ICCA
INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION

The ICCA–IBA Roadmap to Data Protection in International Arbitration

Public Consultation Draft
February 2020 – Not for Citation

with the assistance of the
Permanent Court of Arbitration
Peace Palace, The Hague

The ICCA Reports No. 7

Contents

MEMBERS OF THE ICCA-IBA JOINT TASK FORCE

Co-Chairs

Kathleen Paisley, Brussels, New York

Melanie van Leeuwen, Derains & Gharavi

Members

Lawrence Akka QC, 20 Essex Street

Rosa Barcelo, Squire Patton Boggs

Niuscha Bassiri, Hanotiau & van den Berg

Lisa Bingham, ICCA

Markus Burianski, White & Case

Hugh Carlson, Three Crowns

Daniel Cooper, Covington & Burling LLP

Javier Fernández-Samaniego, Samaniego Law

Hilary Heilbron QC, Brick Court Chambers

Robert Maddox, Debevoise & Plimpton

Charlie Morgan, Herbert Smith Freehills LLP

Philippe Pinsolle, Quinn Emanuel Urquhart & Sullivan LLP

Jacques de Werra, University of Geneva

Acknowledgments

The Task Force received the invaluable assistance and input of its rapporteurs:

Emily Hay, Hanotiau & van den Berg

Brianna Gorence, Freshfields Bruckhaus Deringer

INTRODUCTION

This ICCA-IBA Roadmap to Data Protection in International Arbitration ("**Roadmap**") has been developed by the ICCA-IBA Task Force on Data Protection in International Arbitration to help arbitration professionals better understand the data protection and privacy obligations to which they may be subject in relation to international arbitration proceedings.

A. Data Protection and Arbitration

Data protection laws and regulations are generally of mandatory application. The entry into force of the European Union's ("**EU"**)[1] General Data Protection Regulation[2] ("**GDPR**") in May 2018 and similar laws in other jurisdictions[3] caused corporates and organisations to review their data collection, retention, processing and security policies. 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 or EUR 20 million, whichever is higher[4]), it is important for arbitration professionals to consider what data they process, where, by what means, with which information security measures and for how long.

Although most data protection laws apply to arbitration, they do not address *how* they should be applied to arbitration. In the absence of specific guidance, it is important to think through the steps of the arbitral process and document the measures adopted in the different phases of an arbitration within the framework of whatever data protection law(s) apply. To that end, this

[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. According to the terms of the Withdrawal Agreement, the GDPR applies in the UK for the time being and as a practical matter the GDPR will apply to the UK until a further decision is taken, which will occur at 31 December 2020 at the earliest and the terms of which are uncertain.

[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 9 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 need to be considered, too. 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, Rec. 10). Annex 9 also includes a list of the data protection laws of the EU Member States.

[4] Under the Brazilian General Data Protection Act (Statute 13709/18) ("LGPD"), the fines may be up to 2% of gross revenue in Brazil or R$50 million. Under a proposed personal data protection law in India, penalties prescribed for data controllers are linked to global turnover in certain cases for serious offences. The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. ("CCPA") similarly provides for monetary penalties: depending on the violation occurred, the penalty may be up to $2,500 for each violation or $7,500 for each international violation. In addition, and unlike the GDPR and LGPD, the CCPA does not provide a maximum amount of penalty.

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 individuals and legal entities. An arbitration, as such, is not subject to data protection obligations. However, it is important to appreciate that even if 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.

"Accountability" is a central feature of the GDPR and other modern data protection laws. It requires those who process personal data to document the approach and measures they have taken towards compliance. 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 compliance.

B. Intended Scope and Purpose of the Roadmap

Types of Proceedings. The type of arbitration (for example, commercial or investor-State) does not determine whether data protection laws apply. Rather, whether data protection laws apply is determined by whether the data processing falls within the material and jurisdictional scope of the relevant law.[5]

Arbitral Participants. This Roadmap is only addressed to **Arbitral Participants**, which is defined in this Roadmap as including the parties, their legal counsel, the arbitrators and arbitral institutions (only). 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, court reporters, translation services, 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:

- where an Arbitral Participant is a legal entity,[6] employees of that entity are not considered separately for compliance purposes, rather their actions are attributed to that entity; and
- where arbitration-related information containing regulated personal data is shared with a third party,[7] this is considered to be processing, which requires compliance with data processing rules and transfer restrictions.

[5] While data protection laws also apply to professionals and entities involved in mediation and forms of alternative dispute resolution, they are not addressed in this Roadmap. 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] That 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 (Art. 4(7) GDPR).

[7] 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).

General Data Protection Principles. The Roadmap addresses data protection compliance in international arbitration under general data protection principles, rather than the law of a particular jurisdiction (unless otherwise indicated by way of illustration). However, the Annexes and the examples provided in the Roadmap focus on the GDPR because it is one of the most comprehensive and onerous data protection regulations in force to date and has been widely drawn upon by jurisdictions outside the EU (including Brazil and the state of California), as a result of which it is becoming a global reference.

Roadmap Organisation. The Roadmap is divided into two sections:

- Section I describes the primary data protection principles potentially applicable to international arbitration; and

- Section II addresses how the data protection principles described in Section I may apply during the different stages of an international arbitration, and how they may affect the Arbitral Participants during the arbitral process.

The Roadmap is accompanied by a set of Annexes that provide greater detail, practical information, checklists, references aimed at enabling Arbitral Participants to apply data protection principles in the context of an arbitration and a glossary of data protection notions, which are also defined in the footnotes. Practice tips are provided throughout the Roadmap and gathered for ease of reference in Annex 2, while a more detailed checklist is provided in Annex 3 addressing how to operationalise the practice tips.

Goal. The aim of this Roadmap is to enable Arbitral Participants to identify and effectively address data protection issues in the context of arbitral proceedings; not to suggest that the process is so complicated that they should be daunted by the prospect. There are sensible solutions to the data protection challenges that arise in arbitrations, and Arbitral Participants will soon become familiar with the issues and accustomed to dealing with them.

No Legal Advice. Importantly, nothing in this Roadmap or Annexes can be taken as legal advice. This Roadmap provides information and resources to foster a better general understanding of data protection and the Arbitral Participants' obligations. However, assessing data protection obligations is a fact- and case-specific undertaking. In case of doubt, Arbitral Participants may wish to obtain legal advice.

The Roadmap and its Annexes will necessarily be a living document. It is hoped that over time, data protection authorities and courts will clarify how data protection laws should be applied to international arbitration, whilst recognizing 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 modern data protection laws as applied to international arbitration. The European Union, Brazil,[8] India,[9] and the State of California[10] are used as examples to give context, however, similar principles apply under many other modern data protection regimes (major exceptions being China, Russia and parts of the United States unless the entity has signed up to the Privacy Shield).[11] For the avoidance of doubt, references to specific legislation or to a jurisdiction serve as an indication only, and should not be read as legal advice.

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. The extent of these obligations will depend on the applicable law and the Arbitral Participant's status under that law as a data controller or a data processor. For data controllers, these obligations typically include issuing GDPR-compliant data privacy notices, ensuring the lawfulness of their personal data processing and transfers, minimizing the personal data they process, and adopting appropriate data security measures, data breach procedures, data retention policies, and procedures for addressing data subject complaints.[12]

Given the interlinking nature of these obligations and the potential risk of non-compliance, Arbitral Participants should consider taking out insurance, as well as imposing insurance obligations and indemnities on each other through the use of a data protection protocol[13] or other instrument. There are insurance products available that may enable Arbitral Participants to mitigate their risks. Coverage may also be available as part of, or as an add-on to, professional liability insurance taken out by lawyers and others. At this relatively early stage and in the absence of experience with lengthy claims, it has not proved easy for insurers to properly quantify the risk, and as a result, premiums vary substantially.[14]

---

[8] *See* LGBD, fn. 4.

