wgs

The Sedona Conference

Principles for International Arbitration

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

May 2025
Public Comment Version
Submit comments by July 7, 2025,
to comments@sedonaconference.org

Principles for International Arbitration

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

MAY 2025 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Contributing Editors

H. Christopher Boehning
Ross Gotler
Chuck Kellner
Kathleen Paisley
Chuck Ragan

Steering Committee Liaisons

Hon. James Francis (ret.)
Taylor Hoffman
Eric P. Mandel
Wayne Matus

Staff Editors

David Lumia
Michael Pomarico

Preface

Welcome to the public comment version of The Sedona Conference's *Principles for International Arbitration* ("*Principles*"), a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, data security and privacy law, and artificial intelligence. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG6 is to develop principles, guidance, and best practice recommendations for information governance, discovery, and disclosure involving cross-border data transfers related to civil litigation, dispute resolution, and internal and civil regulatory investigations.

The Sedona Conference thanks Contributing Editors Chris Boehning, Ross Gotler, Chuck Kellner, Kathleen Paisley, and Chuck Ragan for their contributions, and Judge James Francis, Taylor Hoffman, Eric Mandel and Wayne Matus for their guidance and input as Steering Committee liaisons to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of *Principles* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of *Principles* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of *Principles* is open for public comment, and suggestions for improvement are welcome. Please submit comments by July 7, 2025, to comments@sedona conference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, trade secrets, and artificial intelligence. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Kenneth J. Withers
Executive Director
The Sedona Conference
May 2025

Table of Contents

PRINCIPLES FOR INTERNATIONAL ARBITRATION

Principle 1. During the course of an arbitration, Arbitral Participants should adopt a reasonable, cooperative, and proportionate approach to complying with all Data Protection Laws applicable to the proceedings while at the same time respecting the rights of the parties and their interests in the fair and efficient conduct of the proceedings.

Principle 2. The exchange of Documents and Evidence in International Arbitration should be minimized and narrowly tailored to the Documents and Evidence that are relevant to a party's claim or defense, nonduplicative, and material to the resolution of the matter. Disclosure should be undertaken in compliance with the Data Protection Laws as applied in a reasonable and proportionate manner, balancing the rights of the Data Subject and relevant third parties with those of the Arbitral Participants, reflecting the consensual nature of International Arbitration, and in consideration of the efficiency goal of the process (including cost and time), confidentiality, privacy, and enforceability.

Principle 3. An agreement between the parties as to the scope of document disclosure should be respected by an Arbitral Tribunal, provided their agreement is consistent with Principles 1 and 2.

Principle 4. **W**here document disclosure is considered appropriate, and the parties are not able to agree on the scope of the disclosure, or if the agreement they propose is inconsistent with Principles 1 or 2, the Arbitral Tribunal should apply Principles 1 and 2 in deciding the extent of disclosure to be ordered.

Principle 5. Applying Data Protection Laws to arbitration proceedings may require the Arbitral Tribunal to issue binding Data Protection Directions on the parties applicable to the Data Protection Laws at issue. The Arbitral Tribunal should consider issuing such directions after judging the parties' conduct under a standard of good faith, reasonableness, and proportionality, taking into account the considerations in Principles 1–4. While not binding on them, courts and Data Protection Authorities should respect and give reasonable deference to the decisions of the Arbitral Tribunal[1] as to the application of Data Protection Laws to the Processing of Protected Data in International Arbitrations.

1. Here, Arbitral Tribunal refers to the panel in its decision-making capacity (please see the formal definition of the term "Arbitral Tribunal" in Section II, *infra*). We note, however, that the arbitral institutions may establish rules and controls impacting privacy interests and should be guided by these principles as well.

Principle 6. Arbitral Participants should put in place technical and organizational measures appropriate to ensure a reasonable level of information security of the Documents and Evidence, taking into account the scope and risk of the Processing, the capabilities and regulatory requirements of the Arbitral Participants, the costs of implementation, and the nature of the information being processed or transferred, including whether it includes Protected Data, privileged information, or sensitive commercial, proprietary, or confidential information.

I. INTRODUCTION

The Sedona Conference launched its Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) in July 2005 with a program in Cambridge, England, entitled *International Issues: E-Information Management, Disclosure and Discovery*. In the ensuing years, WG6 has produced more than a dozen publications in furtherance of its mission "to develop principles, guidance and best practice recommendations for information governance, discovery and disclosure involving cross-border data transfers related to civil litigation, dispute resolution and internal and civil regulatory investigations." One significant area of dispute resolution that has not been addressed in those papers is discovery and disclosure in international arbitration. This publication seeks to fill that gap.

International commercial arbitration is a consensual process pursuant to which persons and commercial entities agree that disputes arising out of or relating to their business relationship should be subject to arbitration and exclude or severely limit court jurisdiction. These entities may choose arbitration for a variety of reasons, including certain characteristics of international arbitration that are discussed in Section III of this paper. Two of those features that are important are that arbitration: (1) may be private and (2) is intended to be a more efficient than litigation for resolving disputes.

Because arbitration is a matter of contract, participants are not bound to follow a defined set of rules or procedures, as is generally the case in litigation, but have substantial flexibility to tailor the dispute resolution proceedings—including the law, language, and procedural rules to be applied—to fit the particularities of their matter. However, these issues can also be addressed in the arbitration agreement, which then becomes binding on the parties unless they agree otherwise.

Fact-finding is an essential element of International Arbitration, as in all forms of dispute resolution. Given the global nature of commerce, the fact-finding process in arbitration often implicates the cross-border processing of significant amounts of data. Such data may include Personal or other Protected Data subject to various data protection laws and regulations in jurisdictions throughout the world.

