ICCA
INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION

ICCA–IBA Joint Task Force on Data Protection in International Arbitration

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

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

The ICCA Reports No. 7

INTERNATIONAL COUNCIL FOR
COMMERCIAL ARBITRATION

ICCA–IBA JOINT TASK FORCE ON DATA PROTECTION IN INTERNATIONAL ARBITRATION

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

THE ICCA REPORTS NO. 7

2022

ICCA is pleased to present the ICCA Reports series in the hope that these occasional papers, prepared by ICCA interest groups and project groups, will stimulate discussion and debate.

INTERNATIONAL COUNCIL FOR
COMMERCIAL ARBITRATION

ICCA–IBA JOINT TASK FORCE ON DATA PROTECTION IN INTERNATIONAL ARBITRATION

ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION

THE ICCA REPORTS NO. 7

2022

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

www.arbitration-icca.org

Published by the International Council for Commercial Arbitration
www.arbitration-icca.org

ISBN 978-94-92405-34-0

For further information, please contact us at bureau@arbitration-icca.org.

All views expressed in this Report are those of the Task Force and not ICCA, the IBA or their governing bodies or members. This Report is the result of the collective efforts of the Task Force, the views expressed are not attributable to any particular Task Force member and all Task Force members served in their individual capacity.

About ICCA

ICCA is a worldwide nongovernmental organisation (NGO) devoted to the use and improving the processes of arbitration, conciliation and other forms of resolving international disputes. Its activities include convening biennial international arbitration congresses; sponsoring authoritative dispute resolution publications (including the ICCA Yearbook Commercial Arbitration, International Handbook on Commercial Arbitration and ICCA Congress Series); and promoting the harmonisation of arbitration and conciliation rules, laws and standards. ICCA has official status as an NGO recognised by the United Nations. See www.arbitration-icca.org.

About the IBA

The IBA is the foremost organisation for international legal practitioners, bar associations and law societies. Established in 1947, shortly after the creation of the United Nations, the IBA was born out of the conviction that an organisation made up of the world's bar associations could contribute to global stability and peace through the administration of justice. The present membership is comprised of more than 80,000 individual international lawyers from most of the world's leading law firms and some 190 bar associations and law societies spanning more than 170 countries.

The IBA Arbitration Committee focuses on the laws, practice and procedures relating to the arbitration of transnational disputes. It currently has over 3,000 members. Through its publications and conferences, the Committee seeks to share information about international arbitration, promote its use and improve its effectiveness. The Committee maintains standing subcommittees and, as appropriate, establishes task forces to address specific issues.

ACKNOWLEDGEMENTS OF THE CO-CHAIRS

In view of the complexity and importance of the ICCA-IBA Roadmap to Data Protection in International Arbitration ("Roadmap"), it is impossible to acknowledge all those who contributed to the project. Yet, the Roadmap would not have seen the light of day without the invaluable contributions of the following individuals and organisations.

First, the members and rapporteurs of the ICCA-IBA Joint Task Force on Data Protection in International Arbitration ("Task Force") have devoted countless hours, attending task force meetings, drafting and reviewing the Roadmap and the Annexes, and hosting and participating in events to ensure we had adequate feedback from the arbitration community, as well as the many other administrative tasks involved in a project of this size. Thank you for all you have contributed, for your good cheer and constructive attitude throughout the process. A special word of thanks goes to Emily Hay of Hanotiau & van den Berg, for her generosity and hard work, without which this Roadmap simply would not have been possible.

We would also like to extend our heartfelt thanks and appreciation to ICCA President Lucy Reed, past-Presidents Gabrielle Kaufmann-Kohler (Lévy Kaufmann-Kohler) and Donald Donovan, the ICCA Governing Board, Lise Bosman (Executive Director), Lisa Bingham (Deputy Executive Director), and the members of the ICCA Bureau, whose support throughout the process has been invaluable.

We would also like to sincerely thank the Arbitration Committee of the International Bar Association, and especially its present and past co-chairs, Eduardo Silva Romero, Gaetan Verhoosel, Philippe Pinsolle, Julie Bédard, Samaa Haridi and Valeria Galindez for their support and contributions throughout the project. Special thanks goes to Xavier Favre-Bulle for the thoughtful and constructive input he has provided on the successive drafts.

We are also grateful to the representatives of all the arbitration institutions and international organizations who kindly devoted their time to discussing the Roadmap with the Task Force and commenting on drafts, including the AAA-ICDR, HKIAC, ICC, LCIA, SCC, SIAC, DIS, and VIAC as well as ICSID, the PCA and the WIPO. We know your time is valuable, and we appreciate your help enormously.

We would also like to give our thanks and appreciation to Tatiana Campello (Demarest) and Rodrigo Azevedo (Silveiro), and Aaron Kamath (Nishith Desai) and Payel Chatterjee (Adani Enterprises), who, although not being Task Force members, generously gave their time to address the data protection laws of Brazil and India for the Roadmap.

Likewise, we are grateful to members of the arbitration community who took the time to provide their comments on the public draft of the Roadmap, and whose input was extremely valuable.

Lastly, we would like to thank the law firms of Ambos Law, Derains & Gharavi and Hanotiau & van den Berg for their generous support throughout the process.

The bottom line is that this was a collective effort, going well beyond the Task Force itself. We greatly enjoyed the exchanges and remain forever grateful for all your contributions to the ICCA-IBA Roadmap to Data Protection in International Arbitration.

Kathleen Paisley
Melanie Van Leeuwen
Co-chairs

MEMBERS OF THE ICCA–IBA JOINT TASK FORCE ON DATA PROTECTION IN INTERNATIONAL ARBITRATION

Co-Chairs

Kathleen Paisley, Ambos Lawyers

Melanie van Leeuwen, Derains & Gharavi

Members

Lawrence Akka QC, 20 Essex Street

Rosa Barcelo, McDermott Will & Emery

Niuscha Bassiri, Hanotiau & van den Berg

Markus Burianski, White & Case

Hugh Carlson, Three Crowns

Daniel Cooper, Covington & Burling LLP

Javier Fernandez-Samaniego, Samaniego Law

Hilary Heilbron QC, Brick Court Chambers

Robert Maddox, Debevoise & Plimpton LLP

Charlie Morgan, Herbert Smith Freehills LLP

Philippe Pinsolle, Quinn Emanuel Urquhart & Sullivan LLP

Jacques de Werra, University of Geneva

Rapporteurs

Emily Hay, Hanotiau & van den Berg

Brianna Gorence, Freshfields Bruckhaus Deringer

Table of Contents

INTRODUCTION

This ICCA-IBA Roadmap to Data Protection in International Arbitration ("**Roadmap**") has been developed by the ICCA-IBA Joint Task Force on Data Protection in International Arbitration as a tool to assist arbitration professionals in applying data protection and privacy laws during international arbitration proceedings.

A. DATA PROTECTION AND ARBITRATION

The European Union's ("**EU**")[1] General Data Protection Regulation[2] ("**GDPR**") and similar laws in other jurisdictions[3] apply as a matter of law to the collection, retention, processing and security policies of personal data, including during arbitration proceedings. As non-compliance may trigger civil and/or criminal liability (for example, under the GDPR potential fines for non-compliance may rise to 4% of global gross revenue

---

1. "European Union" or "EU" designates the current twenty-seven EU Member States: Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the Netherlands. It bears noting that the Roadmap throughout uses the term "EU", while in fact the scope of application of the GDPR extends to the whole European Economic Area ("EEA"). The EEA encompasses the 27 EU Member States and three additional states: Iceland, Liechtenstein and Norway. On 31 January 2020, the United Kingdom withdrew from the EU. The UK General Data Protection Regulation ("UK-GDPR") mirrors the GDPR and has been deemed by the EU to be adequate and the UK is an adequacy country. Therefore, at the time of writing, although the UK is no longer a member of the EU, the provisions described herein generally apply in the UK as a matter of application of the UK-GDPR.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016.*
3. To assist in deciding the scope of potential legal responsibilities, Annex 11 contains a table including a non-exhaustive list of references to national and regional data protection laws of important arbitration jurisdictions, including those where the EU has issued adequacy decisions. Moreover, in the EU, it is important to keep in mind that, even when the GDPR applies, the national laws of the relevant EU country also need to be considered. Although the GDPR is a European Regulation that should be consistently applied throughout the EU without the need for national implementing legislation, the GDPR itself allows EU Member States discretion (described as a "margin of manoeuvre") and the possibility to implement derogations in several areas potentially relevant to arbitration (*e.g.*, GDPR Recital 10). Annex 11 also includes a list of the data protection laws of the EU Member States.

or EUR 20 million, whichever is higher[4]), it is important for arbitration professionals to consider what data they process, as well as where, why, by what means, with which information security measures and for how long they do so.

Data protection laws and regulations are generally of mandatory application. They prescribe the legal rules applicable whenever personal data is processed, including when, where and how personal data may be processed. However, such laws and regulations do not address how they should be applied in specific contexts, such as in arbitration. Moreover, although data protection authorities have provided guidance as to the way data protection rules should be given effect in certain industries, such guidance is not yet available for international arbitration. It is also not possible to draw conclusions from how such laws apply to courts, because, at least in the EU, courts are generally not subject to the jurisdiction of the data protection authorities. It is therefore necessary for arbitration professionals to consider how these laws apply to them generally and in their cases specifically.