[9] India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011. ("Indian Act"). The Indian Act addresses data protection in certain contexts and for certain types of data but Indian has also proposed a comprehensive data protection law, which is not yet in force.

[10] *See* CCPA, fn. 4.

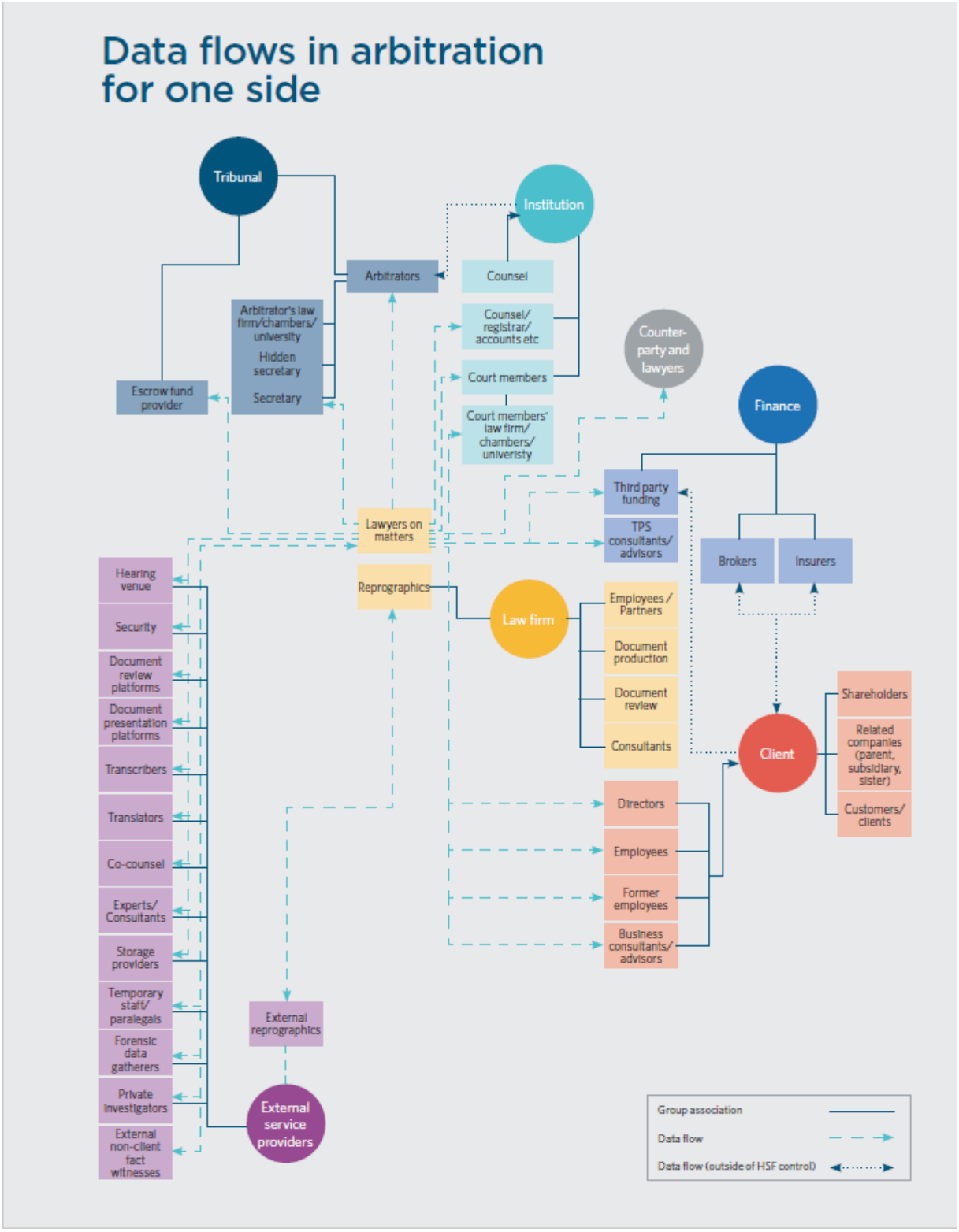
[11] 'Privacy Shield' refers to the EU-US Privacy Shield Framework, designed by the US Department of Commerce and the European Commission to provide a basis for data transfers with adequate data protection from the EU to the US (https://www.privacyshield.gov/welcome).

[12] *See* e.g. Annex 3, which provides a checklist of data protection issues that parties and their counsel may want to consider.

[13] 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.

[14] There is some debate about whether regulatory fines can be insured against. That is clearly a matter for the applicable law. In certain jurisdictions it is considered illegal, contrary to morals or public policy, to allow an individual or entity to insure against such fines. It is therefore not uncommon for policies to be sold on the basis that they will cover fines "to the extent allowed by law." For similar reasons, it may not be possible for contracting parties to provide that one will indemnify the other against fines if incurred.

Data Flows. The following chart depicts typical data flows in an international arbitration and reveals how extensive and interconnected they are:[15]



[15] 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.

A. Material Scope of Data Protection Laws

Modern 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"[16], "processing"[17] and "data subjects"[18] is 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 in the context of an arbitration by Arbitral Participants.

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; LGPD, Art. 5, I; and CCPA Sections 1798.140(b) and (o)[19]).

[16] '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;" LGPD, Art. 5(I).

[17] '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 (GDPR Art. 4(2)); any operation carried out with 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 (LGPD Art. 5(X)).

[18] '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 (LGPD Art. 5(V)).

[19] While the definition of "personal information" under the CCPA is substantially similar to "personal data" under the GPDR, the CCPA does not define personal information as extending 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.

A substantial portion of the information exchanged during a typical international arbitration is likely to contain data that qualifies as personal data. Under many laws, including the GDPR and the LGPD, 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 law.

2. Data Subject

The individuals who are identified or identifiable are referred to as "data subjects" -- legal entities are not data subjects. [20]

3. Processing

Data protection laws impose obligations that must be complied with whenever personal data is "processed." Processing is defined broadly 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 Rec. 15, Art. 2(1))[21] or similar means (*e.g.*, LGPD Art. 1).[22] 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 modern 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 (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, 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. This leads to significant scope creep, even beyond the already broad territorial reach

[20] *See* fn 15.
[21] A 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (GDPR Art. 4(6)).
[22] "This Act provides for the processing of personal data, including by digital means…" (LGPD Art. 1).

of the GDPR. Similar provisions are found in numerous other modern data protection laws throughout the world. [23]

Example:

An EU-based arbitrator is appointed to an arbitration administered by a non-EU based institution, together with two other arbitrators from outside the EU who are not otherwise subject to the GDPR. Legal counsel are all established outside the EU and are also not otherwise subject to the GDPR. The EU-based arbitrator will be subject to 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 making transfers of personal data outside the EU in connection with the arbitration.

Depending on the circumstances, this may involve putting in place the European Commission-approved standard contractual clauses with the fellow arbitrators, or relying on the derogation to the GDPR's third country transfer restrictions for transfers "necessary for the establishment, exercise or defence of legal claims," which also requires that efforts be made to ensure the data is protected after the transfer.[24] This may have the practical result that the non-EU based Arbitral Participant agrees to be bound by the main provisions of the GDPR in order to allow the transfer of data.

C. Roles under Data Protection Laws

Arbitral Participants covered by a modern data protection regime have obligations under the data protection laws that apply to their data processing activities. The extent of these obligations depends on the Arbitral Participant's status under the applicable data protection law as a

[23] The LGPD, 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 (iii) the personal data subject to processing has been collected on Brazilian territory (LGPD, Art. 3). The CCPA applies to organizations "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).

