an active figure in the international disputes community and host of the podcast, *Tales of the Tribunal*, where he discusses topics related to international law and interviews people from across the field. Chris regularly writes and speaks on topics related to technology, energy, oil & gas and DEI. He is a graduate of the Darla Moore School of Business and the Joseph F. Rice School of Law at the University of South Carolina (Formerly South Carolina School of Law).

make their case, but instead gave tribunals the powers to pull back the veil of secrecy and to let the parties see a glimpse of their future in this case if the matter were to be decided right then and there. Some national legal systems already include a version of this ability, and other authors have written of similar versions of this procedural mechanism and described it as “arbitrator facilitation.” With some strategic and practical adjustments to these sources of inspiration and as a means of ascribing the enhanced role this notion purports to give tribunals, this chapter coins the term Arbitral Foresight (“Foresight”) for consideration for the broader arbitration community.

Foresight is the ability of tribunals to give preliminary perspectives on the issues in dispute before them, on an anonymous basis, and with party consent. This is a neatly distilled tribunal superpower and one that could greatly assist arbitrators and therefore the parties in resolving their claims without the need of continuing through standard arbitral proceedings.

From the beginning of the proceedings, arbitrators are imbued with a special trust, positioned by the parties as the arbiters of their fate in these proceedings. With that great power comes great responsibility.¹ The point is not to prejudge the case or to deprive any party of the opportunity to make their case, instead the goal is to give the parties foresight so that they can make informed decisions at the earliest point possible.

II The Problem: The Financial and Temporal Costs

Before delving into defining and explaining the virtues of Foresight, it is important to understand the problems that lead to this proposed solution. Indeed, there are three fundamental factors: (i) the cost of arbitral proceedings, (ii) the amount of time required to complete the arbitral process and (iii) understanding why clients go to arbitration in the first place.

1 Financial Costs

From the moment a matter fails to resolve itself in pre-dispute negotiations until the final award is rendered, the financial costs begin to accrue, whether that be theoretical costs like opportunity

¹ Stan Lee, *The Amazing Spider-Man & Amazing Fantasy* No. 15, 245 (1962), quoting, *Convention Nationale, Collection Générale des Décrets Rendus par la Convention Nationale* 72 (Chez Baudouin, Imprimeur de la Convention Nationale, Paris, 1793).

or sunk costs, or the costs immediately realized with the processing of each invoice from the tribunal, the hired experts or external counsel.

The costs in international commercial arbitrations can vary widely. Industry reports advise that the low-end of such costs can be greater than USD 1 million but can also reach atmospheres of USD 10 million+.² A survey from the Chartered Institute of Arbitrators reported that both these costs tend to be between USD 1.6 million and USD 1.8 million, with nearly 74% of those costs being accrued in legal fees.³ Therefore, in order to meaningfully control the overall costs of arbitral proceedings, one must endeavor to limit the primary cost drivers in the process, in this case, legal fees.

Framed another way, if we can shorten the length of the proceedings, then this presumably would also lessen the amount of legal support required and ultimately succeed in limiting costs.

2 Temporal Investment

Here, the old adage rings true “time is money,”⁴ and for every moment a company’s staff members are supporting dispute resolution, instead of their primary business function, this is time they are now providing substantive value to the company and thus subtracting from profit-inducing activities. Even in matters that are largely outsourced to external counsel, there are still likely to be hundreds of hours of non-productive time incurred that bear little chance of being recoverable but are costs realized, nonetheless.

Additionally, when one considers the average length of an arbitration from beginning to end, it is on average between fifteen and twenty-two months.⁵ This is the time where both the previously mentioned internal resources are occupied and where parties to the proceedings are hostage to the time that it takes to resolve the dispute. In an era where companies are living quarter to quarter, a victory on the merits of the proceedings drawn out over the course of 1.5-2

² Allocation of Costs, Jus Mundi, January 2, 2024.

<https://jusmundi.com/en/document/publication/en-allocation-of-costs> (accessed March 1, 2024).

³ Chartered Institute of Arbitrators, CI Arb Costs of International Arbitration Survey 11 (2011), <https://shorturl.at/bgBN4> (accessed February 20, 2024).

⁴ Franklin B., “Advice to a Young Tradesman,” in George Fisher (ed.), *The American Instructor: or Young Man’s Best Companion* (1748).