In the absence of specific guidance, it is important to think through the steps of the arbitral process and document the data protection and procedural measures adopted in the different phases of an arbitration within the framework of whatever data protection law(s) apply. To assist in that process, this Roadmap identifies the data protection issues that may arise in the context of international arbitration proceedings, as well as solutions that may be adopted to address them.

Data protection obligations apply to the processing of personal data by individuals and legal entities that fall within the material and jurisdictional scope of the relevant data protection law. Therefore, it is not the processing of personal data for the arbitration as such that is subject to the data protection laws. Rather, the individuals and entities that are involved in the arbitration are subject to the data protection laws. Each of them may fall under the scope of a different data protection law, or none at all, which means that in any arbitration proceedings, different data protection rules may apply to different participants. Some of those involved may have certain data protection obligations and others may not.

---

4. Under the Lei Geral de Proteção de Dados (Brazilian General Data Protection Act) (Statute 13709/18) ("Brazil Act" or "LGPD"), the fines may be up to 2% of gross revenue in Brazil or BRL 50 million. The Brazil Act unified 40 pre-existing laws to regulate processing of the personal data of individuals. The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. ("California Act" or "CCPA") similarly provides for monetary penalties: depending on where the violation occurred, the penalty may be up to USD 2,500 for each violation or USD 7,500 for each international violation. In addition, and unlike the GDPR and the Brazil Act, the California Act does not provide a maximum amount of penalty.

It is important to appreciate that if even one participant in an arbitration is subject to data protection obligations, this may have an impact on the conduct of the arbitration as a whole. This is because the participant's compliance with its data protection obligations may have a spill over effect on the arbitration and require others to process the personal data for the arbitration in a particular way.

B. INTENDED SCOPE AND PURPOSE OF THE ROADMAP

The Roadmap's intended scope and purpose consists of the features set forth in this Section.[5]

Types of Proceedings. The type of arbitration (for example, commercial or investor-State) typically does not determine whether data protection laws apply.[6] Rather, the application of data protection laws is determined by whether the data processing during the arbitration by a specific participant falls within the material and jurisdictional scope of a relevant law.

Arbitral Participants. The Roadmap is only addressed to **Arbitral Participants**, which is defined in the Roadmap as, and limited to, the parties, their legal counsel, the arbitrators and arbitral institutions. However, while it is not explicitly addressed to them, the guidance provided herein is also relevant to those working for or with Arbitral Participants during an arbitration, such as tribunal secretaries, experts and service providers (*e.g.*, e-discovery experts, information technology professionals, transcribers, translation services, online case management platform providers, remote hearing platform providers, etc.). Therefore, Arbitral Participants who are assisted by others during the arbitral process should consider how data protection laws affect those relationships, taking into consideration that:

---

5. While data protection laws apply in a similar manner to professionals and entities involved in mediation and forms of alternative dispute resolution, they are not expressly addressed in this Roadmap. Moreover, in many jurisdictions, including those of the EU, special rules apply to courts, including self-regulation and certain exemptions, which are also not addressed in this Roadmap.
6. In the case of arbitrations administered by an international organisation, determining whether any relevant privileges and immunities will impact the application of data protection laws turns on the breadth and scope of the relevant privileges and immunities, as well as the language of the relevant data protection law, both in terms of whether data protection laws would come within their scope, and, if so, which Arbitral Participants would be covered by them. This is an institution-specific and arbitration-specific enquiry, which is beyond the scope of this Roadmap.

- where an Arbitral Participant is a legal entity,[7] employees of that entity are not considered separately for compliance purposes, rather their actions are attributed to that entity;
- where arbitration-related information containing personal data is shared with a third party,[8] this is considered to be processing, which requires compliance with data processing rules and transfer restrictions; and
- where an Arbitral Participant uses a third party to undertake data processing activities on its behalf (such as a data analytics company), both parties are responsible for compliance with the data protection laws during that processing.[9]

General Data Protection Principles. The Roadmap addresses data protection compliance in international arbitration with reference to general data protection principles, rather than the law of a particular jurisdiction (unless otherwise indicated by way of illustration). However, the examples provided in the Roadmap are often based on the GDPR because it is one of the most comprehensive and onerous data protection regulations, and is becoming a global reference. The GDPR and its predecessor legislation, the Data Protection Directive,[10] have been widely drawn upon by jurisdictions across the globe for their data protection laws, which are referred to in the Roadmap as "EU-style" data protection laws.

Roadmap Organisation. The Roadmap is divided into two sections:

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

7. The entity may qualify as a data controller. A "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (GDPR Art. 4(7)).
8. A "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (GDPR Art. 4(10)).
9. GDPR Data Controllers and Data Processors, https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/.
10. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281/31, 24.10.1995 ("Data Protection Directive").

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

Roadmap Annexes. In order to provide practical guidance to practitioners, the Roadmap is accompanied by a set of Annexes that provide greater detail, practical information, checklists, sample language, and references aimed at enabling Arbitral Participants to apply data protection principles in the context of an arbitration, and a glossary of data protection terms, which are also defined in the footnotes. These Annexes are organised as follows:

- **Annex 1** contains a glossary of data protection terms;
- **Annex 2** contains practice tips for applying data protection principles in specific cases;
- **Annex 3** provides a more detailed checklist addressing how to operationalise these tips;
- **Annex 4** provides a checklist on the use of an Online Case Management Platform;
- **Annex 5** contains a non-exhaustive list of considerations that should be applied in performing a Legitimate Interests Assessment;
- **Annex 6** provides a sample set of "standard contractual clauses" for controller-controller transfers under the GDPR;
- **Annex 7** contains some non-exhaustive sample provisions for data protection directions for the first procedural order or the terms of reference;
- **Annex 8** contains a sample data protection protocol, taking into account the GDPR;
- **Annex 9** provides sample data privacy notices for (A) arbitral institutions (other than international organisations),[11] (B) arbitrators, and (C) legal counsel;
- **Annex 10** provides a list of sources per category, used in the drafting of this Roadmap; and
- **Annex 11** contains a compendium of selected data protection laws.

Goal. The aim of the Roadmap is to enable Arbitral Participants to identify and effectively address data protection issues in the context of arbitral proceedings. There are sensible solutions to the data protection challenges that arise in arbitrations, and Arbitral Participants should become familiar with the issues and become accustomed to dealing with them.

11. *See* fn. 6.

No Legal Advice. Data protection laws impose mandatory legal obligations on those coming within their scope. Importantly, while providing guidance, nothing in the Roadmap or Annexes can be taken as legal advice. The Roadmap provides information and resources to foster a better understanding of the data protection rules that may apply during an arbitration, and the Arbitral Participants' potential obligations thereunder. However, assessing data protection obligations is a fact-driven and case-specific undertaking.

The Roadmap and its Annexes will necessarily be a living document. Over time, data protection authorities and courts may clarify how data protection laws should be applied to international arbitration, whilst recognising the balance that must be struck given the important role arbitration plays in the administration of justice and the enforcement of legal rights and obligations on the international plane.

I. GENERAL DATA PROTECTION PRINCIPLES RELEVANT TO INTERNATIONAL ARBITRATION

The purpose of this Section of the Roadmap is to provide a general understanding of the data protection principles embodied in most EU-style data protection laws as they may apply to international arbitration. The EU, Brazil,[12] Canada,[13] India,[14] and the State of California[15] are used as examples to give context. However, similar principles apply under many other EU-style data protection regimes. For the avoidance of doubt, references to specific legislation or to a jurisdiction serve as an indication only.

General Obligations. Arbitral Participants have general obligations under the data protection laws that apply to their data processing activities regardless of their involvement in a specific arbitration.[16] The extent of these obligations will depend on the applicable law and the Arbitral Participant's status under that law as a data controller, joint controller or a data processor. Arbitral Participants will generally be data controllers, and joint controllers under certain circumstances. For data controllers and joint controllers (who are jointly responsible), these obligations typically include ensuring and demonstrating compliance, ensuring the lawfulness of their personal data processing and transfers, minimising the personal data they process, issuing GDPR-compliant data privacy notices, and adopting appropriate data security measures, data breach procedures, data retention policies, and procedures for addressing data subject complaints.[17]

---

12. *See* Brazil Act.
13. Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"), SC 2000, c 5, http://canlii.ca/t/541b8 retrieved on 20 September 2020, which applies to organisations that collect, use or disclose personal information in the course of commercial activities in Canada.
14. India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011 ("India Act"), which addresses data protection in certain contexts and for certain types of data. India has also proposed a comprehensive data protection law, which has yet to be adopted.
15. *See* California Act.
16. In the case of arbitrations administered by an international organisation, *see* fn. 6.
17. *See*, *e.g.*, Annex 3, which provides a checklist of data protection issues that Arbitral Participants may want to consider. While the most important way to avoid liability is through compliance, given the interlinking nature of these obligations and the potential risk of non-compliance, Arbitral Participants should consider taking out insurance, and where appropriate imposing insurance obligations and indemnities on each other during proceedings where there are significant data protection risks.

A. MATERIAL SCOPE OF DATA PROTECTION LAWS

EU-style data protection laws apply whenever:

- "personal data" about a
- "data subject" is
- "processed",

during activities falling within the jurisdictional scope of the relevant data protection laws.