[24] 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. 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)); and (3) an exception to the right to erasure or to stop processing (GDPR Art. 17(3)(e)).

controller (who often will be acting in parallel with other independent controllers), a joint controller acting jointly with other controllers,[25] or a processor.[26]

1. Data Controllers

Under modern data protection laws, the data controller is primarily responsible for compliance and demonstrating compliance. Data controllers can be natural or legal persons, irrespective of whether they are for profit or not,[27] private law or public law entities and their size.

A data controller determines "the purposes and means of the processing of personal data" (see, e.g., GDPR Art. 4(7); LGPD, Art. 5(VI)). Applying this definition, most Arbitral Participants are likely to be considered data controllers for their processing (but not that of others) 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. For example, both barristers[28] and solicitors[29] are considered to be data controllers by relevant data protection authorities in the EU and the UK.

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. This means that in any given arbitration there will be multiple data controllers and others bound by data protection laws in relation to the same personal data. Each has individual responsibility and potentially joint responsibility to ensure the protection of that personal data, which obligations are not restricted to the first person or entity that obtains the data from the data subject.

> ***Example:***
>
> To prepare a claim, a party collects documents containing personal data that it provides to its outside legal counsel. 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

[25] 'Joint controllers' are where two or more controllers jointly determine the "purposes and means" of the data processing (GDPR 26(1)).
[26] 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)).
[27] An exception being California where the CCPA only extends to controllers that are for-profit.
[28] 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 an independent 'controllers' when processing data in the course of legally representing their client." Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor", WP 169, 16 February 2010, at 29. Emphasis added.
[29] The ICO is the UK Information Commissioner's Office set up to uphold information rights, including under data protection law. It is the UK's national supervisory authority established pursuant to GDPR, Article 51. The ICO has taken the view that solicitors are data controllers. EU Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', WP 169, 16 February 2010, at 28; ICO, 'Data controllers and data processors: what the difference is and what the governance implications are', Data Protection Act 1998, ¶¶ 40-43.

their duties, the institution and arbitrators process the personal data contained therein. In this scenario, under modern data protection laws, the party, its legal counsel, the institution and the arbitrators are all likely to be data controllers and thus subject to the rules established in the applicable data protection laws for data controllers. Their potentially overlapping individual compliance responsibilities create competing obligations that need to be reconciled. This is further complicated by the fact that some Arbitral Participants may not be subject to the data protection laws at all and may be hesitant to agree. In order to address these issue in the context of an arbitration a data protection protocol may be used. See Annex 4.

2. Data Processors

Data 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)).[30] Under modern data protection law, 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 following criteria must be met:

(1) act under the instruction of a data controller in undertaking their tasks;
(2) not being responsible for deciding the purposes and means of the data processing; and
(3) 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 arbitration context, Arbitral Participants will therefore rarely qualify as data processors because their function is such that they control the purposes and means of the processing.

However, an Arbitral Participant may wish to engage a third party that it wants to be considered a data processor, in which case they should ensure that the controller retains control over the purposes and means of the processing and that a compliant data processing agreement be put in place.[31]

Tribunal secretaries, e-discovery professionals, transcribers, interpreters and other vendors may be considered data processors, depending on who directs the purposes and the means of the processing, as well as whether the right to process can be withdrawn at any time. Moreover, the nature of the relationship may be such that obtaining a GDPR compliant data processing agreement is difficult.

[30] A similar definition of data processor is found on LGPD Art. 5(VII): "natural person or legal entity, of public or private law, that processes personal data in the name of the controller".
[31] *See* GDPR Art. 28 (3) for the requirements for a GDPR-compliant data processing agreement.

3. Joint Controllers

Following relevant case law in the EU under its predecessor legislative instrument, the Data Protection Directive[32], the GDPR has introduced the concept of "joint controllers" who "jointly" determine the "purposes and means" of the data processing.[33] 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. This concept is also found in the LGPD, but not in many older data protection laws.[34] In the case where Arbitral Participants are joint controllers, they are required to make arrangements to allocate the risks involved, for example through a data protection protocol.

In the arbitration context, to establish whether Arbitral Participants are (i) controllers, who are likely to be acting alongside other controllers with parallel responsibilities, or (ii) 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 processing. Although not related to arbitration, recent decisions of the European Court of Justice (CJEU) under the Data Protection Directive indicate that the notion of joint controllership is broadly interpreted. However, the liability of a joint controller is limited to the processing for which that controller "actually determines the purposes and means", and does not extend to the overall chain of processing for which it does not determine the purposes and means.[35] The possibility of shared or parallel responsibility of Arbitral Participants bears out the importance of data protection compliance by all Arbitral Participants.

D. Data Transfer Rules

One of the most obvious ways that the data protection laws apply to international arbitrations is through the restrictions on data transfers between jurisdictions.

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.

Third country data transfer is inherent to the international arbitration process. Modern data protection laws restrict the transfer of data to third countries with the goal of ensuring that legal obligations are not circumvented by the transfer of data to jurisdictions where the standard of protection of personal data is lower. The same restrictions may also apply to data transfers to international organisations, as is the case in the EU.[36] Some countries, including China and

[32] 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").
[33] GDPR Art. 26(1).
[34] The LGPD provides that "controllers who are directly involved in the treatment of which damage has occurred to the data subject are jointly and severally liable …"(LGPD Art. 42, Paragraph 1, II).
[35] *See* Judgment of 29 July 2019, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629, ¶¶ 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.
[36] GDPR, Chapter V.

Russia, apply a more stringent transfer regime, essentially prohibiting most data transfers out of the jurisdiction.

Modern data protection laws require a lawful basis for third country data transfers, as well as for processing. By way of example, there 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 adequate data protection (*i.e.*, it is the subject of an "adequacy decision")[37];

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" **[Annex 7]**;[38]

3. Third, in case 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

4. Lastly, if none of the express derogations is applicable, a party may rely on its "compelling legitimate interests" as a basis for transfer, which, however, 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.[39]

Importantly, regardless of the lawful basis for the third country transfer, "any transfer of personal data which [is] undergoing processing or [is] intended for processing after transfer ... shall take place only if… [a]ll provisions in this Chapter [are] applied in order to ensure that

[37] An 'adequacy decision' refers to a decision by the European Commission made by reference to a set of criteria to the effect 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 Art. 45(1)).

[38] The standard contractual clauses include obligations such as (1) an undertaking by the data exporter that the data has been collected, processed and transferred in compliance with applicable law, (2) an undertaking by the data importer that it has appropriate technical and organisational measures in place to protect the data, (3) any third party given access by the data importer must also respect and maintain the confidentiality and security of the data, (4) the data importer must make its data processing facilities available for audit or certification by the data exporter where reasonably requested, (4) an obligation on the data importer to comply with specific data protection principles, (5) a right of data subjects to enforce certain clauses as third party beneficiaries, and (6) an obligation on both parties to abide by a decision of a competent court or final decision of a competent supervisory authority from the data exporter's country of establishment. **[Annex 7]**

[39] EDPB, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679', 6 February 2018 ("Data Transfer Guidance").

the level of protection of natural persons guaranteed by this Regulation is not undermined" (GDPR Art. 44).[40]

Applying these requirements to a typical arbitration, the first point to keep in mind is that the transfer rules, like all data protection principles, apply to the Arbitral Participants, not to the arbitration as such. This means that each Arbitral Participant that is required to make transfers to other jurisdictions in the context of an arbitration will need to consider what data transfer restrictions apply to them and what the standard of protection is in the jurisdiction to which they intend to transfer the data. Under the GDPR, they would need to consider the following:

- Does the country to which transfer would be made have an adequacy decision? For example, data transfers from the EU to a party in the US that has signed up to the Privacy Shield (only), Canada (commercial entities only), Switzerland or Japan are lawful because they have been declared to be adequate jurisdictions;[41]

- If not, is it possible to put appropriate safeguards in place? For example, data transfers from the EU to an arbitrator based in the United States are lawful if the arbitrator is willing to enter into standard contractual clauses;

- If not, 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 transfer, requires the third country transfers to be "occasional", "necessary for the establishment, exercise or defence of legal claims" and applied in a manner that "ensure[s] that the level of protection of natural persons guaranteed by this Regulation is not undermined" (*e.g.*, GDPR Art. 44-49, Rec. 111). Moreover, advice from the EU Working Party suggests that the personal data should be minimised in advance of the transfer, including culling for relevance, redaction or pseudonymisation of personal data, and confidentially provisions should be entered into.[42]

- If not, is there a compelling legitimate interest in the data being transferred, in which 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.