With this background in mind, WG6 offers the *Principles for International Arbitration* ("*Principles*") relating to the secure processing, review, and disclosure of data—particularly Personal or other Protected Data—in the specific context of document disclosure in International Arbitration. The purpose of *Principles* is to suggest a reasonable and proportional approach to the use and protection of data in international arbitration that: (1) respects the data protection and privacy rights of relevant Data Subjects while at the same time recognizing the due process rights of the Arbitral Participants, including the right of parties to adduce evidence material to resolution of the matter; and (2) ensures reasonable and good-faith compliance with Data Protection Laws, while at the same time respecting the quasi-judicial role of International Arbitration and ensuring that arbitral proceedings are not unduly hindered.

The focus of *Principles* is on the cross-border data transfer aspects of International Arbitration. By adopting the suggested approach and striking the appropriate balance, participants in International

Arbitration can mitigate potential conflicts with privacy laws and regulations in the context of cross-border data transfers during International Arbitration Proceedings.

A. Structure of This Publication

Principles starts with a statement of the six Principles of International Arbitration, followed by this Introduction (Section I) and a list of Definitions (Section II). Section III provides background on the characteristics of international commercial arbitration. The core of the paper can be found in Section IV, which addresses the six Principles of International Arbitration and provides commentary for each principle with explanatory guidance. A conclusion follows in Section V.

B. Intended Audience

Principles is primarily addressed to the parties to the arbitration, their legal counsel, the Arbitral Tribunal, any arbitral institution administering the dispute, and any consultants, advisors, or experts retained during the arbitration (collectively "Arbitral Participants," as defined in the Definitions section below).

Principles is additionally addressed to data protection authorities and other enforcement bodies responsible for applying Data Protection Laws throughout the world. Given the important role that arbitration plays in the cross-border administration of justice, it is hoped that supervisory authorities will find *Principles* to be a valuable resource in assessing whether the Arbitral Participants have adequately addressed the rights of Data Subjects and applied data protection principles in their arbitration proceedings.

Principles advances the position that data protection and data disclosure can co-exist in International Arbitration. Data Protection Laws are not antithetical to the core tenets of International Arbitration addressed herein. Arbitral Participants regularly come to agreements to ensure that data processed, disclosed, transferred, and maintained in their arbitration will be subject to rigorous security and confidentiality requirements geared towards compliance with Data Protection Laws. In the same vein, Arbitral Participants often make efforts to minimize disclosure where possible in line with international data minimization principles.

C. Role of Cooperation in International Arbitration

Principles is based on the belief that, through cooperation, Arbitral Participants and Data Protection Authorities can work together to ensure that the rights and needs of both Data Subjects and Arbitral Participants are considered and met. Such cooperation is a hallmark of The Sedona Conference, as

reflected in its widely accepted *Cooperation Proclamation*, published in July 2008,[2] as well as in the subsequent publication, *The Case for Cooperation*.[3]

Accordingly, *Principles* is intended to facilitate the process of cooperation among the Arbitral Participants, and to help chart the course for compliant, efficient, and defensible data processing, review, and disclosure of data in international commercial arbitration proceedings. In doing so, *Principles* is intended to promote and advance the complementary interests of fair adjudication and data protection.[4]

D. Rejecting the Weaponization of Data Protection Laws

Some aspects of *Principles* are worth highlighting at the outset. First, Arbitral Participants and Data Protection Authorities should take care to ensure that Data Protection Laws are not used as a shield to prevent the disclosure of key information in the course of an International Arbitration. Rather, when data-related disputes arise, *Principles* urges that Arbitral Participants work together in good faith to find practical solutions based on the reasonable and proportional needs of the individuals involved, ensuring that the rights of Data Subjects are respected, and that material information is not withheld from the Arbitral Tribunal so as to impair its ability to fairly adjudicate the matter. Key considerations in doing so may include: (1) the risk to the Data Subject were the data to be processed and disclosed; (2) the hardship on the Arbitral Participants were the data to be withheld; (3) the categories and scope of the data at issue, including whether it contains Personal Data, "special or sensitive category" data, or criminal offense data; and (4) the protections in place and mitigating measures available to ensure the data will be kept secure and confidential, preventing further processing or onward transfer.

2. The Sedona Conference, *Cooperation Proclamation* (2008), 10 SEDONA CONF. J. 331 (2009 Supp.), *available at* https://thesedonaconference.org/publication/The_Sedona_Conference_Cooperation_Proclamation (calling upon adversaries to work collaboratively during the discovery phase of litigation as a means of reducing costs and delays). These tenets can and should also be applied in the context of International Arbitration.

3. The Sedona Conference, *The Case for Cooperation*, 10 SEDONA CONF. J 339, 344 (2009 Supp.) (observing that "cooperation is not in conflict with the concept of zealous advocacy. Cooperation is not capitulation.").

4. While the *Principles for International Arbitration* ("*Principles*") is principally intended to guide Arbitral Participants partaking in international commercial arbitration, it is anticipated that it also will be a valuable resource to parties in bilateral investment treaty arbitration, mediation procedures, and other related contexts, including arbitrations between parties from a single country for which cross-border transfers of personal information may be necessary or appropriate.

II. DEFINITIONS

The following definitions apply throughout the *Principles for International Arbitration*:

"**Arbitral Participants**" means the parties to the arbitration, their legal counsel, the Arbitral Tribunal, any arbitral institution administering the dispute, and any consultants, advisors, or experts retained during the arbitration.

"Arbitral Tribunal" means the panel of adjudicators (arbitrators) convened to hear and resolve a dispute submitted for International Arbitration. The Arbitrational Tribunal is distinguished from the arbitral institution (e.g., ICC, LCIA, JAMS, ICDR, and AAA).[5]

"**Data Controller**" means the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means for the processing, transfer, and disclosure of Protected Data. For the purposes of *Principles*, it is assumed that Arbitral Participants are Data Controllers or joint controllers for at least some of these activities during International Arbitration proceedings.

"**Data Protection Authorities**" means any person or entity charged with enforcing Data Protection Laws.

"**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 Laws**" means any law or regulation—regardless of whether it takes the form of a Data Protection Law, a privacy regulation, a blocking statute, or other protection—that addresses the processing of Personal Data, including appropriate usage, transfer, or disclosure of data; requires safeguarding data; or imposes obligations in the event of compromises to the security or confidentiality of data.