⁵ For more information, see following article which quotes the ICC, ICDR, HKIAC, LCIA and SIAC statistics: “What is the Median Length of an International Arbitration?,” MoloLamken LLP, <https://www.mololamken.com/knowledge-what-is-the-median-length-of-an> (accessed March 11, 2024).

years may simply be untenable. As the financial battles for a client are raging, the reinforcements of a favorable arbitral award may arrive after the commercial battles are already long concluded.

All of these are reasons why even the most fervent of clients will often look for off-ramps before the full development of the case, an opportunity to cut their losses or count their gains while still being able to frame the exercise as a positive.

3 Client Motivation

What exactly is it that client's look for when utilizing arbitration (or really any dispute resolution mechanism)? For many clients or in-house counsel, their wants can be summarized as follows:

(i) *Predictability.* Commercial operations need reasonable and reliable predictability in their dispute resolution process. They need to understand how their arguments will be weighted and judged as well as by whom and how. This allows commercial leaders to evaluate whether a dispute should be pursued vigorously or whether the business should push for a commercial resolution.

Obviously, a tool in the arbitral process that would allow insight into where the tribunal's mindset is in specific moments and where it may be heading would be invaluable intel that would undoubtedly open up further paths to resolution.

(ii) *Cost Efficiency.* As mentioned above, while cost alone may not be determinative when evaluating a dispute, it is certainly a factor in balancing pragmatism in fighting a dispute. Indeed, when compared side-by-side whether it makes sense to settle or fight a dispute, the costs must not be so burdensome so as to dissuade the party from engaging.

In modern arbitration practice, once the submissions begin, it is somewhat rare for the parties to continue meaningful negotiations. This means that the process is likely to run the full course of the procedure and incur the full legal costs.

A technique that could provide for clear pictures of cost and exposure while providing earlier exits from the dispute would be attractive to many clients.

(iii) *Time savings.* Finally, as also mentioned and briefly summarized here, time is of the essence with disputes—i.e., non-profit producing activities—the more quickly they can be resolved, the better.

III The Concept of Arbitral Foresight

1 Overview of Arbitral Foresight

Foresight is a proposed ability activated in the midst of the proceedings that allows arbitrators to provide an anonymous and preliminary perspective on the issues before the tribunal, contingent

upon the consent of the parties involved in the arbitration. The essence of this concept is to afford arbitrators a mechanism through which they can facilitate a quicker, more cost-effective resolution of disputes.

As with all arbitral mechanisms, Foresight should only be implemented with party consent either expressly or by codification in the various institutional arbitration rules.

If there is consent to apply this ability, when would be the ideal time? The better question is, at what point would the parties most benefit from the insights of such Foresight? Indeed, there is not a fixed time where the ability could be activated, and instead the parties could apply to the tribunal to ask for their perspective at any time during the proceedings. That said, there are likely two points in time that make for attractive options:

- Prior to Document Production. At this point in the proceedings, the parties will have had an opportunity to place both their arguments and the evidence that they intend to rely upon before the tribunal. The tribunal will have had an idea to understand those arguments, and candidly, likely already formed some opinion about the matters before them. Although there can be significant cost in getting to this point, that cost is likely still only a fraction of what will be incurred in the next steps of the proceedings through document production and the hearing. By enacting Foresight, the counsel would have a sobering look at their case, how it is landing with the tribunal and importantly, if they need to express a more grounded reality to their client.

However, perhaps there is information yet to be provided, hidden among the informational mines of document production. It may be premature to ask for even preliminary conclusions based on the submissions before the tribunal. If this is the case, the parties can ask for the tribunal's positions *after* document production.

- Immediately Following Document Production. Document production can cost each party hundreds of thousands of dollars in a commercial arbitration. So deciding to wait until after document production to trigger Arbitral Foresight ensures that a certain amount of cost (and time) will be incurred in the arbitral process. However, and admittedly, as a US litigator, the author appreciates that document production in the arbitral context (and its ruder cousin Discovery) can often reveal case-changing information that will turn the perspective of a case on its head.

Once document production is complete, the tribunal will have the vast majority of the submissions that the party will make. Rather than immediately going into post-document production submissions, the parties could be given the benefit of knowing where the case would land were it to end

that day. Again, another opportunity for an off-ramp in the case before incurring the next major cost drivers of preparing for the final hearing, the hearing itself and then post-hearing submissions.