[40] Under Indian data protection laws, if sensitive personal data is contemplated to be transferred to third countries, then the data transferor can do so only if necessary for performance of a lawful contract, or if the individual has consented to such transfer. The data transferor should also provide in the contract that the data transferee ensures at least the same level of data protection as is maintained by the transferor under applicable Indian data protection laws.

[41] The European Union considers that the data protection laws of Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, 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. **[Annex 9]**

[42] Document Disclosure Guidance, at 10-11.

It is even more difficult to transfer data out of jurisdictions that have localisation regimes, including China and Russia. The reference to localisation refers to the fact that in principle certain types of data, often including personal data, cannot be transferred abroad.

Example:

In an arbitration between a Brazilian and a French company under the rules of an EU institution, arbitrators are appointed from the EU, Brazil and the USA. The EU institution and EU arbitrator will have to comply with the GDPR's data transfer restrictions for data transfer to the Brazilian and USA based arbitrators. Moreover, the Brazilian arbitrator will have to comply with the data transfer restrictions in the LGPD 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.

Practice Tip:

Third Country Data Transfers – 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 could 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.

E. 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 modern data protection laws adopted around the world[43]:

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 legal basis for it.

2. **Proportionality**: The data protection laws should be applied in a proportionate manner, taking into consideration the rights and interests of the data subject, the rights and interests of parties to the arbitration and those of third parties and the need for a fair and efficient administration of justice.

[43] 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 LGPD. *See, eg,* 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).

3. **Data minimization**: The amount of personal data must be limited to what is necessary for the purpose of the 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.

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 organizational security measures to protect the personal data against the risks involved in processing.

8. **Transparency**: Data subjects have a right to information regarding the processing of their personal data, which includes the right to be notified about the processing of their personal data.

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. Personal data may only be processed if there is a legal basis for it.

a) Fairness

The notion of fairness in data protection law aims to ensure that personal data is processed only in ways that data subjects would reasonably expect. The data subject's expectations in this respect are framed by how the personal data was obtained, whether they have been notified, if notice was given, what purpose for the processing was notified to them, and 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 whether the data subject, whose data is processed during the arbitration, could have anticipated the processing in view of how it was collected and the notices given, as well as whether processing will have adverse effects on the data subject that are not justified by the needs of the processing for 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 placing a document on the record 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/pseudomonization may be required in certain circumstances).

b) Lawfulness

The nature of the arbitral process is such that significant amounts of information is exchanged between Arbitral Participants, often across borders, all of which may contain personal data (sometimes including sensitive[44] 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, such exchange of information must be lawful under the applicable data protection laws.

Under most modern data protection laws, for processing of personal data to be lawful, a specific legal ground for the processing must exist, the so-called 'lawful basis' for processing.[45] There are a number of lawful bases available depending on the purpose of the processing and the controller's relation to the data subject.

In most jurisdictions, including in the EU, there is no universal legal basis for lawful processing in the context of arbitration. Rather, the decision as to which legal basis to rely on for processing purposes in 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

[44] The GDPR refers to 'special category 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 LGPD Art. 5(II). The processing of this 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)). The hypotheses for the lawful processing of sensitive data in Brazil are provided for in LBPG Art. 11.

[45] The CCPA 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* CCPA Section 1798.120.

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 is not processed in a manner that is unlawful generally (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. However, 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.[46] Although the arbitral community frequently relies on consent for other purposes, it is generally problematic to rely on consent as a legal basis for the processing or transfer of personal or sensitive data in the context of an arbitration. The EU Working Party has referred to consent as a "false good solution."[47]

It is not recommended to rely upon consent as a lawful basis for the processing or transfer of personal data 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 invalid ground as a legal basis; 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.

Due to the inherent risk that consent is refused or withdrawn at some point, it is 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. By contrast, in other countries like India, consent is the primary basis for data processing[48]. 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 are generally not advised.

Some data protection laws have created a specific legal basis to allow the processing of data in arbitral proceedings. According to the LGPD Articles 7(VI) and 11(II, d), for example, processing of personal data, including sensitive data, is expressly authorized **"**for the regular exercise of rights in judicial, administrative or arbitration procedures." 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 personal data processing (and does not refer expressly to arbitration although its coverage is broad enough to include arbitration).

---

[46] '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 (GDPR Art. 4(11)). A similar definition is found in LGPD Art. 5(XII).

[47] 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.

[48] *See* Indian Act, fn. 9.

In the EU, the following bases are generally best suited to data processing in the context of international arbitration under the GDPR:[49]

- **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 his/her personal data.[50] For example, the data subject 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 we refer to as the "legal claims derogation".[51] The legal claims derogation will often be the preferred basis for processing sensitive data. It may apply to allow 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.

- **Criminal Convictions and Offences, or Related Security Measures.** In addition to requiring a lawful basis for the processing,[52] 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 an supervising authority or if the processing is authorized, by Union or Member State law.

When relying upon legitimate interests for processing or personal data, the GDPR requires a Legitimate Interests Assessment to be undertaken and recorded (see Annex 5 for a checklist), which is to be updated if events occur that might affect the original assessment. If issues are raised about the processing of personal data during the arbitration, it will be important to be able to show the competent authority that a Legitimate Interests Assessment was undertaken contemporaneously.

Example:

The parties present documents and evidence including submissions, work-related emails, witness statements, contracts and other materials identifying individuals. All the information identifying or allowing individuals to be identified constitutes personal data. Note that the entire document will often not be personal data, but only the words, phrases or parts of the document relating to the data subject. This distinction is important in the

[49] 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.
[50] 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 **[Link Annex 5]**
[51] GDPR Art. 9(2)(f).
[52] GDPR Art. 6(1).

context of document production, as data protection requirements would rarely justify withholding a document in its entirety if any personal data which cannot be disclosed could be redacted.

Practice Tip:

Lawful Basis - 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 or data related to children, and further how any data relating to criminal convictions, offences or related security measures can be processed. Some data protection laws have established a specific legal basis for data processing of personal data and/or sensitive data for arbitration. This is the case in Brazil, and for sensitive data under the GDPR, where there is a legal basis in the context of 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 be undertaken (as is the case for personal data under the GDPR). **[Annex 5].** Reliance on consent should be avoided altogether when another lawful basis is available, but may be required in jurisdictions where the system is primarily based on consent, like India.

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 purposes of processing and the risks posed to the data subject, taking into consideration the nature and extent of the personal data being processed in a proportionate manner (e.g., GDPR, Recital 4, Art. 24). [53] The proportionate approach towards compliance is found throughout most modern data protection laws.