Understanding the concepts of "personal data",[18] "data subjects"[19] and "processing"[20] is therefore key to understanding how data protection laws function. "Personal data" and "processing" are broadly defined notions, which encompass information that may not traditionally have been thought of as confidential or sensitive, as well as most of the activities typically undertaken by Arbitral Participants in the context of an arbitration.

---

18. "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art. 4(1)); information regarding an identified or identifiable natural person (Brazil Act Art. 5(I)).
19. "Data subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art. 4(1)); a natural person to whom the personal data that are the object of processing refers (Brazil Act Art. 5(V)).
20. "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR Art. 4(2)); any operation carried out on personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction (Brazil Act Art. 5(X)).

1. Personal Data

Many data protection laws define personal data to include "any information relating to an identified or identifiable natural person" (*e.g.*, GDPR Art. 4; Brazil Act Art. 5, I; and California Act Sections 1798.140(b) and (o)[21]).

Under many laws, including, for example, the GDPR and the Brazil Act, it is irrelevant that the personal data is contained in a business-related document (such as work files, work emails, laboratory notebooks, agreements, construction logs, etc.). Provided that the data relates to an individual who is identified or identifiable, it is considered to be personal data covered by the data protection laws.

A substantial portion of the information exchanged during a typical international arbitration is therefore likely to contain data that qualifies as personal data.

2. Data Subject

Individuals who are identified or identifiable from the data are referred to as "data subjects". Legal entities are not data subjects.[22]

3. Processing

Data protection laws impose obligations that must be complied with whenever personal data is "processed".

Processing is broadly defined to include not only active steps such as collecting, using, disseminating and deleting data, but also passive operations such as receiving, holding, organising and storing data. Moreover, data protection laws usually apply not only to electronically processed information, but also to data in (or intended for) a paper filing system (*e.g.*, GDPR Recital 15, Art. 2(1))[23] or similar means (*e.g.*, Brazil Act Art. 1).[24]

---

21. While the definition of "personal information" under the California Act is substantially similar to "personal data", personal information under the California Act does not extend to publicly available information, which is information that is lawfully made available from federal, state, or local government records, if that data is used for a purpose that is compatible with the purpose for which the data is maintained and made available in the government record.
22. *See* fn. 19.
23. A "filing system" means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (GDPR Art. 4(6)).
24. "This Act provides for the processing of personal data, including by digital means…" (Brazil Act Art. 1).

Most activities undertaken in a typical international arbitration are thus likely to constitute processing.

B. JURISDICTIONAL SCOPE OF DATA PROTECTION LAWS

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

- In the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not (GDPR Art. 3(1)); or

- Where the processing activities are related to the offering (targeting) of goods or services to individuals in the EU (regardless of their residence or citizenship) (GDPR Art. 3(2)(a)).

Moreover, even where the GDPR does not apply as a matter of law, some of its provisions may still apply as a matter of agreement. For example, under the GDPR, whenever personal data is transferred to international organisations or to countries that have not been found by the EU to provide adequate protection,[25] transferors are required to put "adequate protections" in place where feasible. In the case of arbitration, as discussed below in **Sections I.E** and **II.B.3.c(2)**, this is likely to take the form of standard contractual clauses, pursuant to which the parties agree by contract to abide by the most important provisions of the GDPR. This leads to significant scope creep, even beyond the already broad territorial reach of the GDPR. Similar provisions are found in numerous other EU-style data protection laws throughout the world.[26]

---

25. The EU considers that the data protection laws of Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay are adequate (*see* Annex 11). The EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the European Commission to provide a basis for data transfers with adequate data protection from the EU to the US, was invalidated by the CJEU in the 2020 *Schrems II* decision. *See* Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilian Schrems*, C-311/18, ECLI:EU:C:2020:559. In March 2022, the EU and the US announced an in-principle agreement on a new "Trans-Atlantic Data Privacy Framework" to be put in place to address the *Schrems II* decision.
26. The Brazil Act, for example, applies to any data processing operation carried out by a natural person or by a public or private legal entity, regardless of the medium, the country of its headquarters or the country where the data is located, provided that: (1) the processing operation is carried out in the Brazilian territory; (2) the processing activity aims at offering or supplying goods or services or processing data of individuals located in the Brazilian territory; or (3) the

Example: An EU-based arbitrator is appointed in an arbitration administered by a non-EU based institution. No other Arbitral Participant is subject to the GDPR. The EU-based arbitrator will be bound by the GDPR and obliged to process any personal data in connection with the arbitration in compliance with the GDPR's requirements, including having a lawful basis for transferring data outside the EU in connection with the arbitration. Depending on the circumstances, this may involve putting in place European Commission-approved standard contractual clauses, which will have the practical result that the non-EU based Arbitral Participants agree to be bound by the main provisions of the GDPR. Where it is not feasible to put standard contractual clauses in place for a justifiable reason, it may be possible to transfer based on the derogation for transfers "necessary for the establishment, exercise or defence of legal claims".[27]

C. ROLES UNDER DATA PROTECTION LAWS

Arbitral Participants covered by an EU-style data protection regime have obligations under the data protection laws that apply to their data processing activities including during an arbitration.

personal data subject to processing has been collected on Brazilian territory (Brazil Act Art. 3). The California Act applies to organisations "doing business in California", a criterion that is not precisely defined within the law. However, citing the California Franchise Tax Board, commentators have written that "out-of-state entities collecting, selling or disclosing personal information of California residents [may be understood to] fall under the scope of the CCPA" if they are "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit." (Data Guidance, *Comparing Privacy Laws: GDPR v. CCPA*, available at https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf).

27. The GDPR provides a specific derogation or exception from certain of its provisions where processing is "necessary for the establishment, exercise or defence of legal claims", which should be applied to arbitration and is referred to herein as the "Legal Claims Derogation". This includes: (1) the derogation from the GDPR's third-country transfer restrictions for transfers (GDPR Art. 49(1)(e)); (2) a lawful basis for processing sensitive data (GDPR Art. 9(2)(f)); (3) an exception to the right to erasure or to stop processing (GDPR Art. 17(3)(e)); and (4) as applied by some Member State laws, to allow the processing of Criminal Offence Data.

The extent of these obligations depends on the Arbitral Participant's status under the applicable data protection law as a controller (who often will be acting in parallel with other independent controllers), a joint controller,[28] or a processor.[29]

1. Data Controllers

Under EU-style data protection laws, the data controller is primarily responsible for compliance and demonstrating compliance. Data controllers can be natural or legal persons, irrespective of (1) whether they are for profit or not;[30] (2) whether they are private law or public law entities; and (3) their size.

The data controller determines "the purposes and means of the processing of personal data".[31] Applying this definition, most Arbitral Participants are likely to be considered data controllers because, by virtue of their function, they control the purpose and means of the processing of personal data in the context of an arbitration (although they do not control the processing of data by other Arbitral Participants). For example, both barristers[32] and solicitors[33] are typically considered to be data controllers by data protection authorities in the EU and the UK when performing case work.

---

28. "Joint controllers" are where two or more controllers jointly determine the "purposes and means" of the data processing (GDPR Art. 26(1)).
29. A "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR Art. 4(8)).
30. An exception being California where the California Act only extends to controllers that are for-profit.
31. *See*, *e.g.*, GDPR Art. 4(7); Brazil Act Art. 5(VI).
32. With respect to data controllers, the EU Working Party has illustrated the concept of a data controller in the following example: "A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as independent "controllers" when processing data in the course of legally representing their client." EU Working Party, "Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'", WP 169, 16 February 2010, at 29 ("Controller/Processor Opinion").
33. The ICO is the UK Information Commissioner's Office set up to uphold information rights, including under data protection law. The ICO has taken the view that solicitors are data controllers. *See* Controller/Processor Opinion, at 28; ICO, "Data controllers and data processors: what the difference is and what the governance implications are", Data Protection Act 1998, paras 40-43.

2. Joint Controllers

The GDPR has introduced the concept of "joint controllers" who "jointly" determine the "purposes and means" of the data processing.[34] Where the GDPR applies, each of the joint controllers is responsible for compliance with the GDPR. They are also *jointly and severally liable for any data protection violation* with a possibility for recourse against the other joint controller(s) if it can be established that they were responsible for part of the damage.[35] This concept is similarly found in other newer data protection laws enacted after the GDPR, like the Brazil Act, but not in many older data protection laws.[36] If Arbitral Participants are joint controllers, they are required to make arrangements to allocate the risks involved, for example through a data protection protocol.[37]

The possibility of shared or parallel responsibility of Arbitral Participants bears out the importance of data protection compliance by all Arbitral Participants. Although not specifically related to arbitration, decisions of the Court of Justice of the European Union ("CJEU") under the Data Protection Directive indicate that the notion of joint controllership is to be broadly interpreted. However, the liability of a joint controller is limited to the processing of data for which that controller "actually determines the purposes and means" of the processing and does not extend to the overall chain of data processing for which it does not determine the purposes and means. Nevertheless, under the GDPR, the joint controller would likely be liable in full to the person whose data has been unlawfully processed and will then be able to have recourse against other joint controllers.[38]

Unless otherwise indicated, this Roadmap is based on the premise that Arbitral Participants are either data controllers (often in parallel with other controllers) or joint controllers as far as their arbitration activities are concerned. To establish whether Arbitral

---

34. GDPR Art. 26(1). The addition of the joint controller concept to the GDPR followed relevant case law in the EU under its predecessor legislative instrument, the Data Protection Directive, which provided that controllers would be considered "joint controllers" under certain circumstances.
35. GDPR Art. 82(5).
36. The Brazil Act provides that "controllers who are directly involved in the treatment of which damage has occurred to the data subject are jointly and severally liable …" (Brazil Act Art. 42, Paragraph 1, II).
37. A "data protection protocol" refers to a document addressing data protection whereby the roles and responsibilities of data controllers and processors vis-à-vis the processing of personal data are identified and agreed. This is required by the GDPR for joint controllers.
38. *See* Judgment of 29 July 2019, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629, paras 74, 85. *See also* Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* C210/16, EU:C:2018:388; Judgment of 10 July 2018, *Tietosuojavaltuutettu*,, C25/17, EU:C:2018:551; GDPR Art. 82(5).