"**Data Subject**" means any person or entity whose Protected Data is or may be processed, transferred, or otherwise disclosed.

"**Documents and Evidence**" means documents, electronically stored information ("ESI"), and any other relevant evidence that may be exchanged during an International Arbitration (as defined below).

5. ICC is formally known as the International Chamber of Commerce, International Court of Arbitration; LCIA is the London Court of International Arbitration; the arbitral institution "JAMS" was originally named Judicial Arbitration and Mediation Services; ICDR is the International Centre for Dispute Resolution—the international division of the American Arbitration Association (AAA).

"**International Arbitration**" means an arbitration procedure whereby the parties to a cross-border dispute agree either by contract or another legally binding mechanism to submit disputes that may arise between them to an Arbitral Tribunal for decision.

"**Personal Data**" means any data that reasonably relates, directly or indirectly, to an identified or identifiable natural person.

"**Processing**" includes any operation, activity, use, or application performed upon Protected Data by automatic or other means, such as, for example, alteration, collection, disclosure, processing, recording, storage, retrieval, transfer, or use.

"**Protected Data**" is any data irrespective of its form (e.g., paper, electronically stored information, images, etc.) that is subject to Data Protection Laws, including, but not limited to, Personal Data.

III. CHARACTERISTICS OF INTERNATIONAL ARBITRATION

This section is included for the benefit of Arbitral Participants who may be new to International Arbitration and to explain the context from which *Principles* emerges. This section serves as background only, and readers are also referred to the ICCA-IBA Roadmap on Data Protection in International Arbitration,[6] and to the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration.[7]

International Arbitration is a method of dispute resolution that is often chosen as an alternative to resolving a dispute in court. This includes both:

- commercial disputes, where the parties are engaged in commercial activities and agree that any disputes arising from those commercial activities will be subject to arbitration; and

- investor-state disputes, where an investor brings a claim pursuant to a treaty—these claims are often, but not always, administered by international organizations.[8]

Important features of International Arbitration are:

- the centrality of consent, in that parties must have agreed to resolve the dispute by arbitration (in the case of investor-state arbitration, this consent is found in a treaty);

- the importance of due process to the enforceability of awards;

- its neutrality and flexibility, since the parties to commercial disputes can choose the law under which to resolve the dispute, the language in which to conduct the proceedings, and the procedural rules to be applied during the proceedings that are typically selected in the arbitration agreement and become binding on the parties unless amended (in the case of investor-state arbitration, this freedom is circumscribed by the treaty);

- an emphasis on party autonomy, including the ability to tailor the proceedings to fit the particularities of the case and often allowing participation in the selection of the

5. International Council for Commercial Arbitration ("ICCA"), The ICCA Reports No. 7: The ICCA-IBA Roadmap to Data Protection in International Arbitration (2022), *available at:* https://www.arbitration-icca.org/icca-reports-no-7-icca-iba-roadmap-data-protection-international-arbitration.

6. ICCA, THE ICCA REPORTS NO. 6: ICCA-NYC BAR-CPR PROTOCOL ON CYBERSECURITY IN INTERNATIONAL ARBITRATION (2022), *available at:* https://www.arbitration-icca.org/icca-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration. ICCA is an acronym for the International Council for Commercial Arbitration; NYC references the New York City Bar Association; and CPR refers to the International Institute for Conflict Prevention and Resolution.

7. Different legal instruments may have different definitions of an international organization. Pursuant to the European Union's General Data Protection Regulation ("GDPR") Art. 4(26), "international organization" means an organization and its subordinate bodies governed by public international law, or any other body that is set up by, or on the basis of, an agreement between two or more countries.

arbitrator(s), which is typically addressed in the arbitration agreement and becomes binding on the parties unless amended (in the case of investor-state arbitration, this autonomy is circumscribed by the treaty);

- the ability to conduct private and often confidential proceedings in commercial disputes and to limit the disclosure of Personal and Protected Data in the award (in some cases investor-state arbitrations are resolved with some degree of transparency to the public);

- the importance of efficiency;

- the parties' fundamental right to present and prove their respective cases, which includes gathering and producing evidence, and in certain instances obtaining evidence from other parties; and

- fair and equitable treatment of the parties.

A. Type of Arbitration Proceedings

As noted above, *Principles* addresses two types of International Arbitration proceedings (i.e., commercial and investor-state). The type of arbitration, however, does not determine whether Data Protection Laws apply. That issue is determined by whether the data Processing falls within the material and jurisdictional scope of the relevant laws. *Principles,* therefore, does not distinguish between international commercial and investor-state arbitrations; also, *Principles* may be applied to other types of International Arbitration as appropriate, even though not specifically called out within.

1. Commercial Arbitration

Consent is fundamental to arbitration. International commercial arbitration is undertaken pursuant to the agreement of the parties. The parties may include an agreement to arbitrate in their business contract or enter into a separate agreement after a dispute arises. In either event, the agreement may refer to a set of arbitration rules, in which case those rules will govern the proceeding. Generally, proceedings take place before a tribunal made up of a sole arbitrator or a panel of three arbitrators.

In applying Data Protection Laws to arbitration, it will be important to recall that the Arbitral Participants are all required to comply with the arbitration agreement, including any arbitration rules referred to therein, provided that in doing so, they comply with mandatory principles of law, including Data Protection Laws.

2. Investor-State (or Treaty) Arbitration

International Arbitration may be carried out on the basis of an agreement to arbitrate contained in a treaty rather than a contract between two commercial entities. The dispute under a treaty may, for example, be between an investor and a state, or between two states.

While investor-state arbitration is conducted on a different legal basis than commercial arbitration, this does not, in principle, alter the way that Data Protection Laws apply to the Arbitral Participants unless this is expressly provided for in the Data Protection Law.

However, when the dispute is administered by an international organization, which is often the case in investor-state arbitration, the Data Protection Laws may exclude international organizations from its scope. Furthermore, the host country agreement and the privileges and immunities of the international organization in question generally contain special rules, pursuant to which the international organization itself, and potentially others, may be immune from or fall outside the scope of the otherwise applicable Data Protection Laws.