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. Consideration should be given to the type of personal data being presented in the arbitration, what risks the processing for the arbitration poses to the data subject as an individual, what purpose for the processing was notified to them, whether they are involved in the arbitration, how the personal data was collected, and what were/are their expectations about the processing

[53] *See*, for EU, *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 (Dec. 19, 2019); see also Handbook on European Data Protection Law, European Union Agency For Fundamental Rights (2018).

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 a professional email correspondence to 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 risks posed to the data subject is greater from the processing of his/her medical records compared with standard business correspondence. Consideration should also be given to the other rights and interests at stake in the arbitration.

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 the data protection 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. But in all cases, adequate protection must be afforded to the data subject and his or her personal data.

Practice Tip:

Proportionality – The rules established by the data protection laws are intended to be applied in a proportionate manner that respects the data subject's rights taking into consideration the risk posed by the processing (considering, for example, the nature and amount of data being processed and the circumstances), and at the same time respects the rights of third parties. This means in practice that when determining data protection obligations and deciding how to comply, Arbitral Participants may consider the nature of the data being processed and the potential harm for a data subject caused by the processing of their personal data for the arbitration, as well as the rights of the parties being served in the arbitration. In all cases, however, the rights of the data subjects must be afforded adequate protection.

3. *Data Minimisation*

The concept of data minimisation is fundamental to modern 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')".[54]

[54] According to the LGPD Article 18(IV), 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.

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).

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 modern data protection laws, keeping in mind that document production for arbitration is more limited than in litigation.

Example:

A law firm asks their 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 it 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.[55] While the transfer is likely to be lawful on the basis of the legal claims derogation, it may be necessary to consider how the volume of personal data transferred can be minimised prior to the transfer. For example, the EU Working Party has provided guidance in the context of data transfer to the US for purposes of discovery for US litigation, setting out that the data set should be culled for relevance,[56] efforts should be made to redact or pseudonymise personal data[57] and confidentiality provisions put in place where possible before the transfer is made.

[55] Under the GDPR, a 'third country' means any country outside of the European Union and EEA.
[56] 'Culling' means filtering data.
[57] '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. It is similar to redaction but requires that the data subject not be identifiable without additional measures (GDPR Art. 4(5); LGPD Art. 13 Paragraph 4; CCPA 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 must then be limited to the purpose that was notified to the data subject. [58]

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.

The factors to be considered when deciding whether further processing is compatible with the originally notified purpose, under the GDPR, 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. [59]

Deciding whether the purpose is compatible 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 his or her 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 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, [60] unless

[58] 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')."
[59] GDPR, Rec. 50.
[60] Meaning that the processing is "necessary for the establishment, exercise or defence of legal claims".

the data subject has an overriding interest in not having the data processed.[61] 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 LGPD are preserved.[62]

Example:

When the General Counsel was hired at Company X, she was informed that her personal data would be processed where necessary in the normal course of her activities as General Counsel. She has 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 her signature on a contract, minutes of meetings she attended and emails she exchanged. The further processing of her personal data for purposes of the arbitration is within the scope of her function at the company as notified to her. Hence, it would likely fall within the purpose limitation.

5. *Data Subject Rights*

Modern data protection laws, including the GDPR and the LGPD, 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 where there are significant differences among countries with modern data protection regimes.[63]

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

- the right of access and to obtain a copy[64] of the personal data being processed (also referred to as a "data subject access request");[65]

[61] German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680, Section 24.
[62] LGPD Art. 7, Para. 7.
[63] The LGPD Art. 18 lists the main data subject rights in Brazil, including:
I – confirmation of the existence of the processing;
II – access to the data;
III – correction of incomplete, inaccurate or out-of-date data;
IV – anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of the LGPD;
V – portability of the data to another service or product provider, pursuant to the regulation of the supervisory agency, by means of an express request and subject to commercial and industrial secrecy;
VI – erasure of personal data processed with the consent of the data subject;
VII – information about public and private entities with which the controller has shared data;
VIII – information about the possibility of denying consent and the consequences of such denial;
IX – revocation of consent.
[64] GDPR Art. 15(4).
[65] GDPR Art. 15; CCPA Sections 1798.100(d), 1798.110, 1798.115.

- the right to request modification of their data, including the correction of errors and the updating of incomplete information;[66]

- the right to withdraw consent if consent was the basis for processing, which bears out why consent is risky to rely on as a lawful basis, except that "[t]he right to obtain a copy … shall not adversely affect the rights and freedoms of others." [67]

- the right to object to processing where the lawful basis relied upon is a legitimate interest, in which case the controller should demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject;[68] and

- the right to erasure – also referred to as the right to deletion or the right to be forgotten – allows a data subject to request, under certain circumstances, that their personal data be erased.[69]

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.

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), and who believes that his or her data is being processed. These data subject requests will need to be addressed within a prescribed timeframe (30 days under the GDPR) and 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 LGPD, for example, provide that the data subject has the right to obtain from the controller 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. [70]

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

[66] GDPR Art. 16; in contrast to the GDPR, no right of rectification exists under the CCPA.
[67] GDPR Art. 7 (3)
[68] GDPR Art. 21; CCPA Section 1798.120.
[69] GDPR Arts. 12, 17; CCPA Sections 1798.105, 1798.130(a), 1798.145 (g)(3)
[70] *See* GDPR, Recital 63 and Art 15 (4).

copy thereof, provided the provision of electronic access or a copy does "not adversely affect the rights or freedoms of others." [71]

When acceding to a data subject access request Arbitral Participants should carefully consider the impact that meeting the request might have on 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 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 to restrict the onward transfer of any information disclosed in response to the data subject access request.[72] However, the GDPR provides expressly that "the result of those considerations should not be a refusal to provide all information to the data subject."[73]

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 within 30 days, 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)). This may affect whether, and if so, what, documents or document extracts the sub-contractor is provided with. The responding party should also consider whether an exception applies under national law. Considering these issues in advance and defining who has the obligation to address data subject requests, perhaps through a data protection protocol, may help minimise any impact on the process.

[71] *Id.*
[72] *B v General Medical Council [2018] EWCA Civ 1497, 28 June 2018 (UK)*
[73] GDPR, Recital 63 and Art 15 (4).

Practice Tip:

Data Subject Rights – Arbitral Participants should put in place measures to comply with data subject rights, including data subject access requests, update and correction requests. The mechanics of addressing data subject rights should be considered early in the proceedings and potentially addressed in a data protection protocol.

6. *Data Quality*

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.[74] 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 application of a pre-agreed data protection protocol may limit any negative impact the rights request will have on the arbitration.

7. *Data Security*

Modern 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 technical and organisational measures."[75] Deciding what security measures are "appropriate" requires consideration of the potential risk to data subjects, the existing information security measures

[74] See, for example, Art. 5(1)(d) GDPR: "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')".
[75] *See*, GDPR Art. 32.

of the Arbitral Participants, and what physical and technical measures are appropriate given the risks to the data subjects.

By way of example, Article 32 of the GDPR imposes the primary obligation on controllers and processors to ensure that data is processed securely. 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.

The GDPR provides that "appropriate" technical and organisational measures could include, as appropriate:

- 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.[76]

In assessing the appropriate level of security under the GDPR, account shall be taken of the risks that are presented by the processing[77], in particular from:

- accidental or unlawful destruction;
- loss;
- alteration;
- unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[78]

Applying information 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 organisation 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, and the damage or distress that may be caused to the data subject if the personal or sensitive data were to be compromised. In the international arbitration practice, increasingly, these issues are 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 ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitration (2020 Edition)

[76] GDPR Art. 32(1).
[77] Under the LGPD Art. 42, 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.
[78] GDPR Art. 32(2).

[Link] and the IBA Cybersecurity Guidelines (2018) **[Link].** While these initiatives do not address data protection specifically, 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 information 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.