Participants are either (1) controllers (who are likely to be acting alongside other controllers with parallel responsibilities); or (2) joint controllers, involves a factual assessment, which turns on the question as to whether they can properly be considered to *jointly* determine the "purposes and means" of the processing of personal data.

3. Data Processors

Data controllers (including joint controllers) can delegate the processing of data under their control to a data processor, which is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (*e.g.*, GDPR Art. 4(8)).[39] Under EU-style data protection laws, data controllers may only delegate processing activities to data processors if they enter into data processing agreements on terms prescribed by the applicable law.

To qualify as a data processor, the party must meet the following criteria:

- Act under the instruction of a data controller in undertaking their tasks;
- Not be responsible for deciding the purposes and means of the data processing; and
- Be retained under a (GDPR-compliant) data processing agreement allowing the data controller to direct the processing and stop it at any time.

In the context of arbitration, Arbitral Participants will generally not qualify as data processors because, by virtue of their function, they control the purposes and means of the data processing.

However, an Arbitral Participant may wish to engage a third party to process data, in which case they should ensure that the controller retains control over the purposes and means of the data processing and that a compliant data processing agreement is put in place.[40]

Tribunal secretaries, e-discovery professionals, transcribers, interpreters, online case management platform providers, remote hearing platform providers and other service providers (not being employees of the Arbitral Participants) may be considered data processors, depending on who directs the purposes and the means of the processing, requiring that a GDPR-compliant data processing agreement is entered into with such persons or entities.

---

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

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

The collecting and collating of documents relevant to potential claims may be carried out by database service providers, whose job it is to collect data on the instruction of the party or counsel. They would thus be considered to be data processors without the responsibility for deciding the means and purposes for data processing, subject to the rules established in the applicable data protection laws for data processors.

Counsel distils from those documents the relevant information, which includes personal data, and records that information in submissions and evidence, which is then provided to the administering institution and the tribunal. In order to perform their duties, legal counsel, the institution and arbitrators are likely to determine the "purposes and means" of the data processing and will therefore be considered to be data controllers (or joint controllers if they jointly control the purpose and means of the processing) and thus subject to the rules established in the applicable data protection laws for data controllers or joint controllers.

These potentially overlapping individual compliance responsibilities create competing obligations that need to be reconciled. This is further complicated by the fact that Arbitral Participants may not be subject to the same data protection laws and others may not be subject to any data protection law at all. The orderly conduct of the proceedings will therefore be facilitated by the issuance of Data Protection Directions in the first procedural order, the terms of reference or in a data protection protocol (*see* **Section II.B.3.c** and **Annexes 7** and **8**).[41]

D. LAWFUL BASIS FOR PROCESSING

Where an EU-style data protection law applies to an Arbitral Participant, the most fundamental question one must address is what is the "lawful basis" for the data processing.

41. "Data Protection Directions" are procedural directions issued by an arbitral tribunal in the form of a procedural order, terms of reference, or a data protection protocol setting out how data protection will be addressed during the arbitration. They may be issued on an agreed basis or ordered by the arbitral tribunal.

Arbitral Participants exchange significant amounts of information, often across borders. This information contains personal data (sometimes including sensitive[42] and criminal data). Those exchanges are essential for the proper administration of justice by means of international arbitration and the enforcement of the parties' rights in the arbitral process. However, these exchanges of information must also be lawful under the applicable data protection laws.

Under most EU-style data protection laws, a specific legal ground for the data processing must exist in order for the processing to be lawful (the so-called "lawful basis" for processing).[43] Depending on the purpose of the data processing and the controller's relationship to the data subject, the controller has a number of available lawful bases upon which to process data.

In most jurisdictions, including in the EU, there is no universal legal basis for lawful processing of data in the specific context of arbitration. Rather, the decision as to which legal basis to rely on for the processing of personal data in an arbitration is fact-driven and case-specific. Depending on the circumstances of the case, the potential lawful bases may be different for different Arbitral Participants and for different types of personal data (*e.g.*, witness data, data contained in the documentary evidence, sensitive or "special category" data, criminal data). Moreover, it is also required that the personal data is not processed in a manner that is unlawful generally (for example not in breach of confidentiality obligations).

As set forth below in Section II, the proper functioning of an arbitration where an EU-style data protection law applies to an Arbitral Participant requires establishing the lawful basis of the data processing at the outset of the proceedings.

---

42. The GDPR refers to "special categories of personal data", which is also commonly referred to as "sensitive data", and is defined in the GDPR as data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. A similar list of sensitive data is found in Art. 5(II) of the Brazil Act. Under the GDPR, processing of special category data is allowed, among other reasons, where necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (GDPR Art. 9(1) and 9(2)(f)).
43. The California Act does not have a list of positive legal grounds required for collecting, selling, or disclosing personal information. Rather, it only provides that businesses must obtain the consent of consumers when they enter into a scheme that gives financial incentives on the basis of the personal information provided. *See* California Act Section 1798.120.

Example: The parties present documents – such as submissions – and evidence including work-related emails, witness statements, contracts and other materials identifying individuals. All the information identifying or allowing individuals to be identified constitutes personal data and requires a lawful basis for processing. In the context of an arbitration under the GDPR, the lawful basis is likely to be based on legitimate interests (*see* **Section II.B.3.c(1)**).

E. DATA TRANSFER RULES

In addition to a lawful basis for data processing, EU-style data protection laws require a *lawful basis for third-country data transfers*.

This is one of the most obvious ways that data protection laws apply to international arbitrations. Given the transnational nature of international arbitration, it is common for an arbitration to involve Arbitral Participants from different jurisdictions, who are subject to different data protection regimes. Each personal data transfer to each different region or country typically must have a lawful basis.

EU-style data protection laws restrict the transfer of data to third countries to ensure that individuals receive a universal level of rights under the laws and that a party does not circumvent its legal obligations by transferring data to a jurisdiction where the standards of protection of personal data are lower. The same restrictions may also apply to data transfers to international organisations, as is the case in the EU.[44] Some countries, including China and Russia in some instances, may apply a more stringent transfer regime, essentially prohibiting most data transfers out of the jurisdiction in certain circumstances.

By way of example, below are four scenarios in which third-country data transfers are allowed under the GDPR:

1. First, third-country transfers are allowed if the country has been deemed by the EU Commission to provide an adequate level of data protection (*i.e.*, the country is the subject of an "adequacy decision");[45]

44. GDPR Art. 44.
45. An "adequacy decision" refers to a decision by the European Commission that a third country's data protection laws are considered to be adequate. An adequacy decision allows data to be transferred outside the EU/EEA or to an international organisation without any further authorisation or notice because adequate protections apply as a matter of law (GDPR

2. Second, if data is to be transferred to a country without an adequacy decision, one of the expressly listed "appropriate safeguards" should be put in place where feasible, which in the case of arbitration most likely would be the "standard contractual clauses" (*see* Annex 6);[46]
3. Third, where there is no adequacy decision and appropriate safeguards are not feasible either, a specific derogation can be relied on, which in the case of arbitration will often be the legal claims derogation, allowing transfers where "necessary for the establishment, exercise or defence of legal claims", and provided that the other conditions for the application of that derogation are met including that the transfer is occasional, necessary for the arbitration, and that the personal data has been minimised;[47] and
4. Lastly, if none of the express derogations is applicable, a party may rely on its "compelling legitimate interests" as a basis for the transfer of data. However, this is a high threshold to meet, and also requires notification to both the data subjects and the supervisory authority, which means that it is unlikely to be often applied in practice in international arbitration.[48]

As set forth below in Section II, where an EU-style data protection law applies, the basis relied upon for third-country data transfers should be established at the outset of the proceeding to avoid issues at a later stage.

Example: In an arbitration between a Brazilian company and a French company under the rules of an EU arbitral institution, arbitrators are appointed from the EU, Brazil and the USA. The EU arbitral institution and EU-residing arbitrator will have to comply with the GDPR's data transfer restrictions for data transfer to the Brazilian and USA based arbitrators. Since neither Brazil nor the USA is deemed to provide adequate protection, standard contractual clauses or another adequate safeguard should be put in place where feasible. If that is not feasible, the legal claims derogation can be relied upon, in which case certain requirements must be met, including that the transfer is occasional, necessary for the arbitration, and that the personal data has been minimised. The Brazilian arbitrator will also have to comply with the data transfer

Art. 45(1)). The most recent adequacy decision prior to the publication of the Roadmap covered the UK after Brexit.