This must be determined on a case-by-case basis and for each Arbitral Participant individually. Moreover, even when Data Protection Laws do not apply, the international organization may have its own data protection policy.

B. Ad Hoc versus Administered Arbitration

International commercial or treaty arbitration may be conducted under the auspices of an arbitral institution or international organization or on an ad hoc basis without any administering institution, although even ad hoc arbitrations may use an arbitral institution or international organization to hold funds or assist with the appointment of arbitrators.

It is more common for arbitrations to be administered, which implies that an arbitral institution or international organization provides administrative support and some degree of oversight and review of awards. The extent of oversight and review varies greatly among institutions and international organizations. Moreover, some institutions provide secure online data platforms to facilitate the exchange of information during the arbitration process.

C. Enforceability

One of the main benefits of International Arbitration is that, unlike judgments of national courts in matters involving parties from different nation-states, International Arbitration awards are widely enforceable under international treaties, most notably the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention") and the Washington Convention on the Settlement of Investment Disputes between States and Nationals of Other States (the "Washington Convention").

The New York Convention is an international treaty providing that the contracting states will enforce arbitration awards rendered in other contracting states unless the award runs afoul of one of the few listed bases for the refusal of enforcement. Bases for the refusal of enforcement focus on the agreement to arbitrate and the arbitrability of the subject matter, and enforcement can be denied if the award has been set aside at the arbitral seat (with some exceptions) or if enforcement would otherwise be contrary to the public policy of the enforcing state. This latter basis is often used to argue that awards resulting from proceedings that lacked due process or violated the right to be heard or to apply fair and equitable treatment to the parties should not be enforced, although in practice these arguments are rarely successful in overturning an arbitral award. At the time of

publication, 172 states were parties to the New York Convention,[9] which makes the enforcement of awards under its terms essential to the fabric of International Arbitration.

The Washington Convention also provides an enforcement mechanism for investor-state awards issued under the Washington Convention. International Centre for Settlement of Investment Disputes (ICSID) awards are "automatically" enforceable as a judgment of the national courts in any contracting state, unless annulled in accordance with the procedure set forth in the Washington Convention. The bases for annulment are even more narrow than those set forth in the New York Convention.

D. Applicable Law

In any given arbitration, different legal regimes may be applicable or relevant to different aspects of the case. By way of example, in the context of a hypothetical International Arbitration:

- the governing law of the contract underlying the parties' dispute may be English law;
- the legal seat of the arbitration may be Geneva, bringing in the application of Swiss law to the procedural aspects of the arbitration;
- the parties to the arbitration may be established in the U.S. and in Brazil, with regulatory and other reporting requirements under the relevant local laws;
- the parties' legal counsel will be subject to both legal and professional obligations (including regarding privilege) in the jurisdiction(s) where they are admitted to practice;
- the Arbitral Participants are all required to comply with applicable economic sanctions and money-laundering laws and regulations; and
- the Arbitral Participants are all required to comply with the Data Protection Laws and regulations applicable to them.

All of these legal regimes constrain the behavior of the Arbitral Participants. In particular, the law of the legal seat of the arbitration places procedural constraints on the proceedings and the arbitrators. If the law at the legal seat is not respected, the award is at risk of being vacated or refused enforcement under the New York Convention.

As demonstrated by the above hypothetical, data protection is just one of several applicable laws to be taken into account by Arbitral Participants. As with compliance with sanctions and money laundering regulations, compliance with Data Protection Laws is mandatory and part of the legal landscape in which arbitrations are being conducted.

---

8. *Contracting States*, NEW YORK CONVENTION, https://www.newyorkconvention.org/contracting-states (last visited Dec. 19, 2024).

Most Data Protection Laws do not expressly address their application to arbitration. That is why it is important to think through and document the solutions adopted within the framework of whatever Data Protection Laws apply to a given proceeding, in order to (1) demonstrate compliance efforts if challenged, (2) defend the Arbitral Participants' good-faith efforts in the event of an unintended data protection breach or cybersecurity incident, and (3) minimize disruption to the proceeding by anticipating and resolving issues early on and ensuring agreement on those solutions among Arbitral Participants.

E. Conduct of Proceedings

International Arbitrations are conducted according to procedures and principles drawn from a mix of legal traditions, of both common law and civil law backgrounds. However, notwithstanding the diversity of the Arbitral Participants and the laws and procedures under which they may be conducted, international commercial arbitral proceedings have developed a certain level of uniformity in recent years.

The arbitration usually begins with a demand or request for arbitration. If the arbitration agreement provides for an arbitral institution, that institution and its rules typically govern the submission of additional preliminary pleadings and appointment of arbitrators.

One of the commonalities in International Arbitration that has developed in recent years is an early meeting of the Arbitral Participants to specify the procedure and timeline to be applied during the proceedings, including how evidence is adduced.

The Processing of evidence in an International Arbitration typically starts with the parties, who, before lodging a claim, will typically gather the facts and the evidence supporting those facts. This evidence is then transferred to their legal counsel, who will determine which of those facts and evidence to present to a tribunal in support of their party's case.

Proceedings often include a "disclosure" process, in which each party may request documents from the other(s) that are relevant to their own case and material to resolution of the matter, following which disclosure may take place voluntarily or as ordered by the tribunal. Following disclosure, a more limited group of further evidence may be submitted by each party to the tribunal as proof of its case.

As information submitted in an International Arbitration will often contain Protected Data, the gathering, Processing, production, and adducing of evidence needs to be squared with the rights of the Data Subjects who are identified in or are identifiable through the evidence, while at the same time recognizing the due process rights of the parties to the disputes. Parties should also consider that the arbitration award itself may contain Protected Data. These principles must be reconciled in a manner that is reasonable and proportionate to the rights at issue.