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. He travels frequently, fails to use a screen protector and regularly connects from public wifi and has documents printed at his 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 would likely violate applicable data protection standards.

Practice Tip:

Information Security – Arbitral Participants should apply a proportionate, risk-based approach to information security. They should consider agreeing 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, potentially as part of a data protection protocol, to help manage risk. Reference may be made to the ICCA/NY City Bar/CPR Cybersecurity Protocol for International Arbitration (2020 Edition) **[Link]** and the IBA Cybersecurity Guidelines (2018) **[Link]** where appropriate.

In case information security measures in place fail to prevent a data breach, most modern data protection laws impose notification requirements.

In an arbitration context, it is important to consider the nature of the personal, sensitive, and criminal offence data being processed. It may be that notification is not required where the only personal data being processed for the arbitration is business email and other commercial correspondence and documentation. However, this is a case-specific determination. Even where no notification is compulsory, a record of the breach must be kept.

In the case of the GDPR, for example, data controllers are required 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 (*e.g.*, GDPR Arts. 33-34). The data subjects themselves must also be notified of the breach if the risk to personal data and data subjects from a breach is considered to be "high" (*e.g.*, GDPR Art. 34).[79]

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." [80]

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. The burden to prove the absence of risk in a data breach rests on the data controller (*e.g.*, GDPR Arts. 33-34).

In addition to legal reporting requirements, data breaches raise important questions about when an arbitrator or counsel should inform the parties of a data breach under their general obligations as an arbitrator or counsel to protect the integrity of the proceedings or their express ethical obligations taking into consideration the risk that notification of a minor data breach will significantly disrupt the process. Given the risks associated with data breaches, questions should be addressed in advance in the context of the proceedings.

Example:

An arbitrator becomes aware that his system has been compromised and that access to all his files in 20 ongoing cases have been exposed. The arbitrator will need to consider whether this breach is likely to result in a risk for the rights and freedoms of those data subjects whose data has been exposed, in which case he must notify the breach to the supervisory authority within 72 hours of becoming aware of the breach. A key consideration will be the nature of the personal data compromised. For example, if it

[79] Art. 48, Para.1 of the LGPD requires a notification "within a reasonable period of time".
[80] 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.

includes sensitive personal data, such as data concerning health[81] or information regarding individuals' race, ethnicity or sexual orientation, or data concerning a child, notification to the supervisory authority may well be required. Depending on the circumstances, notification to the data subject may also be required. This is fact specific, but the notification requirement may not apply where the personal data relates to the type of business correspondence we often see in international arbitration, although the issue remains whether there is an obligation to inform the parties.

***Practice Tip*:**

Data Breach Notification – Arbitral Participants should consider and document in advance what will constitute a data breach, the procedure that will be followed if a breach occurs, the format for reporting, and who will be notified. This is important given the tight deadlines for notification of certain types of data breaches established by some data protection laws and the potential uncertainty about when there is an obligation to inform the parties.

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 and specific notices or a combination of the two.

General Notices. Even before a specific arbitration is contemplated, Arbitral Participants should consider publishing privacy notices, explaining to actual and potential data subjects why and how they process their personal data and what rights the data subjects have. Privacy notices should generally 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 is part of complying with the obligations imposed by, for example, GDPR Articles 13 and 14.[82]

Specific Notifications. In addition to general privacy notices, Arbitral Participants who are data controllers are responsible for ensuring that data subjects in a specific arbitration are put

[81] **'**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 reveal information about his or her health status (GDPR Art. 4(15)).

[82] Annex 6 provides the structure of examples of privacy notices for consideration by institutions, arbitrators and legal counsel governed by the GDPR. This annex may be a starting point for Arbitral Participants when deciding what to put in their privacy notices. The drafts in Annex 6 can also be used by those whose activities are outside the scope of the GDPR, but within the scope of another data protection law, where the notification requirements are similar. Arbitral Participants should note that privacy notices are fact-specific and require careful consideration and tailoring to each Arbitral Participant's particular situations, activities and needs.

on notice that their personal data is being processed for the arbitration and other details about the processing.

Given that any arbitration involves multiple data controllers, this could lead to one data subject receiving multiple notices. 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.

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 counsel).[83]

However, each Arbitral Participant will need to determine the position on a case-by-case basis. The position 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.

***Example*:**

Evidence is collected for an arbitration from 25 employees identifying at least 500 individuals. Subject to consideration of other potential restrictions under applicable labour law, the transparency doctrine requires that each individual identified (or identifiable) in those emails should either be notified of the processing for the arbitration (for example when their email boxes are screened for relevant information) or the processing should be compatible with 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 relationship to either party, and for whom notification may be problematic. The question is whether the data subjects have been given adequate notice of the processing for dispute resolution, 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, a further question is 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

[83] Under the GDPR, Article 14 (5) and Recital 62, where the data controller did not originally collect the personal data, 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.

employees at the time of the dispute can compromise the confidentiality of the process or create strategic concerns. These are considerations that may justify not giving additional notice when the dispute arises, especially in cases where the personal data is contained in business correspondence, to which data subjects should reasonably attach a lower privacy expectation than to personal records. Where a data protection protocol is employed, consideration should be given to allocating responsibility for making these determinations on the Arbitral Participant that collected the personal data.

Practice Tip:

Transparency – 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.

9. *Accountability*

Accountability requires data controllers to take personal responsibility for data protection compliance and 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 these principles as they are implemented throughout the GDPR.[84] 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.[85] 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 LGPD Art. 6(X).

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 LGPD's accountability principle. All Arbitral Participants

[84] GDPR Art. 5(2); *see also* GDPR Art. 24(1).

[85] 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.

should therefore keep records of the steps they take to comply with applicable data protection laws in a manner that can be shown to a competent authority.

Practice Tip:

Accountability – Arbitral Participants should document all measures and decisions taken regarding data protection compliance (in particular, the lawful basis relied on for data processing/third country transfers of data and any legitimate interests analysis, etc.) to allow them to demonstrate compliance with applicable laws to the competent authorities and other Arbitral Participants, if necessary. A data protection protocol can play an important part in documenting compliance, provided it is understood that it can be shared with the authorities, if necessary.

II. DATA PROTECTION COMPLIANCE DURING INTERNATIONAL ARBITRATION PROCEEDINGS

Based on the overview in Section I describing the application of the how data protection to arbitration and Arbitral Participants, this Section II considers how data protection compliance may affect a specific arbitration and the implications this may entail for Arbitral Participants.

This Section is organised around the typical procedural steps of an arbitration. It should be considered together with the Annexes, which contain examples of privacy notices, generic language to be considered for data protection protocols, procedural orders and terms of reference, 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.

A. Preparing for Arbitration

It is important to recall that data protection laws apply not only during the arbitration, but also when preparing for an arbitration. This sub-section reviews the data protection implications while preparing for arbitration, which will principally concern parties and their legal counsel.

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 consideration as to whether the various Arbitral Participants fall within the scope of a relevant data protection law.

In the first place, the privacy notices issued by the Arbitral Participants will provide insight into the approach that Arbitral Participant takes to data protection compliance, as well as their view of their status under the data protection laws as a controller, perhaps in parallel with other independent controllers, 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.

For example, where a party is required to transfer data to another country or jurisdiction, the party will want to consider the lawful basis for the transfer and may be required to review, minimise, cull and potentially redact personal data before transferring a more limited data set to Arbitral Participants in another country or subject to a different data protection regime.

> ***Practice Tip:***
>
> **Applicability –** 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 is prior to the initiation of the arbitration, for the institution as of the moment a party indicates that it is or may be starting an arbitration and for the arbitrators that moment is when they are contacted with a view to their appointment as arbitrator in a specific case.