46. As described in Annex 6, the standard contractual clauses include the most important obligations under the GDPR, in which case data can be transferred outside the EU without any further protections because adequate protections apply as a matter of contract..
47. GDPR Art. 49(1)(e).
48. GDPR Art. 49(2); EDPB, "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679", 6 February 2018 ("Data Transfer Guidance").

restrictions in the Brazil Act whenever personal data covered by that Act is transferred to the other Arbitral Participants, and the US arbitrator will need to consider what data protection laws apply to them and what can be done to facilitate personal data transfer during the arbitration, including entering into standard contractual clauses if requested to do so.

F. DATA PROTECTION PRINCIPLES APPLICABLE IN ARBITRATION

As a survey of all data protection laws in force globally is not feasible, the Roadmap focuses on nine principles of data protection law that are common to EU-style data protection laws adopted around the world:[49]

1. **Fair and Lawful Processing.** Personal data must be processed in a manner that is fair and lawful, which means that data can only be processed if there is a lawful basis for it (as discussed in **Section I.D**).

2. **Proportionality.** Data protection laws should be applied in a proportionate manner, taking into consideration the rights and interests of the data subject, as well as the rights and interests of third parties, for example, including parties to the arbitration and the need for fair and efficient administration of justice, keeping in mind that in all cases adequate protection must be afforded to the data subject and their personal data.

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

4. **Purpose Limitation.** Personal data may only be collected for a specific and legitimate purpose and may not be processed in a manner that is not compatible with that purpose.

5. **Data Subject Rights.** Individuals whose personal data is collected and processed have the right to access their personal data and other important rights with respect to the processing of their data.

---

49. These principles overlap to some extent, and the list could be expanded, but they are common to most data protection laws around the world. In the EU, these principles are consolidated in Articles 5 and 12–22 of the GDPR, and in Brazil in Article 6 of the Brazil Act. *See, e.g.,* Daniel Cooper and Christopher Kuner, "Data Protection Law and International Dispute Resolution", 382 Recueil des cours/Collected Courses of the Hague Academy of International Law 9-174 (2017), at 43 (describing similar principles as they applied under the Data Protection Directive).

6. **Accuracy.** Personal data that is collected and processed must be valid, relevant, complete for the purposes for which it is used and must be kept up to date.

7. **Data Security.** Data controllers must take appropriate technical and organisational security measures to protect personal data against the potential risks involved in processing, including procedures in the case of data breach.

8. **Transparency.** Data subjects have a right to information regarding the processing of their personal data, which includes the right to be notified that such processing is taking place and their rights under the relevant law.

9. **Accountability.** Data controllers are required to keep a record of their data protection compliance efforts in order to demonstrate compliance.

The remainder of this Section considers each of these nine principles in turn.

1. Fair and Lawful Processing

Personal data must be processed fairly and lawfully in relation to the data subject.

As discussed in the preceding Section, lawfulness entails that personal data may only be processed if there is a legal basis for it.

With respect to fairness, the notion of fairness in data protection law aims to ensure that personal data is processed typically only in ways that data subjects would reasonably expect. The data subject's expectations are framed by considerations such as: (1) how the personal data was obtained; (2) whether they have been notified; (3) if notice was given, what purpose for the processing was notified to them; and (4) whether they could have expected that their personal data would be used in the manner in which it is being used. The notion of fairness also entails that personal data cannot be used in a manner that has an unjustified adverse effect on the data subject (note that the processing can have adverse effects, provided they are justified).

In the arbitration context, fairness triggers the question as to whether the data subject, whose data is processed during the arbitration, could have anticipated the processing thereof in view of how it was collected and the notices given to the data subject. It will also take into account whether processing will have adverse effects on the data subject that are not justified by the needs of the processing for the arbitration. This may depend on the role the data subject played in the underlying dispute as well as in the arbitration.

Example: Email correspondence is submitted in an arbitration, identifying individuals who are employees of the parties. The emails also identify other data subjects who are not employed by either party. Applying the fairness principle, the party and its counsel that are processing the document for the arbitration should query: (1) whether, considering all the facts, the individuals would have expected this processing; (2) whether it will have adverse consequences for them; and (3) if so, whether the consequences are justified. While the outcome will depend on the nature of the personal data in question and the purposes of the use in the arbitration, the fairness doctrine will typically not prevent personal data most commonly found in business email correspondence from being adduced as evidence (although culling and redaction/pseudonymisation may be required in certain circumstances).

2. Proportionality

As a general matter, data protection laws are intended to be of a mandatory nature. Yet, the fundamental right to the protection of personal data is not an absolute right. Under the GDPR, this requires consideration of the nature, scope, context and purpose of processing and the risks posed to the data subject, taking into consideration the nature and extent of the personal data being processed (*e.g.*, GDPR, Recital 4, Art. 24).[50] This "proportionality principle" is found throughout many modern data protection laws.

Proportionality cannot lead to the inapplicability of data protection laws, but rather may impact how data protection laws should be given effect based on the context of the data processing, the risk posed to the individual whose data is being processed, and the nature and extent of the personal data being processed.

In the context of an arbitration, this means that, where the law so provides, consideration should be given to the rights and interests of the data subject, the rights and interests of parties to the arbitration, those of third parties, and the need for a fair and efficient administration of justice.

Depending on the context, relevant considerations could be, among others: (1) the type of personal data being presented in the arbitration; (2) what risks the processing for the

50. *See*, for the EU, European Data Protection Supervisor, "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data", https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (Dec. 19, 2019); *see also* Handbook on European Data Protection Law, European Union Agency for Fundamental Rights (2018).

arbitration poses to the data subject as an individual; (3) what purpose for the processing was notified to them; (4) whether they are involved in the arbitration; (5) how the personal data was collected; and (6) what were/are their expectations about the processing of that data based on the notices they have been provided. Consideration should also be given to the parties' rights and interests at stake in the arbitration, as well as those of third parties that may be impacted.

In practice, for example, proportionality would generally entail that sensitive data (such as medical records) is subject to a higher level of protection than business related personal data (such as business email communications) because the data subject could reasonably expect data contained in professional email correspondence may be processed for a legal claim, while such expectation may be much less obvious for the data subject's medical records depending on the case. Moreover, the risk posed to the data subject may be greater from the processing of their medical records compared with standard business correspondence.

However, although the means by which the data protection rules are applied may vary based on the rights at stake and the risks to the data subject, this does not mean that those rules do not apply, but rather that the manner in which they are applied may vary – for example the extent of the security requirements to be applied or how much data minimisation is required. In all cases, however, adequate protection must be afforded to the data subject and their personal data.

3. Data Minimisation

The concept of data minimisation is fundamental to EU-style data protection regimes. For example, Article 5(1)(c) of the GDPR states that "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".[51]

In the context of arbitration, data minimisation is required in all stages of the arbitral process. Data minimisation requires Arbitral Participants to ensure that the amount and type of personal data processed is adequate, relevant and limited to what is necessary for the lawful purpose of the processing (*i.e.*, preparing a case for arbitration, prosecuting, defending against, or deciding a claim, administering the proceedings, or retaining data in relation to the arbitration after completion of the proceedings).

---

51. According to Article 18(IV) of the Brazil Act, for example, data subjects have the right to obtain the anonymisation, blocking or deletion of unnecessary or excessive data or data processed in a manner that is not compliant with the law.

Data minimisation obligations are particularly relevant in the selection, production and disclosure of documents. It remains to be seen whether in practice timely and more extensive culling for relevance and redaction of unnecessary personal data will become more widespread as a result of EU-style data protection laws, keeping in mind that document production for arbitration is more limited than in litigation.

Example: A law firm asks its client (a potential party to an arbitration) to provide a copy of the email boxes of anyone potentially related to the transaction at issue in a potential arbitration from the time the transaction was first contemplated until the present time. The data minimisation principle requires both client and law firm to consider whether the personal data likely to be contained in the email boxes is relevant for the purpose of bringing or defending the claim and whether the request has been limited to what is necessary for the purpose of bringing or defending a claim in arbitration. If not, efforts should be made to limit: (1) the volume of data collected, for example by restricting date ranges to the most relevant time periods and custodians to those specific employees who were directly involved in the transaction in question; and (2) the amount of personal data that is included.

In the case of the GDPR, for example, if the law firm is based in the US and the party in the EU, this will also raise third-country data transfer concerns.[52] Standard contractual clauses or another adequate protection should be put in place where feasible, and where this is not feasible, transfer may be lawful on the basis of the legal claims derogation on certain conditions. In terms of what conditions may apply when the derogation is relied on, the transfers must be occasional and, for example, the EU Working Party provided guidance in the context of data transfers to the US for purposes of discovery for US litigation, setting out that the data set should be culled for relevance,[53] efforts should be made to redact or pseudonymise personal data[54] and confidentiality provisions put in place where possible *before* the transfer is made.