It is a general principle of arbitration that each party has the burden of proving its claims in the manner that it sees fit, within the applicable arbitration agreement and the law and under the control of the Arbitral Tribunal. In presenting its case, a party will typically submit written, and in many cases oral, evidence in support of it. That evidence may take many forms, such as written statements

by a witness of fact, the opinion of an expert, or written evidence including business documents, correspondence, emails, images, or video. In its award, the Arbitral Tribunal decides whether each party has discharged its burden of proof in relation to the allegations made.

The documentary and other evidence exchanged in International Arbitration proceedings will typically exceed that which would be exchanged in typical civil law or Islamic (Sharia) court proceedings, but it may be less than that exchanged in common law courts, particularly in the United States under broad rules of civil procedure for discovery. This middle ground between the various legal systems reflects that International Arbitration involves parties from different legal traditions who have chosen arbitration over public, civil litigation as an arguably more efficient dispute resolution method.

F. Due Process, Fair and Equitable Treatment, and the Right to be Heard

Due process is the all-encompassing obligation of a tribunal to ensure procedural fairness. Due process requirements are enshrined in most, if not all, modern legal systems, arbitration rules, national arbitration laws, and the New York Convention.

An important due process requirement is affording all parties to the arbitration an opportunity to present their case, also referred to as the "right to be heard." This includes giving the parties notice of and access to the same information about the proceedings, the opportunity to and reasonable time in which to make submissions of evidence and legal arguments, and allowing them the opportunity to respond to the submissions of the other party(ies). The right to be heard generally encompasses a party's right to be represented by the legal counsel of its choice and to be heard by an independent and impartial tribunal. Moreover, the tribunal's decision cannot be based on grounds that the parties did not have an opportunity to address.

Another component of due process is the right to fair and equitable treatment. Many arbitration rules and national arbitration laws explicitly require that parties to an arbitration be treated equitably, and it is crucial in International Arbitration that no party has an unfair advantage.

Where legally allowed, these fundamental due process rights of the parties may be considered in deciding how the Data Protection Laws are to be applied to Arbitral Participants in International Arbitration proceedings, provided that the rights of Data Subjects are adequately protected. Due process, fair and equitable treatment, and the right to be heard require a tribunal to enable the parties to present their cases and the evidence supporting them. At the same time, Arbitral Participants must respect and comply with applicable Data Protection Laws ensuring that the rights of Data Subjects are protected.

G. Party Autonomy

The principle of party autonomy is an important reason parties opt for arbitration, as it allows them to tailor the proceedings to the particularities of the dispute and the needs of the parties. Under this principle, parties enjoy a considerable degree of freedom to agree as to how the arbitral process should be structured and conducted. Indeed, under the New York Convention an arbitral award

may be denied recognition if the proceedings that led to the award were conducted in a manner that is not in accordance with the parties' agreement.

Where parties do not agree on matters related to the conduct of proceedings, the Arbitral Tribunal generally has broad discretion in deciding those issues. In addition, party autonomy may be limited by mandatory provisions of the law of the legal seat of the arbitration. Failure to comply with such provisions may result in setting aside the award and/or refusal of enforcement. Such mandatory rules often include the fundamental principles of due process, fair and equitable treatment, and the right to be heard, described above. Moreover, party autonomy is restricted by mandatory principles of the substantive law applicable to the arbitration, which will often include Data Protection Laws.

H. Procedural Efficiency

The efficiency of arbitral proceedings over litigation may be one reason to choose International Arbitration; it is an effort to avoid unnecessary procedures and costs that come with standard litigation in public courts. Accordingly, the arbitrators should consider procedures that will not cause undue delay or create unnecessary complexity. Data Protection Laws should be applied in this context to International Arbitration, while protecting the rights of Data Subjects impacted by the proceeding. Unless properly managed, the strict application of some of the principles of Data Protection Law could lead to a significant expenditure of time and resources. Data protection principles incorporated into applicable Data Protection Laws should therefore be applied reasonably and proportionately, having due regard for the efficiency of the proceedings.

I. Privacy and Confidentiality

International Arbitration proceedings are not accessible to the public or third parties, reducing the probability of public disclosure of Protected Data.[10] However, in limited situations, information disclosed in a proceeding and, especially arbitration awards, may be further disclosed. Due to the consensual nature of commercial arbitration, the parties can agree that strict confidentiality obligations will apply to everyone involved in the proceedings. Where agreement is not possible, the Tribunal can issue a protective order. The consideration of protective orders is encouraged to address these situations and may be able to reduce the risk of disclosure of Protected Data. Privacy and confidentiality are often highly valued by commercial parties, who may not wish their disputes to be heard in an open, publicly accessible courtroom because of commercially sensitive information (e.g., trade secrets and cost/pricing information), the wish to limit damage (e.g., reputational), and the desire to enhance the efficient resolution of the dispute.

In the context of commercial arbitration, the award may be intended to remain confidential. Even in confidential arbitrations, however, there is a risk that the award will become public if it is enforced in a country where awards (or parts thereof) become public in the enforcement process. Furthermore, arbitral institutions increasingly publish awards and other decisions (or excerpts thereof) as a matter of course, unless the parties object.

9. Investor-state arbitrations are typically public, and thus a noted exception.

In the context of investor-state arbitration, given the involvement of state actors, case materials such as pleadings, submissions, procedural orders, decisions, and awards are often published. This is because in treaty arbitration, there generally is a greater desire for transparency, especially where public interests are at stake.

It is foreseeable in international commercial or investor-state arbitrations that, as with some courts, public access to proceedings and published materials may unavoidably expose some Personal Data. Depending on the obligations of the Arbitral Participants under the applicable Data Protection Law, it may, therefore. be necessary for the Arbitral Tribunal or the arbitral institution to require proactive measures to protect that Personal Data in filings (e.g., by means of redaction).

IV. PRINCIPLES OF INTERNATIONAL ARBITRATION AND COMMENTARIES

Principle 1. During the course of an arbitration, Arbitral Participants should adopt a reasonable, cooperative, and proportionate approach to complying with all Data Protection Laws applicable to their proceedings, while at the same time respecting the rights of the parties and their interests in the efficient conduct of the proceedings.