It is important to emphasize that Foresight *does not* render a decision that is binding upon the parties, nor should it be viewed as prejudicial such that a party could rely on favorable preliminary perspective, but rather it invites the parties into the current of the tribunals at a given moment in time of the case. The matter is not prejudged; it is considered with the then-known facts and arguments before the tribunal.

2 Comparative Example

Under standard arbitration procedures, parties coordinate with each other as well as the tribunal to fashion a timeline and procedure to bring the matter through the arbitration process.

Unfortunately, once the matter progresses to arbitration, neither side is usually willing to amend its position without significant developments during the case, or unforeseen external factors.

Generally described, the phases of an arbitration consist of:⁶⁻⁷

- (i) Phase 1—Beginning and Positioning of the case;
- (ii) Phase 2—Initial Argumentation and Presentation of Evidence;
- (iii) Phase 3—Document Production and Maturation of the Case;
- (iv) Phase 4—Hearing Preparation; and
- (v) Phase 5—The Hearing and Post-Hearing Submissions.

Within the framework of these phases, it is not uncommon for the parties to agree for there to be a “Settlement Window”⁸ woven in among the planned issues outlined in the procedural order. Such a period can be as little as two to five weeks but is ultimately intended to give the parties an opportunity to reconsider their case before advancing to the next phase of the proceedings.

Table 3.1 contemplates a dispute valued at around USD 10 million, complex enough to warrant at least one expert, and with potential counterclaims from the respondent. Obviously, there is a wide-spectrum of variance that could occur in the below procedural framework;

⁶ International Chamber of Commerce (ICC), “Arbitration Procedure,” <https://iccwbo.org/dispute-resolution/dispute-resolution-services/arbitration/rules-procedure/arbitration-procedure/> (accessed March 11, 2024).

⁷ American Arbitration Association (AAA), “Stages of the Arbitration Process,” https://www.adr.org/sites/default/files/document_repository/AAA_Stages_of_the_Arbitration_Process.pdf (accessed March 11, 2024).

⁸ The Mediation Window: An Arbitration Process Measure to Facilitate Settlement, 13(1) NYSBA New York Dispute Resolution Lawyer (Spring 2020).

however, what is important are the opportunities to employ Foresight, and where those opportunities fall in terms of driving costs throughout the proceedings. These are the cost estimates for *one* party in this hypothetical dispute.

Table 3.1 Mock Arbitral Timetable

<i>Phase</i>	<i>Time Passage</i>	<i>Actions</i>	<i>Cost</i>
Phase 1: Beginning & Positioning of the Case	16 weeks	Request for Arbitration/Answer & Counterclaims/ Reply to Answer	USD 435,000
Phase 2: Initial Argumentation and Presentation of Evidence	28 weeks	Case Management Conferences/ Statement of Claim/ Statement of Defense/	USD 605,000
Opportunity for Arbitral Foresight ⁹	5 weeks	Application for Arbitral Foresight/Tribunal issues its preliminary perspective/Settlement Window	
Phase 3: Document Production and Maturation of Case	12 weeks	Parties exchange document production requests/Parties present objections/Tribunal rules on objections and orders production/Parties produce/Parties consider documents and evaluate next steps	USD 570,000
Opportunity for Arbitral Foresight	5 weeks	Application for Arbitral Foresight/Tribunal issues its prospective opinion/Settlement Window	

⁹ Note that the parties would be free to apply for Arbitral Foresight at whatever time they deemed appropriate; the author's suggestion is that the discretion of whether to grant such an application would be assistive to the parties at the time of the request—plainly, the idea is not that there be three required periods for application of Arbitral Foresight.

Phase 4: Hearing Preparation	33 weeks	Statement of Reply/Statement of Rejoinder and Reply/Statement of Rejoinder to Counterclaim/Expert Meetings/Final Hearing Preparations/The Hearing	USD 460,000
Opportunity for Arbitral Foresight	5 weeks	Application for Arbitral Foresight/Tribunal issues its prospective opinion/Settlement Window	
Phase 5: Hearing and Post-Hearing	1 week	The Hearing/ Final Submissions by the Parties	USD 550,000
TOTAL:			USD 2,595,000

What we *see* in Table 3.1 is that there are three general opportunities for the tribunal to provide its critical perspective that could assist the parties in resolving the case, immediately before or after Phase 3 (Document Production) and before Phase 5 (Hearing). Doing so *before* document production would represent a savings of 60% of the estimated cost figures, and even doing so before the hearing would save the parties a final 21% of their costs. These savings scale to the size of dispute, and even the most hardline believers in their positions would be hard pressed to ignore these savings.