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 whenever any Arbitral Participant is bound by data protection laws, this is likely to 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. **[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.

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 and transcribers;

- Parties, their legal counsel, and arbitrators may engage experts;

- Arbitrators may engage *ad hoc* tribunal secretaries (who are not employees of their firm); and

- Institutions may assist the parties with hearing facilities where translation and transcription services are provided, as well as other services performed by third parties.

Depending on who controls the purpose and means of the processing, some of the above service providers may be considered data controllers in their own right, while others are data processors acting only under the instructions of the controller **[Section I.C]** The personal data related to the arbitration may need to be transferred to each of these third-party service providers in order for them to provide their services.

Data transfers are considered to be data processing and, as such, data transfers to third parties require a lawful basis. Moreover, the fact that data may be transferred to a third party, the type of service provider, the purpose for the transfer and the lawful basis should be included in the data controller's privacy notice.

The Arbitral Participant will typically be a data controller. If this is the case, and the transfer is to another data controller within the same territory, for example within the EU, nothing further needs to be done. However, if the transfer is to a data controller in a third country or outside the EU, then the third country data transfer rules will need to be complied with.

If the data transfer is from a data controller to a data processor within the same territory, as opposed to a data controller, then a data processing agreement complying with the relevant data protection law should be put in place. For example, a data transfer from an EU based lawyer (data controller) to an EU based e-discovery professional (data processor) requires a GDPR-compliant data processing agreement.

When the data transfer is to a service provider acting as a data processor in a third country without an adequacy decision, the same requirement for a data processing agreement applies, however, in addition, there must be a lawful basis for the transfer to the third country the service provider is based in. In those cases, the most suitable method to ensure that there is a lawful basis for the transfer may be by including standard contractual clauses in the data processor agreement.[86] **[Section I.D]**

[86] 'Standard contractual clauses' refers to clauses adopted by the European Commission (or is 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). The Commission has adopted clauses for use between a processor and a

Practice Tip:

Service Providers – When engaging third parties to assist in proceedings (experts, court reporters, translators, etc.), Arbitral Participants should consider whether applicable data protection laws require them to enter into a data processing agreement with the third party and compliance with any applicable third country data transfer restrictions.

4. *Data Collection and Review*

When a dispute arises, the first thing that parties and their legal counsel typically do is review the facts by going back through the chain of events that led to the dispute. This often involves the review of emails and other contemporaneous evidence of the relevant events. Moreover, 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 legal proceedings.

The act of obtaining documents for the purpose of or in the context of an arbitration – whether collecting documents directly or through a document production exercise, receiving them from another Arbitral Participant – 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 processing activities, as well as a lawful basis for any third country data transfer that may be necessary in that framework.

Practice Tip:

Data Collection and Review – When preparing cases, parties and their legal counsel should identify and document the: (1) relevant data subjects or categories thereof; (2) categories of personal data, sensitive data, personal data of children and any data related to criminal proceedings that are likely to be processed and whether it is primarily low risk business correspondence and documentation; (3) likely impact of that processing on the relevant individuals; (4) 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) steps to minimise the processing of personal data to

controller or between two processors (GDPR Arts. 28(3), (4), (7), Recital 81; LGPD Art. 33(II, b)). According to the LGPD Art. 35, the national supervisory authority in Brazil – ANPD – will be in charge of defining the contents of the standard contractual clauses.

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.).

B. Successive Steps of the Arbitration Proceedings

This sub-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 personal data set forth in a request for arbitration in accordance with the arbitration agreement and the applicable rules fall squarely within the realm of processing.

In the case of institutional arbitration, the request for arbitration will typically be filed with an arbitral institution or international organisation, and in the case of an *ad hoc* arbitration, directly with the opposing party. To the extent the subsequent submissions involve personal data, the filing thereof also constitutes processing. In ad hoc proceedings, at least after the appointment of the tribunal, communication is directly with the arbitrator (s).

However, when the dispute is administered by an international organisation, which is often the case in investor-State arbitration, the data protection laws may exclude international organisations from its scope. Generally, because of privileges and immunities in the constituent treaty or in a host country host country agreement, the administering international organisation may provide special rules pursuant to which the international organisation itself, and potentially others (such as arbitrators and counsel) may be subject, existing outside the scope of the otherwise applicable data protection laws.

In arbitrations administered by an international organisation, the following elements should be considered when deciding whether and to what extent data protection laws apply to the Arbitral Participants' activities in the context of that particular arbitration:

- Whether the international organisation is bound by data protection laws according to their terms;
- Whether and to what extent some or all Arbitral Participants are covered by privileges and immunities (*e.g.*, both ICSID and the PCA extend immunity to "adjudicators," which category encompasses arbitrators);
- Where the data protection laws are nonetheless applicable in whole or in part to an Arbitral Participant, they should be applied; and
- Where the international organisation has its own specific data protection rules, these should be followed.

Therefore, the principles described in this Roadmap do not apply to (1) international organisations that are exempted from the application of national data protection laws and/or (2) certain Arbitral Participants that may also be immune from the application of data protection

laws under a particular legal instruments in the context of arbitrations administered by international organisations. Where this is not the case, the rules stated herein apply.

When arbitration institutions are bound by legal or other data protection regimes in the context of cases they administer, they 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).

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."

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 filing. This is especially necessary in cases where the filing of the request raises data protection concerns, where data transfer is required, information 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 administering 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, for certain purposes. From that point onwards, when processing personal data, the administering institution must comply with the privacy principles contained in the applicable data protection law, as described in Section I.

In practice, this means that the institution will need to have a lawful basis for the processing of personal data and any transfer outside the EU, appropriate information 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.

If the institution is covered by the GDPR, for example, all these aspects of processing should be included in its privacy notice, which should comply with Articles 13 and 14 of the GDPR. 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 6A contains an example of a notice that arbitral institutions subject to GDPR may consider. Many of the issues addressed therein will also be relevant to non-EU based institutions.

Applicability – Arbitral Participants should consider at the outset of (or prior to issuing proceedings in the case of parties and their legal counsel) what data protection laws will apply to them and the other Arbitral Participants.

2. *Appointment of Arbitrators*

When selecting arbitrators for cases in which the GDPR or other relevant data protection law(s) may apply, best practice suggests for those making the appointment to consider how it will implicate the application of the data protection laws. Where the potential arbitrator is not subject to the same data protection obligations, 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).

Before an arbitral appointment is made, significant personal data tends to be exchanged about the 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 means.

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 in their privacy notices that their personal data may be processed and transferred during the selection and appointment process and indicate what the legal basis is for such processing. Institutions may consider including specific notices as part of any procedure for potential arbitrators to be considered for appointment, for example by lists.

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 case of third country data transfer. Note that this is a mere notice, not consent. Asking arbitrators to consent to data processing and transfer triggers the risks discussed above and should be avoided. **[Section I.E.1]**

Practice Tip:

Arbitrator Selection – When selecting an arbitrator in a case where a party, arbitrator or institution is aware, or should be aware, that any of the parties or the institution is bound by a data protection law, the Arbitral Participant making the selection should take steps to

ensure that personal data may be processed by (including transferred to) the arbitrator in accordance any applicable data protection law.

3. *During the Arbitral Process, Who Should Raise Data Protection When?*

Once the arbitration is underway, the question arises as to who should raise data protection and when during the procedure.

The earlier the existence of and the allocation of responsibilities for compliance with data protection obligations is settled, the lower data protection risks and the more the impact on the proceedings can be minimised.