Comment

Principle 1 recognizes that tension can exist between disclosure in International Arbitration and Data Protection Laws. Arbitral Participants should be aware of obligations triggered by applicable Data Protection Laws and should apply them in a reasonable and proportionate manner that respects the rights of Data Subjects and third parties while at the same time respecting the rights of the Arbitral Participants, the integrity of the proceedings, and the need for the proper, prompt, and efficient administration of justice through arbitration.

The Arbitral Participants should consider compliance with Data Protection Laws that are applicable to the proceedings or to any Data Subjects at issue in their proceedings—as well as compliance obligations under those Data Protection Laws, which are usually of mandatory application and apply alongside the applicable arbitration rules to both international commercial and investor-state arbitrations. Such consideration should take place no later than the organizational meeting conducted early in the arbitration to establish the procedural guidelines and timetable for the proceedings in order to ensure compliance.

When balancing compliance with Data Protection Laws with the parties' due process and efficiency interests, Principle 1 encourages the Arbitral Participants to consider, among other things:

A. the scale, extent, and nature of the Personal Data, "special category" data, data relating to a child, or criminal offense data being Processed and the lawful basis for the Processing;

B. the degree of risk to the rights and interests of Data Subjects from the Processing of their Personal Data, taking into account the extent to which various privacy, confidentiality, and security protections and mitigating measures have been put in place to anonymize, secure, or otherwise limit this risk and the extent to which the Data Subjects have been notified of and given an opportunity to challenge the Processing;

C. the potential impact on the rights and interests of the parties to the International Arbitration and third parties were the data to be withheld, taking into account whether the information sought via disclosure could be obtained through other, less invasive means;

D. whether cross-border transfers will be required for the orderly conduct of the proceedings and whether measures have been, or may be, taken to provide a lawful

basis for any such transfers (for example, Standard Contractual Clauses under the EU General Data Protection Regulation ("GDPR")); and

E. the protections in place to ensure that the data is and will be kept secure and confidential throughout the arbitral proceedings, and whether any other mitigating measures, such as redaction or pseudonymization of Personal Data, could be put in place to enhance such protections.

Principle 2. The exchange of Documents and Evidence in International Arbitration should be minimized and narrowly tailored to the Documents and Evidence that are relevant to a party's claim or defense, nonduplicative, and material to the resolution of the matter. Disclosure should be undertaken in compliance with the Data Protection Laws as applied in a reasonable and proportionate manner, balancing the rights of the Data Subject and relevant third parties with those of the Arbitral Participants, reflecting the consensual nature of International Arbitration, and in consideration of the efficiency goal of the process (including cost and time), confidentiality, privacy, and enforceability.

Comment

Arbitration is a means to resolve disputes different from and as an alternative to litigation. For common law countries, one difference between arbitration and litigation is that prehearing discovery or disclosure of information is generally more limited in scope in arbitration. In International Arbitration, prehearing disclosure of information is even more limited, in part because some participants come from countries where no prehearing disclosure occurs; indeed, some arbitral rules discourage prehearing disclosure requests.

The following recommendations are designed to further the objectives embodied in Principle 2:

A. International Arbitration is undertaken by contracting parties seeking to reach a resolution that is fair and equitable, in accordance with applicable law, and can be enforced globally under applicable law and international treaties. Where possible, it is, and should be, a substantially cooperative endeavor.

B. International Arbitration should be cost effective and time efficient. Core issues are, and should be, quickly identified and evaluated. Arbitral Participants should not waste resources on ancillary issues.

C. Personal Data should not be subject to unnecessary Processing, disclosure, or transfer, especially when it contains Protected Data.

D. International Arbitration is private and can be made substantially confidential. Where confidentiality attaches, the privacy of the Arbitral Participants is, and should be, recognized and respected. This may be mandated when the International Arbitration is subject to the Data Protection Laws.

A significant obstacle to the achievement of these benefits occurs where expansive disclosure of Documents and Evidence of possible relevance to the disputes is permitted without sufficient justification under Principles 1 and 2. With the proliferation of electronic communications in recent years, the extent of available Documents and Evidence (especially ESI) has grown exponentially, as have party disagreements related to their collection and exchange. Compounding this problem, the rules and practice governing the exchange of Documents and Evidence—including the Data Protection Laws applicable to such exchange—vary widely across jurisdictions throughout the world.

Moreover, tension may exist between the private nature of arbitrations and the transparency requirements to Data Subjects under some Data Protection Laws. Parties, especially those who frequently are part of International Arbitration, may consider addressing this through ensuring that the applicable privacy notices or processes include appropriate references to the potential use of Protected Data in such proceedings.

Acknowledging these obstacles, Principle 2 encourages parties to work together in International Arbitration to scope the exchange of Documents and Evidence to that which is nonduplicative, relevant, material to resolution of the dispute, and proportional to the needs of the matter. In doing so, Principle 2 recognizes two fundamental tenets governing the exchange of Documents and Evidence in International Arbitrations:

A. The Documents and Evidence Processed in International Arbitrations, including any Protected Data contained therein, should be minimized.

1. Parties should engage in targeted collection efforts, and to the extent feasible should collect and exchange only unique and nonduplicative Documents and Evidence that are relevant and material to the resolution of the dispute.

2. To the extent that parties must collect and exchange Protected Data, such data should be limited to that which is proportional to the needs of the dispute and that which is necessary and cannot be obtained from other sources.

B. To the extent available and consistent with the efficiency goal of the process (including cost and time), the Arbitral Participants are encouraged to leverage technology solutions during the proceedings, including for the disclosure and management of Documents and Evidence, where applicable.

1. Technology solutions may facilitate compliance with Data Protection Laws during the International Arbitration by minimizing the scale of Documents and Evidence to be collected and exchanged, enabling pseudonymization or redaction of Protected Data where possible, tracking and minimizing cross-border transfers of Protected Data, securing Documents and Evidence including Protected Data on secure servers with advanced data security infrastructures, and ensuring timely destruction of Documents and Evidence.