3 Form of the Preliminary Perspectives

The tribunal would be free to provide their views in whatever written form that they wish, so long as the critical elements of anonymity for each arbitrator are respected, all of the issues are addressed, and that they make clear that the views of the tribunal are preliminary in nature and non-binding.

For reference in imagining what such a schedule could look like, the below is an example of the relevant language and a prototype schedule:

Campbell's Preliminary Perspective Schedule

The tribunal hereby issues these preliminary perspectives ("Perspectives") pursuant to the application from [Claimant/Respondent/Both] and does so for the express purpose of assisting

the parties in any potential discussions regarding the resolution of this matter. The perspectives contained herein are non-binding and without prejudice to the submissions previously made or to be made in these proceedings. The parties have agreed that provision of these Perspectives shall not be used as grounds to challenge or otherwise impede enforcement of the award.

Table 3.2

	<i>Arbitrator #1</i>	<i>Arbitrator #2</i>	<i>Arbitrator #3</i>
Issue #1: [Description of issue]			
Issue #2: [Description of issue]			
Issue #3: [Description of issue]			
Additional Comments to the Parties at the current stage of the proceedings			

IV Arbitral Foresight in Practice

1 Party Consent

As dynamic as Foresight could be, it is absolutely fruitless if the parties do not consent to apply such a mechanism *before* the dispute arises, either expressly through their contractual terms, arbitrator's inclusion in their Terms of References and Procedural Orders and/or finally implementation into institutional arbitral rules and guidelines themselves. Let us turn to each briefly in-kind.

2 Contractual Language & Institutional Model Clauses

Many model clauses from arbitral institutions have the same or similar elements, so for the purpose of focusing on the addition to such a clause, this chapter uses an ICC model clause as an example:

[Language]. Once the tribunal has been constituted, and at any time prior to the issuance of the final award of the tribunal, either party may request that the tribunal issue an advisory preliminary perspective (“Perspective”) that indicates how the tribunal would rule on the matters then before it, were no further submissions by the parties to be made. The tribunal, in its sole discretion, may provide such an Opinion so long as the Opinion is anonymized as to the identity of each member of the tribunal. Said Opinion is non-binding and may not be relied upon should the dispute continue after the Opinion is provided. The parties agree that the tribunal’s provision of the Opinion shall not be grounds of any attempt to set aside, annul, or otherwise undermine the award.¹⁰

With a clause like the one above, the parties could directly opt in to the usage of Foresight, in what is probably the most immediate way to observe the utility of the mechanism. However, in order for the technique to gain wider application and therefore assist parties in mitigating financial and temporal investment in the process, persuading arbitral institutions to implement said rules would add meaningful authority. There need not be a fundamental overhaul or rewrite of the entire rule-set; instead, Foresight can be written into the powers of arbitrators appointed under such rules.

3 Arbitral Practice & Counsel Recommendation

Aside from express agreement in the parties’ contractual terms, a more immediate step would be usage of Arbitral Foresight by counsel and arbitrators.

For counsel, the benefits of such a tool are obvious. Clients are already displeased about having to use a formalized legal process in the first place. Having external counsel recommend a procedure that could substantially decrease the amount of cost and time required to resolve a dispute would instill further trust in the client-attorney relationship as counsel would be recommending a process that might reduce their potential fees, but for the sake of pursuing

¹⁰ Draft language from the author that could be incorporated into the ICC Rules.

resolution as efficiently as possible. Furthermore, even if the matter does not settle after an application for Foresight, counsel would gain valuable insight from the tribunal about the effectiveness of their arguments to the tribunal. This would in turn allow counsel to advise their clients in a more informed manner and make a decision about the strategy in the case.

As for arbitrators, the value in Foresight comes down to how the role of the arbitrator is perceived. Is an arbitrator meant to be passive, merely calling balls and strikes when it comes to the issues placed before them? Or is there a rightful expectation that arbitrators should be actively assisting the parties in coming to a resolution? Are they private judges or equitable peacemakers? These questions are important in understanding the initial assumptions in the untapped power of a regime like Foresight.

Much like the incentives to counsel, arbitrators would benefit from this ability by helping parties have an ever sobering look at how their case is being perceived, exposing the porosity of the arguments that the clients assumed would hold water at the beginning of the proceedings. Effectively implemented, the parties, even the unsuccessful ones, would be thankful to the tribunal for saving them the increased time, resources and financial cost of a lengthy proceeding when, in actuality, there were key issues that were clear to the tribunal early in the process.