52. Under the GDPR, a "third country" means any country outside of the European Union and the EEA, including, for example, the US and the UK after Brexit.
53. "Culling" means filtering data.
54. "Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. *See* GDPR Art. 4(5); Brazil Act Art. 13 Paragraph 4; California Act Sections 1798.100(e), 1798.140(r), 1798.145(i).

4. Purpose Limitation

The principle of purpose limitation is related to the transparency requirement, in that the data subject should receive a notice, identifying the purpose of the processing of their personal data. The subsequent processing activities should then be limited to the purpose that was notified to the data subject. [55]

Typically, a large portion of personal data contained in documents exchanged during an arbitration will be personal data of the parties' employees/staff, clients or business counterparties, gathered in the context of the ordinary business or other activities that led to the dispute. The evidence processed by a party will normally not have been created for the purpose of bringing a claim, but is collected and processed for use in an arbitration.

If personal data is processed by Arbitral Participants who did not originally collect the data, which is often the case, the possibility of processing for the purpose of the arbitration must either have been included in the original notice given to the data subject or be compatible with the purpose identified therein.

For example, under the GDPR, the factors to be considered when deciding whether further data processing is compatible with the originally notified purpose are: (1) the presence of any link between the original purpose and the new purpose; (2) the context in which the data was collected ("in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use"); (3) the nature of the personal data (for example, business correspondence and documents as opposed to patient medical information); (4) the possible consequences of the further processing; and (5) the existence of appropriate safeguards.[56]

Deciding whether the purpose is compatible with the originally notified purpose involves a fact-specific analysis. Compatibility depends on the original purpose notified to the data subject. For example, the use of employee and business-related information in an arbitration, in which the specific data subject's actions are at issue, may well be compatible with the purpose for which the data was originally processed, given their role in the organisation. Depending on the employee's role, they may have known or expected that information containing their personal data could potentially be processed for legal proceedings. This may be the case where the personal data is contained in business emails and other business correspondence and documents. Making this determination depends

55. GDPR Art. 5(1)(b) states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ('purpose limitation')".
56. GDPR Recital 50.

on the purpose for which the data was originally collected. Although not determinative, it is helpful if the data subject was informed in advance of the possibility that their personal data could be used in a dispute resolution procedure.

In the EU, Member States can derogate from the application of the purpose limitation. In Germany, for example, controllers are permitted to process personal data for a purpose other than the one for which the data was collected where the legal claims derogation applies,[57] unless the data subject has an overriding interest in not having the data processed.[58] In Brazil, new uses – for other purposes – of personal data made manifestly public by the data subject are permitted, provided that the purposes for the re-processing are legitimate, that the data subject rights are guaranteed, as well as that the fundamental rights and principles set out in the Brazil Act are preserved.[59]

Example: When the General Counsel was hired at Company X, they were informed that their personal data would be processed where necessary in the normal course of their activities as General Counsel. They have now left the company. A dispute arises with Company Y and an arbitration is commenced. Company X would like to submit evidence in the arbitration that contains the General Counsel's personal data, including their signature on a contract, minutes of meetings they attended and emails they exchanged. The further processing of their personal data for purposes of the arbitration would be within the scope of their function at the company as notified to them. Hence, it would likely fall within the purpose limitation.

5. Data Subject Rights

EU-style data protection laws, including for example, the GDPR and the Brazil Act, grant data subjects important rights with respect to the processing of their personal data, several of which are likely to apply to Arbitral Participants. Data subject rights is an area in which there are significant differences among countries with EU-style data protection regimes.[60]

57. Meaning that the processing is "necessary for the establishment, exercise or defence of legal claims".
58. German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 Section 24.
59. Brazil Act, Art. 7, Para. 7.
60. Art. 18 of the Brazil Act lists the main data subject rights in Brazil, which are similar to those in the GDPR.

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

- The right of access and to obtain a copy of the personal data being processed (also referred to as a "data subject access request"),[61] except that "[t]he right to obtain a copy … shall not adversely affect the rights and freedoms of others";[62]
- The right to request modification of their data, including the correction of errors and the updating of incomplete information;[63]
- The right to withdraw consent if consent was the basis for processing, provided that "[t]he withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal";[64]
- The right to object to data processing where the lawful basis relied upon is a legitimate interest, in which case the controller should demonstrate that a compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject;[65] and
- The right to erasure – also referred to as the right to deletion or the right to be forgotten – which allows a data subject to request, under certain circumstances, that their personal data be erased.[66]

Arbitral Participants subject to the GDPR should also keep in mind that national laws may provide derogations from the GDPR, which may impact the extent of the data subject rights in arbitration proceedings.

Example: An individual who acted as a sub-contractor to the claimant makes a data subject access request to respondent's counsel (or the tribunal) requesting access to all personal data about them that has been processed in the context of the arbitration proceeding. Under the GDPR, for example, respondent's counsel (or the tribunal) must address the request without undue delay and in any event within one month, unless extended. The responding party should bear in mind, however, that the right to electronic access or to obtain a copy "shall not adversely affect the rights and freedoms of others" (GDPR Art. 15(4)) and that it must consider its own legal and ethical obligations before providing the requested information. This may affect whether documents

61. GDPR Art. 15; California Act Sections 1798.100(d), 1798.110, 1798.115.
62. GDPR Art. 15(4).
63. GDPR Art. 16; in contrast to the GDPR, no right of rectification exists under the California Act.
64. GDPR Art. 7(3).
65. GDPR Art. 21; California Act Section 1798.120.
66. GDPR Arts. 12, 17; California Act Sections 1798.105, 1798.130(a), 1798.145 (g)(3).

or document extracts are provided to the sub-contractor, and if so which ones. The responding party should also consider whether an exception applies under national law (for example, in Germany with respect to privileged information). Considering these issues before they materialise through Data Protection Directions will help minimise any impact on the process (*see* **Section II.B.3.c** and **Annex 7**).

6. Data Accuracy

Data controllers are expected to take all reasonable steps to ensure the personal data they process is not incorrect or misleading as to any matter of fact.[67] There is also a general obligation to keep the personal data up to date, although this will depend on the purpose of the processing (for example, in an arbitration, it should not be required to update personal data in the record about facts which occurred in the past, unless it becomes clear that the facts in the record are wrong or misleading). If it comes to light that personal data is incorrect or misleading, reasonable steps should be taken to promptly correct or erase it.

Example: Evidence is submitted in an arbitration including evidence involving an employee of the respondent, for which the claimant submits emails and photographs as evidence. The employee claims that the evidence has been falsified and brings a data subject request to the claimant, claimant's counsel, the institution and the tribunal asking that their personal data be corrected. This question is complex, and addressing these issues will be highly case specific, but advance planning, for example, through the adoption of Data Protection Directions may limit any negative impact the rights request will have on the arbitration (s*ee* **Section II.B.3.c** and **Annex 7**).

7. Data Security and Data Breach

EU-style data protection laws require all users of personal data, including both data processors and data controllers, to apply reasonable data security to personal data, referred to in this Roadmap as information security measures and in the GDPR as "appropriate

67. *See*, *e.g.*, GDPR Art. 5(1)(d): "personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')".

technical and organisational measures".[68] Deciding what security measures are "appropriate" requires consideration of the potential risk to data subjects, the existing information security measures of the Arbitral Participants, and what physical and technical measures are appropriate given the risks to the data subjects. Moreover, as part of entering into standard contractual clauses, the parties to those clauses are required to provide a description of the data security provisions that will be in place after the transfer (see Annex 6).

As discussed further in Section II, Article 32 of the GDPR imposes the primary obligation on controllers and processors to ensure that data is processed securely, which will need to be applied during an arbitration where the GDPR applies. When deciding what information security measures are appropriate, consideration must be given to the "state of the art", implementation costs, data minimisation, and the circumstances and the risk level of the processing, with a focus on the risks to the data subject.

When a data breach occurs, this raises important questions about what notification requirements apply to the Arbitral Participants. Given the risks associated with data breaches, as discussed in Section II, these questions should be addressed at the outset of the arbitral proceedings, and agreeing to a data breach protocol as part of the Data Protection Directions is usually advisable.

Example: An arbitrator involved in a case in which significant personal data has been exchanged in the record uses a personal email account with an insecure email password and no encryption. They travel frequently, fail to use a screen protector and regularly connect from public Wi-Fi and have documents printed at their hotel. It is unlikely that the degree of information security applied by the arbitrator is appropriate to protect the personal data exchanged in the arbitration and it would likely violate applicable data protection standards.

The arbitrator becomes aware that their system has been compromised and that access to all their files in 20 ongoing cases have been exposed. The arbitrator will need to comply with their obligations under any data breach protocols in place in those cases. In cases where data breach protocols are not in place, the arbitrator will usually want to promptly notify the other Arbitral Participants so they can comply with their data protection and other obligations.

After becoming aware of the data breach, each Arbitral Participant will then need to decide what notification obligations apply to them. Whether the Arbitral Participant

68. *See* GDPR Art. 32.

has a duty to notify the supervisory authority or the data subject and the extent of this duty is fact specific.

Under the GDPR, they will need to consider whether this breach is likely to result in a risk to the rights and freedoms of those data subjects whose data has been exposed, in which case they must notify the breach to the relevant supervisory authority or authorities without undue delay and, where feasible, do so not later than 72 hours after becoming aware of the breach. If the risk is high, notification is also required to the data subjects impacted (see **Section II.B.3.c(4)**).