2. Assuming access to such solutions is equally available to the parties, widespread use of modern electronic discovery tools, such as technology-assisted review, should be encouraged, where appropriate. Such tools may include predictive coding, assisted review, centralized storage platforms, and analytics tools including, for example, email threading and concept clustering.

3. The Arbitral Participants should also consider leveraging technology solutions to secure their Documents and Evidence during collection, Processing, and disclosure, to ensure the timely and secure destruction of Documents and Evidence once proceedings have closed, and generally to comply with Data Protection Laws and

protect the privacy rights of relevant Data Subjects. For example, where possible, the parties should maintain Documents and Evidence only on secure servers, rely on third-party data processors with advanced data security infrastructures, and employ technology solutions that can assist in identifying and, where necessary, redacting or otherwise protecting Personal Data.

4. The parties should agree on appropriate formats for production that, where possible, include a text-searchable load file. Additionally, they should agree on a production protocol listing the metadata fields to be produced with Documents and Evidence and the kinds of Protected Data to be redacted.

Principle 3. An agreement between the parties as to the scope of document disclosure should be respected by an Arbitral Tribunal, provided their agreement is consistent with Principles 1 and 2.

Comment

Principle 3 recognizes that party consent and autonomy are hallmarks of International Arbitration, facilitating the benefits that make it an appealing mechanism of dispute resolution. Accordingly, and consistent with *The Sedona Conference Cooperation Proclamation*, Principle 3 encourages parties to come to an agreement as to the scope of disclosure that conforms with the tenets recognized in Principles 1 and 2. In particular, such disclosure should be limited to that which is lawful, necessary, and proportional to the needs of the dispute, so as to ensure cost-effectiveness and efficiency and foster the principles of data minimization.

Should the parties reach such an agreement falling within Principles 1 and 2, the Arbitral Tribunal should respect it—while working with the parties to improve it where possible and appropriate to optimize arbitral efficiencies and avoid waste of resources—and ensure that it is followed throughout the arbitration process.

Principle 4. Where document disclosure is considered appropriate, and the parties are not able to agree on the scope of the disclosure, or if the agreement they propose is inconsistent with Principles 1 or 2, the Arbitral Tribunal should apply Principles 1 and 2 in deciding the extent of disclosure to be ordered.

Comment

This Principle recognizes that tension may exist between pure party autonomy and the goal of efficiency. To the extent that parties are unable to come to an agreement as to the scope of disclosure consistent with Principles 1 and 2, Principle 4 encourages Arbitral Tribunals to take steps to limit disclosure to that which is consistent with Principles 1 and 2, as appropriate considering the needs of the particular proceeding. For example, unless explicitly precluded from doing so by the parties' arbitration agreement, Arbitral Tribunals should consider requiring requesting parties to:

A. describe their requests with specificity and narrowly tailor requests so that they are directly tied, and material, to a particular claim or defense and its resolution;

B. restrict requests to specific custodians;

C. restrict requests to specific time periods;

D. limit the number of requests; and

E. minimize the Processing of Protected Data where possible.

Additionally, the Arbitral Participants should utilize methods to limit obtrusive requests for disclosure—for example, by imposing limits against requests that seek data that a) is in the hands of the party making the request, b) is not readily or reasonably available, or c) would impose an undue burden or expense, or implementing a protocol to shift or allocate to the requesting party the costs of an expensive undertaking to acquire such data.

Arbitral Participants should avoid overly broad requests for "any and all documents" on a subject. While parties might even agree on an expansive approach to disclosure, such a broad scope would be inconsistent with the goals of Principles 1, 2, and 4 and may be incompatible with applicable Data Protection Laws. Arbitral Tribunals should consider prohibiting such disclosure unless the requesting party can explain why the requested information is relevant to the claims or defenses, would be material to a resolution of a claim or defense, and proportional to the needs of the proceeding. They may also require requesting parties to affirm that their requests are not interposed for an improper purpose—such as extending the proceedings or increasing the costs—and allow responding parties the opportunity to object on the specific grounds that a request is overbroad, irrelevant, unduly burdensome or costly, subject to a valid privilege, or disallowed under applicable Data Protection Laws.

Another technique the Arbitral Tribunal may use to encourage reasonable and proportionate disclosure of relevant documents is to invite the parties themselves (in addition to their counsel) to

attend case management conferences where the issues are discussed so that there is transparency about the potential costs and burdens of disclosure.

Arbitral Tribunals should also be wary of potential attempts by parties to weaponize the Data Protection Laws by using them as a shield to prevent disclosure of damaging information or to otherwise disrupt the arbitral process. For example, when a party refuses to produce Documents and Evidence that have been ordered by the Arbitral Tribunal, arbitrators may use their discretion and power to draw adverse inferences and, where necessary as a last resort, impose sanctions.

Using these techniques strikes an appropriate balance among the principles of party autonomy, arbitral efficiency, and respect for the privacy interests of Data Subjects and Arbitral Participants. To achieve these objectives, at the outset of an International Arbitration, the Arbitral Participants should have an open dialogue about the data Processing and disclosure protocols to be followed during the arbitration. For example, a disclosure schedule and information security and data breach protocol should be established and should leverage data security advancements, data minimization principles, and document review technologies, when appropriate, to ensure that review and disclosure processes are responsibly and efficiently handled in compliance with applicable Data Protection Laws. The appropriate balance can be achieved by adopting a procedural order, terms of reference, or data protection protocol to ensure orderly proceedings.

Such schedules and protocols should consider, among other things:

A. which Data Protection Laws should be applied to the arbitration (recognizing that multiple Data Protection Laws may apply);

B. necessary categories of Personal Data to be processed and disclosed (if any) during the course of the arbitration, as well as the lawful bases for Processing and disclosing the information;

C. which Arbitral Participants will be considered the controllers of the data and how they will oversee any data processors (recognizing that multiple Arbitral Participants may be considered controllers);

D. whether cross-border transfers will be required during the review and disclosure process and, if so, how adequate protections will be guaranteed and under what legitimizing transfer mechanism, if applicable; and

E. the document review and retention protocols that will be implemented to ensure the efficient review and timely destruction of data.