Where arbitrators are not themselves bound by any data protection regime, they may be inclined to avoid a discussion of data protection if it is not raised by the parties. However, this can create problems down the road as a party may not raise data protection concerns during the first procedural conference but may later claim that it cannot produce documents because disclosure would violate data protection laws. In the interest of compliance with data protection laws, as well as time- and costs efficiency of the arbitration, these issues are best addressed and managed from the outset.

Practice Tip:

Planning – Any Arbitral Participant that considers itself bound by a data protection law in relation to the proceedings should inform the other Arbitral Participants as soon as practicable so that appropriate measures can be undertaken to ensure that the arbitration is conducted in accordance with the applicable law(s). Data protection should be included on the agenda of the first procedural conference to give the Arbitral Participants the opportunity to discuss applicable data protection laws and how they can be complied with in the arbitration in a proportionate manner. **[Annex 3]**

Arbitral Participants should attempt to agree as early as possible on how data protection compliance during the proceedings will be addressed. Where the parties do not raise data protection, the tribunal should consider including it on the agenda of the first case management conference or procedural meeting/hearing and to issue directions where agreement is not achieved.

Directions – Like any other aspect of the administration of arbitral proceedings, arbitral institutions and tribunals are required to issue directions applying data protection principles during the arbitration to the extent necessary for the efficient resolution of the dispute.

In order to ensure the orderly conduct of the arbitration and compliance with applicable data protection law(s), the tribunal and the parties will need to address some, if not all, of the issues addressed in Section I in a data protection protocol, procedural order, or terms of reference. 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 (and sometimes required) to ensure compliance among controllers with parallel and interlinked obligations, as is the case in arbitration. This is often the best option to manage the risk of non-compliance among the Arbitral Participants.

The term "**data protection protocol**" refers to a document agreeing on how data protection is going to be applied in a particular context. Data protection protocols can be usefully employed in arbitrations to effectively manage the compliance issues of all Arbitral Participants. The parties, their counsel and the arbitrators should consider whether to propose entering into a data protection protocol signed by all Arbitral Participants, allocating responsibilities for data protection compliance during the arbitration. [**Annex 4**]

Given that the data protection laws are likely to have the force of mandatory law with respect to the Arbitral Participants (and the potential for significant sanctions for their breach), it is significantly preferable for a data protection protocol to be entered into by all Arbitral Participants (which could be included by reference in the first procedural order or terms of reference) to document how data protection compliance will be managed. This will also limit the ability of data subjects to complain to data protection authorities about matters that are addressed in the data protection protocol. A signed data protection protocol will often be achievable if requested by the Tribunal at an early stage in the proceedings, which again stresses the importance of the Tribunal actively managing these issues from the outset even where the data protection law might not apply to them personally.

Where it is not possible to achieve a signed data protection protocol, many of the issues that would be addressed in a Protocol may need to be ordered by the Tribunal in Procedural Order One with the goal of allowing the data protection rules to be applied in an orderly manner from the beginning and prohibiting parties from using them to delay or disrupt the proceedings. If the parties do not raise data protection as an agenda item for the procedural conference, the tribunal should.

General Annex 3 contains a checklist of items to be considered for data protection compliance during an arbitration and Annex 4 contains a sample data protection protocol.

Practice Tip:

Data protection protocol – Arbitral Participants should consider using a signed data protection protocol to address the data protection issues arising during the arbitration, which could be included by reference in the first procedural order or terms of reference to document how data protection compliance will be managed. Where it is not possible to achieve a signed data protection protocol, many of the issues that would be addressed in a Protocol may be ordered by the Tribunal in Procedural Order One. **[Annexes 3 and 4].**

4. *Disclosure or Production of Documents*

Document disclosure is an important part of the international arbitration process. The obligation to minimise data is particularly relevant to document disclosure. Although data minimisation is a general obligation,[87] 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.

In the context of a data transfer for purposes of US litigation discovery under the previous Data Protection Directive, which remains applicable, the EU Working Party suggested that data minimisation is likely to require (1) culling the data for relevance, (2) redacting personal data before it is transferred in order to avoid third country transfer of unnecessary personal data, (3) entering into protective orders where feasible, and (4) putting data protection safeguards in place after transfer.[88] Similar principles would be expected to apply under the GDPR in the context of an arbitration.

The documents used to prepare for an arbitration are a "mixed data set", in that they contain both personal and non-personal data. Deciding what part of a mixed data set is personal data requires earmarking data as personal if it allows individuals to be identified and if that data is related to an individual.[89]

If the same approach that the Working Party applied to US litigation disclosure were to be applied to the more limited document production in arbitration, this would imply a three-step process aimed at minimising the data disclosed:

1. Limiting the data disclosed to what is relevant to the dispute and non-duplicative;
2. Identifying the personal data contained in the responsive material; and
3. Redacting or pseudonymising unnecessary personal data.

Culling for relevance is a measure already used in the arbitration practice 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.

In the context of arbitration, the issues to be considered by the Arbitral Participants in relation to document production include (1) procedures aimed at limiting personal data exposure through confidentiality provisions; (2) data protection protocols and other risk-reducing procedures; (3) reasonable measures to avoid unnecessary international data transfers; and (4) the objecting party's prior treatment of the same data set. Arbitral Participants should also consider redaction, the scope of the compliance risk and the importance of the data for the

---

[87] 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.

[88] 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.

[89] The ECJ held 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" and it also covers cases where data is about the individual, is used to treat the individual differently, or if the use of the data has an impact on the rights and interests of the individual". Judgment of 6 November 2003, *Lindqvist*, C-101/01, 2003 I-12971, ¶ 24.

arbitration. Technology, including artificial intelligence, may assist in both culling the data for relevance and in redacting personal data. 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.

The impact of data minimisation on the document production process should be considered at the first procedural conference, if not before, to avoid unnecessary data being processed and to reduce cost and time. 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.

Practice Tip:

Document Disclosure – The impact of data protection laws should be 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 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.

5. *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, scrutinizing and notifying awards, etc.

Even in confidential arbitrations, 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. Moreover, in investment and treaty-based arbitrations, awards are often published and commercial institutions increasingly considering the publication of awards if the parties do not object and subject to possible redaction, and (excerpts of) challenge decisions.

In that framework, arbitrators and institutions should consider the basis and necessity for the inclusion of personal data in their 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 data has been redacted it typically remains personal data because the data subject is still identifiable from the remainder of the award or related materials, and therefore must be processed in compliance with data protection laws.

Practice Tip:

Awards – 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 when described by the parties.

6. *After the Arbitration - Data Retention and Deletion*

Both data retention and deletion is considered data processing under many modern 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)). Similarly, under LGPD Articles 15 and 16, 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 their processing. 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.

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, 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. Arbitral Participants 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. **[Section I.E.4]** Parties should bear in mind that potential use in other legal proceedings may not be a sufficient basis for parties to retain data beyond an otherwise reasonable period of time.

Arbitral Participants, like all data controllers, should take a proportionate approach to the extent and in the manner foreseen by the applicable law(s), balancing their needs with the impact of retention on the data subject. 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 informed 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.

> ***Practice Tip:***
>
> **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.

CONCLUSION

The aim of this Roadmap is to enable Arbitral Participants to identify and effectively address data protection issues in the context of arbitral proceedings.

This Task Force encourages Arbitral Participants to take a pro-active, reasonable and proportionate approach towards data protection compliance in international arbitrations where modern data protection laws apply to the Arbitral Participants. In managing data protection issues during arbitration proceedings, consideration should be given to employing signed data protection protocols where possible and documenting compliance efforts in a manner that can be shared with data protection authorities if requested.

We would stress that there are sensible solutions to the data protection challenges that arise in arbitrations, and Arbitral Participants will soon become familiar with the issues and accustomed to dealing with them. The goal of this Roadmap is to facilitate that process.