4 Party Disagreement

There may be times, for various reasons, when one party may not want to consent to an application for Arbitral Foresight. Is it problematic for the tribunal to provide its preliminary perspectives over the objection of the resistant party?

No.

Throughout the course of every arbitral proceeding, tribunals will make decisions that one or both parties may not agree with; that is a fundamental power imbued upon the tribunal to make decisions that the tribunal believes will most readily bring the parties to resolution.¹¹⁻¹²

Providing (pre-agreed) insight to the tribunal's preliminary perspectives bears little difference to other hallmarks of the arbitral process such as: (i) timetables, (ii) scope of evidentiary submissions, (iii) sequence of the proceedings, (iv) virtual versus in-persons hearings, (v)

¹¹ J. Allsop, Authority of the Arbitrator, 30 Arb. Int'l 639 (2014), <https://doi.org/10.1093/arbitration/30.4.639> (accessed August 16, 2025).

¹² Arbitration: The International Journal of Arbitration, Mediation and Dispute Management 68(4), 369-388 (2002).

inclusion of settlement windows, (vi) teaching sessions for expert witnesses and other similar decisions. Foresight would merely be another tool for the parties to use to assist in resolving the dispute.

5 Challenges to Arbitral Foresight

When explaining the virtues of Foresight, listeners seldom disagree with the goal of finding more cost and time-efficient means of resolving disputes. Instead, there tends to be concerns related to: (i) biasing the tribunal and/or (ii) ensuring that each party has had an opportunity to fully present its case *before* an award is rendered.

Broadly stated, these issues trend toward concern related to the due process afforded to the parties in the proceedings. The theoretical issue is that an award rendered after a tribunal implemented Foresight (which would have been requested by at least one party) could be undermined (set aside or not enforced) if the non-prevailing party wanted to attack the award. These concerns are not merely “Due Process Paranoia” and do deserve consideration;¹³ however, these hesitations can be dealt with in a manner that mitigates lingering skepticism.

6 Set Aside and Enforcement

The 1958 New York Convention for the Recognition and Enforcement of Foreign Arbitral Awards (“New York Convention”)¹⁴ sets out the authority for contracting States, of which there are 172, to set aside arbitral awards on a particular and narrow set of grounds.¹⁵ The New York Convention is widely viewed to act as a substantial guiding source for due process requirements. The UNCITRAL International Commercial Arbitration Model Law (“Model Law”)¹⁶ provides the basis for arbitration legislation in more than 85 States in 118 jurisdictions, also dealing with arbitral procedures. Validity and enforceability of the arbitration award under the New York Convention and the Model Law can be considered in regard to Foresight.

¹³ Oldenstam R., “Due Process Paranoia or Prudence?,” in Axel Calissendorff and Patrik Schöldstrom (eds.), *Stockholm Arbitration Yearbook 2019*, at 121 (Kluwer Law International 2019).

¹⁴ Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, June 10, 1958), 330 U.N.T.S. 3.

¹⁵ *Id.*

¹⁶ United Nations Commission on International Trade Law, UNCITRAL Model Law on International Commercial Arbitration, U.N. Doc. A/40/17, Annex I (1985).

The New York Convention at Article V(1)(b) references insufficient notice related to the appointment of an arbitrator, but also if enforcement may be refused if a party was “otherwise unable to present his case” as a means for setting aside an award. While there is no a uniform approach to interpreting and applying this provision, one summary from the English courts is instructive:

If the tribunal is procedurally entitled to conduct its own investigations into the facts in an inquisitorial system, the effect of this provision would be to avoid enforcement if the award is based on facts derived from such investigations where the enforcer was not given a reasonable opportunity to present its case in relation to the results of the investigations.¹⁷

However, the New York Convention’s position via Article V(1)(b) has generally been construed narrowly by national courts, in light of the New York Convention’s goal of encouraging timely and efficient enforcement of awards.¹⁸

The Model Law at Article 18 simply states that “[t]he parties shall be treated with equality and each party shall be given a full opportunity of presenting his case.” Article 34(2) references a standard of “minimum requirements” of due process not being met; indeed Article 34 is understood to be exclusive, and its annulment grounds are viewed as permissive, not mandatory, allowing a court to annul an award if the Article 34(2) ground is met, but not requiring it to do so.¹⁹ Article 36 on enforcement of arbitration awards mirrors Article V(1)(b) of the New York Convention.