To the extent that the parties cannot agree on data review and disclosure protocols—or are unable to resolve disputes related to data review and disclosure on their own—the Arbitral Tribunal should step in and, in the process, ensure that the rights of all parties are respected and the rights of Data Subjects under applicable Data Protection Laws are proportionally considered in the context of the particular case.

Principle 5. Applying Data Protection Laws to arbitration proceedings may require the Arbitral Tribunal to issue binding Data Protection Directions on the parties applicable to the Data Protection Laws at issue. The Arbitral Tribunal should consider issuing such directions after judging the parties' conduct under a standard of good faith, reasonableness, and proportionality, taking into account the considerations in Principles 1-4. While not binding on them, courts and Data Protection Authorities should respect and give reasonable deference to the decisions of the Arbitral Tribunal as to the application of Data Protection Laws to the Processing of Protected Data in International Arbitrations.

Comment

The nature of International Arbitration, as mentioned in Section III.H., above, is such that the Arbitral Tribunal must have the authority to issue binding directives on the parties with respect to the procedure and substance of the dispute. In a case where Data Protection Laws apply, this may require the Arbitral Tribunal to decide how data protection compliance will be addressed. These decisions should be enshrined in written Data Protection Directions in an agreed upon form that are binding on the parties. Provided those decisions are made in good faith and are reasonable, courts and Data Protection Authorities should respect those decisions and give them reasonable deference.[11]

Accordingly, Principle 5 encourages any Arbitral Participant that considers itself bound by a Data Protection Law to inform the other Arbitral Participants as soon as practicable during the proceedings to permit the arbitration to be undertaken in a manner that will maximize data protection compliance while minimizing impacts or burdens on the arbitration. To the extent that other Arbitral Participants do not believe a Data Protection Law applies, they should promptly object to the application. The Arbitration Tribunal should be considered as having the authority to rule on such issues of applicability, and the Arbitral Participants should respect such rulings.

Arbitral Participants may not be subject to the same Data Protection Laws, and some participants may not be subject to any Data Protection Law at all. Moreover, parties may seek to use data protection compliance obligations to their advantage. Principle 5 recognizes the importance of addressing and documenting the resolution of data protection issues that may arise during an International Arbitration in written Data Protection Directions applicable to the specific matter. Addressing these issues early in writing, where possible, will enable better compliance while reducing the burden on the orderly conduct of the arbitral proceedings.

Principle 5 also recognizes the importance of Arbitral Participants maintaining a record of their data protection compliance efforts in a manner that can be shared with Data Protection Authorities, demonstrating that data protection obligations have been addressed and that reasonable, good-faith

10. With that being said, Principle 5 in no way suggests that Arbitral Participants can or should proceed with data Processing activities inconsistent with Data Protection Laws. Where necessary pursuant to applicable Laws, Arbitral Participants should seek approvals from Data Protection Authorities regarding Processing activities and, in any event, they should always carefully consider their obligations under Data Protection Laws.

efforts have been made to institute data protection safeguards during the arbitration proceedings. Data Protection Directions should address the following topics, where appropriate:

A. The lawful basis for data Processing.

B. The lawful basis for data transfer.

C. The exchange of Documents and Evidence.

D. Any data security requirements and data breach protocols.

E. Management of Data Subject rights.

F. Notification obligations.

G. Documentation of data protection compliance.

H. Any use of online case management platforms to assist with data management and data protection compliance.

Principle 6. Arbitral Participants should put in place technical and organizational measures appropriate to ensure a reasonable level of information security of the Documents and Evidence, taking into account the scope and risk of the Processing, the capabilities and regulatory requirements of the Arbitral Participants, the costs of implementation, and the nature of the information being Processed or transferred, including whether it includes Protected Data, privileged information, or sensitive commercial, proprietary, or confidential information.

Comment

Principle 6 contextualizes information security as encompassing the measures that the Arbitral Participants should consider taking to minimize the risks of both unauthorized disclosures of data and cyberattacks. It, therefore, encourages the Arbitral Participants to adopt a protocol to manage information security and promote compliance with Data Protection Laws.

Among the measures that Principle 6 encourages the Arbitral Participants to consider including in such an information security and data breach protocol, in a manner consistent with the other Principles, are the following:

A. Procedural and operational controls to limit access to and proliferation of Protected Data, consistent with industry standards for information governance, data retention, and data destruction.

B. Technical controls including, but not limited to, strong password protocols, data security awareness training, access controls, encryption of data in transit and at rest, redaction, anonymization, or pseudonymization of Protected Data.

C. Minimization or restriction of uses or transport of unencrypted removable media such as USB stick drives, CDs, DVDs, and external hard drives.

D. Centralization of communications, data storage, and collaboration tools to software applications and service providers with appropriate data security and procedural certifications.

E. Preventative and mitigating cyberattack controls including, but not limited to, encryption, perimeter integrity, operational monitoring, incident response, and insurance coverage.

V. CONCLUSION

The six Principles of International Arbitration presented in this publication address the secure processing, review, and disclosure of data—particularly Personal or other Protected Data—in the specific context of document disclosure in international commercial arbitration. The Principles are intended to provide a reasonable and proportional approach to the use and protection of data in international arbitration that: (1) respects the data protection and privacy rights of relevant Data Subjects while at the same time recognizing the due process rights of the Arbitral Participants, including the right of parties to adduce evidence material to resolution of the matter; and (2) ensures reasonable and good-faith compliance with Data Protection Laws, while simultaneously respecting the quasi-judicial role of International Arbitration and ensuring that arbitral proceedings are not unduly hindered. By adopting these six Principles of International Arbitration, participants can better mitigate potential conflicts with privacy laws and regulations in the context of cross-border data transfers during International Arbitration proceedings.