8. Transparency

Transparency requires data subjects to be provided with notice in plain language about the processing of their personal data and the purpose for the processing. This can be done through general notices, specific notices or a combination of the two, as long as the data subject has actual notice of the processing or potential processing of personal data.

Arbitral Participants should determine what transparency requirements apply to them: (1) generally, including the publication of adequate data privacy notices; (2) when preparing a file for arbitration; (3) when initiating arbitral proceedings; and (4) during the arbitral proceedings when new personal data is introduced or processed for a different purpose. Arbitral Participants should consider issuing (or updating pre-existing) privacy notices to meet those requirements.

Privacy Notices. Even before a specific arbitration is contemplated, Arbitral Participants should consider issuing privacy notices, explaining to actual and potential data subjects why and how they process their personal data and what rights data subjects have. Privacy notices will often be posted on the Arbitral Participant's website and should address dispute resolution specifically. These notices will be aimed at third parties whose personal data is being processed. Adopting a privacy notice and posting it on the Arbitral Participant's website will often be part of complying with the obligations imposed by, for example, GDPR Articles 13 and 14.[69]

69. Annex 9 provides the structure of sample privacy notices for consideration by institutions, arbitrators and legal counsel governed by the GDPR and other countries with similar notification requirements. This Annex may be a starting point for Arbitral Participants when deciding what to put in their privacy notices, but privacy notices are fact-specific and require careful consideration and tailoring to each Arbitral Participant's particular situation, activities and needs.

Notifications. In addition to general privacy notices, Arbitral Participants who are data controllers or joint controllers are responsible for ensuring that data subjects in a specific arbitration have been provided with sufficient notification of the data processing. It is important to note that exceptions to the notification requirements may apply where a data subject has already been notified of the processing by someone else (in this case, likely another Arbitral Participant).

***Example*:** Evidence is collected for an arbitration from 25 employees identifying at least 100 individuals. Subject to consideration of other potential restrictions under applicable labour law, the transparency doctrine requires that (i) each individual identified (or identifiable) in those emails has been sufficiently notified of the processing of their personal data for the arbitration (for example when their email boxes are screened for relevant information) unless an exception applies and (ii) the processing of personal data is compatible with the purpose identified in the notice provided to them at the time of collection. However, the emails will likely also identify persons from the opposing party and individuals with no ongoing relationship to either party. Notifying those persons may be problematic. The question is whether the data subjects have been given adequate notice of the data processing, either at the time of original processing of the data in the ordinary course of business, or in the context of collection for the arbitration. If not, it needs to be considered whether there is an exemption from notice requirements in the circumstances of the particular case. In the case of confidential arbitrations, notifying third parties or even employees at the time of the dispute can compromise the confidentiality of the process or create strategic concerns. Where possible, these issues should be addressed and agreed in the Data Protection Directions (*see* **Section II.B.3.c** and **Annex 7**).

9. Accountability

Accountability requires those processing personal data to document the compliance approach they have adopted and measures they have taken towards the protection of such data. It is a central feature of the GDPR and other EU-style data protection laws.

Under the GDPR, for example, data controllers are expected to be able to "demonstrate compliance" with these principles as they are implemented throughout the GDPR.[70] Adequate records should be kept of what compliance measures were taken and why, in such a manner that they can be shown to the competent authorities if compliance issues were

70. GDPR Art. 5(2); *see also* GDPR Art. 24(1).

to arise.[71] Although the obligations of Arbitral Participants may be interrelated, they each have their own independent recording obligations. Similar provisions are found in other data protection laws that are modelled on the GDPR, such as in Brazil Act (Art. 6(X)).

As there is no specific guidance from courts or data protection authorities at present in respect of the application of data protection laws in arbitration, the documentation of the Arbitral Participants' approach and measures is particularly important to demonstrate their good faith efforts towards their compliance with data protection laws.

Example: A complaint is brought before a supervisory authority that the data processing during an arbitration violated applicable data protection laws. The supervisory authority asks the arbitral institution and the arbitrators to provide records evidencing data protection compliance during the case. A failure to be able to provide records would likely be a violation of the GDPR's or Brazil Act's accountability principle. Arbitral Participants should therefore agree to how records will be kept of the steps taken to comply with applicable data protection laws in a manner that can be shown to a competent authority.

71. Organisations with more than 250 employees must document compliance in accordance with Article 30 of the GDPR, which provides a list of record-keeping obligations.

II. DATA PROTECTION COMPLIANCE IN INTERNATIONAL ARBITRATION PROCEEDINGS

Based on the overview in Section I describing the general framework for the application of data protection laws and principles to arbitration and Arbitral Participants, this Section II considers how data protection compliance may affect a specific arbitration and the implications for Arbitral Participants from the time that a party starts to prepare for the arbitration, until the case has been concluded and the documents are stored or destroyed.

This Section II is organised around the typical procedural steps of an arbitration. It should be considered together with the Annexes, which contain samples of privacy notices, generic language to be considered for Data Protection Directions and Data Protection Protocols, as well as non-exhaustive checklists of issues that parties, their legal counsel, institutions and arbitrators may want to consider in establishing whether data protection laws apply to them and how they can be complied with in the context of the arbitration proceedings.

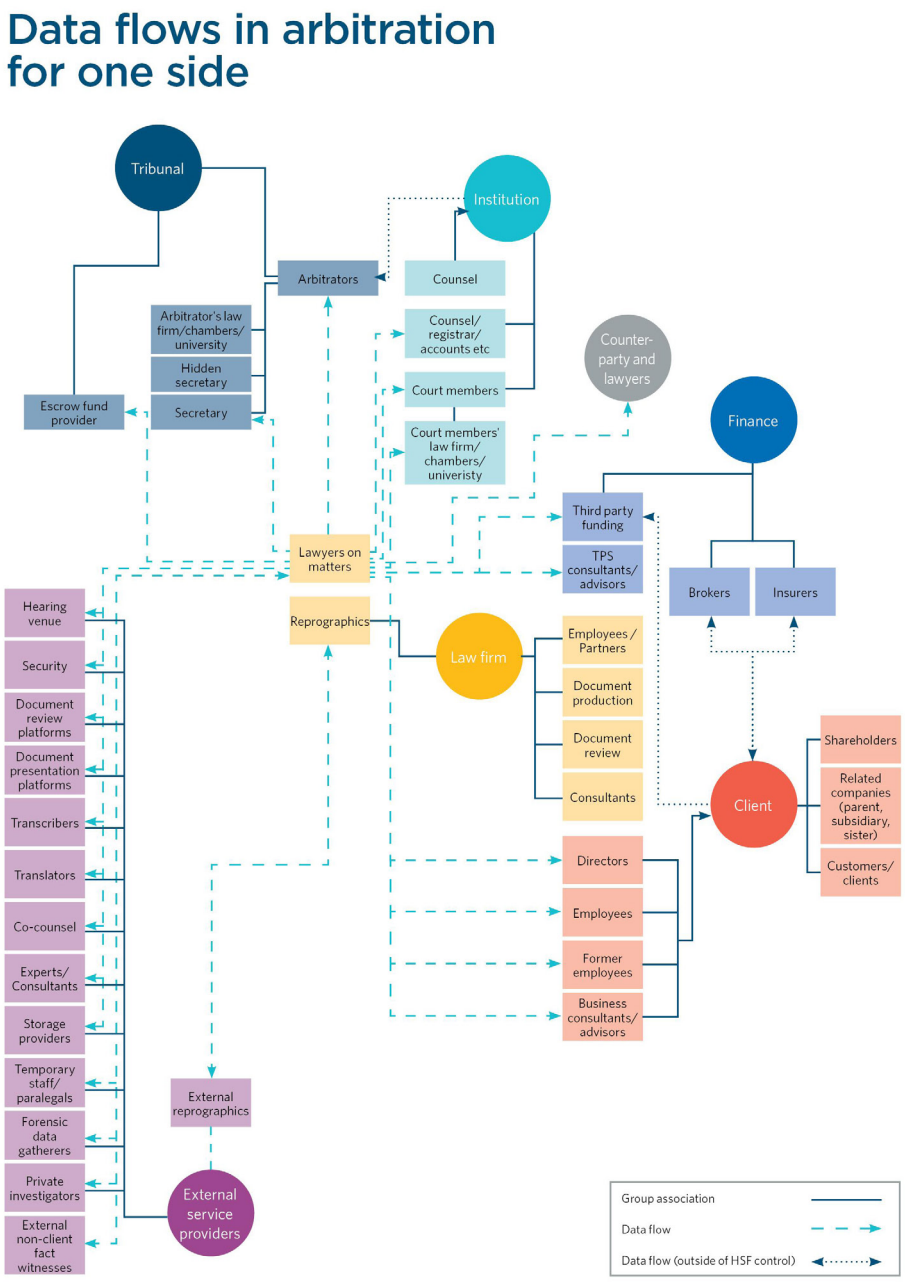
Arbitral Participants should consider from the outset what data protection laws will apply to them and the other Arbitral Participants. For the parties and their legal counsel, that moment may be prior to the initiation of the arbitration when they start to prepare the case. For the institution, applicability should be considered as of the moment a party indicates that it is or may be starting an arbitration. For the arbitrators, that moment is when they are contacted with a view to their appointment as arbitrator in a specific case. In organisations that have appointed a data protection officer, which will often be the case for example in a large law firm or company, the officer may be involved in decisions regarding the protection of personal data during the arbitration.[72]

A. PREPARING FOR THE ARBITRATION

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

72. GDPR Art. 38(1).

Figure 1.