7 Biasing the Tribunal

¹⁷ *Minmetals Germany GmbH v. Ferco Steel Ltd*, [1999] 1 All E.R. (Comm) 315 (Q.B.) (Eng.).

¹⁸ Bermann G., “Recognition and Enforcement of Foreign Arbitral Awards: The Interpretation and Application of the New York Convention by National Courts,” in George Bermann (ed.), *Recognition and Enforcement of Foreign Arbitral Awards*, vol. 23 (Springer 2017) and J. Arbisman, A. Genest and E. Giakoumakis, “Due Process and Procedural Irregularities,” in *The Guide to Challenging and Enforcing Arbitration Awards*, 3rd ed., GAR, <https://globalarbitrationreview.com/guide/the-guide-challenging-and-enforcing-arbitration-awards/3rd-edition/article/due-process-and-procedural-irregularities#footnote-030> (accessed March 11, 2024).

¹⁹ Gary B. Born, *International Arbitration: Law and Practice* 183-184 (3rd ed., Kluwer Law International 2021).

An arbitrator has a duty to remain neutral throughout the duration of the proceedings.²⁰⁻²¹ Critics of Foresight might say that an arbitrator, let alone an entire tribunal, expressing their views on any issue prior to receipt of all submissions from a party on an issue. However, this critique can be addressed with several responses.

Would be critics suggest that Foresight might amount to “prejudgment” of the issues in dispute. Most likely every member of the dispute community, and rightfully so, would be against prejudgment of disputes in arbitration such that an arbitrator came to a *final* conclusion before all of the submissions were made. Indeed, such:

Prejudgment would seem to impede the very heart of the arbitral process, which presumes a quasi-judicial function of deciding legal claims after weighing evidence and argument. The lack of independence may create an imperfect arbitration, but prejudgment renders the process a sham formality, an unnecessary social cost.²²

Foresight, however, is not prejudgment; rather, it is both non-binding and provisional by nature. This is plain by revisiting the principles espoused in describing the technique.

First, as a mechanism that the parties have mutually agreed to implement, they have empowered the tribunal with the ability to provide such insights and cannot therefore complain later if the tribunal decides to exercise such authority.

Second, the critique assumes that arbitrators do not maintain any position on the issues before them until all of the evidence has been submitted, the hearing held, and the final award being written. For a diligent arbitrator, this is certainly not the case; in fact, it is more likely that the tribunal’s positions are constantly evolving throughout the proceedings. Does that point undercut Foresight? No, because Foresight would provide a single snapshot in time that is informed by the submissions made by the parties thus far. Therefore, Foresight would incentivize counsel to provide their most compelling arguments and evidence *earlier* in the process so that if an application for Foresight is received, then their client will be cast in a more favorable light.

²⁰ 6(1) BCDR International Arbitration Review 93-106 (2019), <https://doi.org/10.54648/bcdr2021006> (accessed August 16, 2025).

²¹ R. Feehily, Neutrality, Independence and Impartiality in International Commercial Arbitration: A Fine Balance in the Quest for Arbitral Justice, 7 J. Int’l & Comp. Arb. 1 (February 2019).

²² W.W. Park, Arbitrator Integrity: The Transient and the Permanent, 46 San Diego L. Rev. 3 (2009).

Naturally then, both parties would understand where they are currently placed before the tribunal and the things that they would be best served in addressing should the matter continue, and whether the case should continue at all.

As a final note as to arbitrator bias, as things currently stand in international arbitration, the tribunal already does have their opinions on certain matters before they issue the award. They may well discuss these issues among themselves throughout the proceedings and may cultivate their opinions on certain issues. These informal perspectives are not prejudicial merely for existing and do not magically amount to bias merely because the parties become aware of the tribunal's *preliminary* perspective. To the contrary, the entire process is enhanced by transparency because the parties are able to peer into the future to see how the case might go for them and what they can do to adjust their fates.

8 Opportunity to Fully Present Their Case

By its operation, Foresight does not prevent any party from fully pleading its case. If the parties do not resolve their dispute, then the process will follow its usual course to the issuance of an award. As referenced in the previous section, prejudgment is already a basis for disqualifying an arbitrator. If an arbitrator were to already have an immovable position on any point, regardless of what the parties submit to them, that person would be unfit to serve as an arbitrator and would be a jeopardy to the award.

Foresight embodies just the opposite notion. It says with clarity to the parties: *this is a preliminary perspective at a singular point in time and could be subject to change*. Whatever decisions a party makes after such insight would be solely their own in how they want to plead their case. Furthermore, they may well be more able to effectively present their case, understanding how the tribunal is responding to the pleadings thus far.

V Conclusion

1 Already Existing Forms of Arbitral Foresight

In addition to further imagining the role of the arbitrator in arbitral proceedings, the coining of the term “Arbitral Foresight” is the evolutionary manifestation of similar discussions about similar attributes from other voices in the field.

One example is in the 2018 Prague Rules at Article 2.4,²³ which provide that the arbitral tribunal:

“may at the case management conference or at any later stage of the arbitration, if it deems it appropriate, indicate to the parties:

...

“its preliminary perspectives on:

- i. the allocation of the burden of proof between the parties;
- ii. the relief sought;
- iii. the disputed issues; and
- iv. the weight and relevance of evidence submitted by the parties.

Expressing such preliminary perspectives shall not by itself be considered as evidence of the arbitral tribunal’s lack of independence or impartiality, and cannot constitute grounds for disqualification.”

Notably, the primary distinction between the Prague Rules’ expression of arbitrator facilitation and Foresight is the party triggering the tribunal to provide its preliminary perspectives. By placing that duty with one or both parties, even if one party objects, there is little room to suggest that the tribunal is acting outside of its mandate.

The rules from the Centre for Effective Dispute Resolution (“CEDR”) at Article 5 also provide a framework for arbitrator facilitation which tracks many of the tenants described herein.²⁴

Further still, some national legal regimes already empower judges to provide preliminary perspectives of the submissions before them, for example, the German “Güteverhandlung” process,²⁵ or the Swiss “Referentenaudienz.”²⁶ In each of those examples, not only do the judges provide their opinions before the final submissions before the parties but the litigants also

²³ Rules on the Efficient Conduct of Proceedings in International Arbitration (Prague Rules), December 14, 2018.

²⁴ Centre for Effective Dispute Resolution, Arbitration Rules (2021), <https://www.cedr.com/alternative-dispute-resolution-processes/arbitration/rules/> (accessed August 16, 2025).

²⁵ J.H. Langbein, “The German Advantage in Civil Procedure,” 52 U. Chi. L. Rev. 823 (1985).

²⁶ A. Kozmenko and L. Grosel, “Settlement Facilitation by the Arbitral Tribunal: A Swiss Perspective,” Arbitration.ru (February 1, 2021), <https://journal.arbitration.ru/analytics/settlement-facilitation-by-the-arbitral-tribunal-a-swiss-perspective/> (accessed August 16, 2025).

welcome these perspectives as they give a weighted push for the parties down the path of settlement rather than protracted legal proceedings. Even in common law jurisdictions, there has been a trend toward judges using pre-trial conferences to actively resolve disputes. In these instances, national courts in the United States²⁷ and in the United Kingdom²⁸ are encouraged to actively manage their cases.

2 Summary

In the television gameshow *Deal or No Deal*, contestants try their hand at selecting cases, attempting to find the one that has USD 1 million. After every few selections, they get a call from the mysterious “Banker” who attempts to get them to stop playing in exchange for his offer. The Banker’s offer is never binding, and the contestant could play to their benefit, and sometimes to their detriment. The point is that at each milestone in the game, they were given off-ramps to end it. Arbitration in its current iteration is stuck in the quagmire of often being too slow and too expensive for what clients want.

Foresight is a solution. It is a response to the ever-increasing chorus of demands for a more efficient world of dispute resolution. No client is pleased to be in arbitration, and while it is understood that commercial disputes are part of the cost of doing business, most clients are ever searching for ways to resolve disputes and cut cost and time.

It is appreciated that there are legitimate concerns as to jeopardizing the award with prejudgment or the infection of arbitrator bias. However, these are already sins that if an arbitrator is prone to, they would be likely to commit regardless of the attributes of Foresight. In addition, due process is not harmed by Foresight. This superpower of Foresight is something that goes to the heart of why tribunals are constituted in the first place, to assist the parties in resolving their dispute.

²⁷ Pursuant to 18 C.F.R. § 385.603 (2024).

²⁸ Hogan Loveels, Alternative Dispute Resolution in England and Wales (October 2017).