Data flows in arbitration for one side
Tribunal
Institution
Arbitrators
Counsel
Arbitrator's law firm/chambers/ university
Hidden secretary
Secretary
Escrow fund provider
Counsel/ registrar/ accounts etc
Court members
Court members' law firm/ chambers/ univeristy
Counter-party and lawyers
Finance
Third party funding
TPS consultants/ advisors
Brokers
Insurers
Lawyers on matters
Reprographics
Law firm
Employees / Partners
Document production
Document review
Consultants
Client
Shareholders
Related companies (parent, subsidiary, sister)
Customers/ clients
Directors
Employees
Former employees
Business consultants/ advisors
Hearing venue
Security
Document review platforms
Document presentation platforms
Transcribers
Translators
Co-counsel
Experts/ Consultants
Storage providers
Temporary staff/ paralegals
Forensic data gatherers
Private investigators
External non-client fact witnesses
External reprographics
External service providers
Group association
Data flow
Data flow (outside of HSF control)

1. Applicable Data Protection Laws

In preparing for the arbitration, parties and their legal counsel should consider how data protection may affect the proceedings. Determining what data protection obligations may arise in relation to the arbitration requires advance examination as to whether the various Arbitral Participants fall within the scope of a relevant data protection law.[73]

In the first place, any privacy notices issued by the Arbitral Participants will provide insight into the approach that the Arbitral Participant takes to data protection compliance, as well as their view of what data protection law may be applicable as well as their status under that law as a controller, a joint controller with other controllers or a processor.

In the second place, it is important to consider how data flows are likely to occur in the case and what the legal basis would be for any necessary data transfers that would be subject to data protection limitations. So-called "data mapping" in the arbitration context involves determining where the data processed during the arbitration is located and where it would need to be transferred and processed for the purposes of the arbitration. This mapping exercise allows parties and their legal counsel to adopt an approach to data protection compliance with a minimum impact on the arbitration.

Data Flows. *Figure 1* depicts typical data flows in an international arbitration and reveals how extensive and interconnected they are.[74]

For example, where an Arbitral Participant in the EU transfers data to another country or jurisdiction, they will want to consider the lawful basis for the transfer, including whether the country has been found by the EU to provide adequate protection (*see* **Section II.B.3.c(2)**). If this is not the case, the Arbitral Participant should consider whether it is feasible to enter into standard contractual clauses to permit the transfer. Where this is not feasible, the Arbitral Participant may be able to rely on the legal claims derogation for the transfer, in which case it will need to consider the extent to which it needs to review, minimise, cull and potentially redact personal data before transferring a more limited data set to Arbitral Participants located outside the EU.

---

73. In the case of arbitrations administered by an international organisation, *see* fn. 6.
74. This chart was first published by Herbert Smith Freehills LLP (HSF) in Inside Arbitration – Issue 8, dated 16 July 2019 and is reprinted with permission.

2. Roles of Arbitral Participants

Data protection obligations fall on the individual Arbitral Participants, rather than governing the arbitration proceedings as such. However, the interlinked nature of compliance means that when any Arbitral Participant is bound by data protection laws, this is may have an impact on the other Arbitral Participants and the process. This makes it important to identify potential issues early, even if no action is required.

Parties should form a view early in their case preparation as to which of the Arbitral Participants are likely to be processing data during the arbitration and whether they will do so as controllers (generally in parallel with other controllers), processors, or potentially joint controllers. After the arbitration commences, each Arbitral Participant will need to determine their own status and ensure that they comply with their data protection obligations under the law applicable to them (*see* **Section I.C**).

For example, once an Arbitral Participant receives copies of a party's submissions and evidence, it likely becomes a data controller of the personal data contained therein (often in parallel with other controllers) or, depending on the circumstances, joint controllers as far as their arbitration activities are concerned. On the other hand, tribunal secretaries, e-discovery professionals, transcribers, interpreters, online case management platform providers, remote hearing platform providers and other service providers (not being employees of the Arbitral Participants) may be considered data processors, depending on who directs the purposes and the means of the data processing.

3. Use of Service Providers

Arbitral Participants often use third-party service providers to render services in relation to the preparation and conduct of an arbitration, all of whom may have access to parts of the record. Examples include:

- Arbitral Participants may engage network, cloud hosting and data platform service providers, and other independent contractors;
- Parties and their legal counsel may engage e-discovery professionals, translators, transcribers, online case management platform providers, and remote hearing platform providers;
- Parties, their legal counsel, and arbitrators may engage experts who are likely to be considered data controllers themselves;[75]
- Arbitrators may engage *ad hoc* tribunal secretaries or other assistants (who are not employees of their firm); and

75. *See*, *e.g.*, Controller/Processor Opinion at 28.

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

The personal data related to the arbitration will need to be processed, and may also need to be transferred, by each of these third-party service providers in order for them to provide their services. Depending on who controls the purpose and means of the processing, some of the above service providers (for example, experts) may be considered data controllers in their own right, while others are data processors acting only under the instructions of the data controller (*see* **Section I.C**). In all cases, it will be important that relevant data protection laws are complied with. Specifically for data processors, it will be important that they enter into an EU-compliant data processing agreement with the Arbitral Participant who is the controller.

4. Data Collection and Review

When a dispute arises, the first thing that parties and their legal counsel typically do is to review the facts by going back through the chain of events that led to the dispute. This often involves the review of emails, other communications (texts, WhatsApp messages, etc.) and other contemporaneous evidence of the relevant events. Moreover, in advance of the arbitration, the potential for disclosure during the arbitration may require the parties and others to suspend their usual data destruction policies or to make changes to their usual retention or deletion processes to cater for a "litigation/arbitration hold" in contemplation of arbitration proceedings.

The act of collecting or obtaining documents for the purpose of preparing for an arbitration, or in the context of an arbitration in a broader sense, will constitute processing of the personal data contained in the documents. This means that during the document collection and review process, parties and their legal counsel will need a lawful basis for their data processing activities, as well as a lawful basis for any third-country data transfer that may be necessary in that framework. For example, third-country data transfers during the preparation or prosecution of an arbitration between a party and their lawyer, between the offices of a law firm, between co-counsel, or between opposing counsel all require a lawful basis, in which case standard contractual clauses or other adequate protection measures can be put in place to ensure compliance.

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

(4) the lawful basis for processing that data for the arbitration; (5) how applicable transparency obligations have been, or can be, complied with, including whether it is feasible to provide additional notices without infringing the parties' rights or the integrity of the proceedings; and (6) the steps to minimise the processing of personal data to what is necessary for the lawful basis pursued (*e.g.*, by limiting data collection to specific custodians, data ranges or applying search terms, redaction, pseudonymisation, etc.).

Online case management platforms, which will often be administered by a third-party provider, can assist Arbitral Participants to comply with their data protection obligations. The consistent use of an online case management platform can make it easier to comply with these obligations – the relevant data flows and data security arrangements can be discussed beforehand with the platform provider (*e.g.*, using the questionnaire at Annex 4, Online Case Management Platform Provider Checklist). Once the purposes and manner of processing arbitration data has been agreed, user access permissions can help to ensure that data is shared only with necessary parties and only for as long as is necessary. Furthermore, as discussed below in **Section II.B.3.c(8)**, online case management platforms can also assist with discrete data protection obligations during the course of the proceedings.[76]

B. DURING THE ARBITRATION

This Section considers on a step-by-step basis how data protection obligations may affect Arbitral Participants and the conduct of the arbitration after an arbitration is initiated.

1. Filing the Request for Arbitration

The first step in an arbitration is filing the request for arbitration or the equivalent thereof, which will include personal data. The filing of the request for arbitration thus falls squarely within the realm of data processing.

***Ad hoc* Arbitration**. In the case of an *ad hoc* arbitration, the request for arbitration is typically filed directly with the opposing party at which point the relevant data protection obligations come into effect. In *ad hoc* proceedings, at least after the appointment of the tribunal, communication is directly with the arbitrator(s), which will also involve the processing and transfer of personal data.

76. For further information on the drivers for using online case management software in arbitration, reference can be made to the "Protocol for Online Case Management in International Arbitration' Working Group on LegalTech Adoption in International Arbitration (2020) ("**Online Platform Protocol**").

Institutional Commercial Arbitration.[77] In the case of institutional commercial arbitration, the request for arbitration will typically be filed with an arbitral institution. The filing of the request for arbitration will amount to the processing and transfer of the personal data contained in the request. This means that from the time that the arbitral institution receives the request, it becomes bound by the relevant data protection laws applicable to it.

In an institutional arbitration or in arbitrations where recourse to an appointing authority is anticipated, parties should consider whether it may be helpful to raise the potential impact of data protection laws on the arbitration with the institution in advance of the filing. This is especially necessary in cases where the filing of the request raises data protection concerns, data security is in doubt, or where the transfer of the file to the opposing party could raise a data protection concern.

The first step for arbitral institutions is to consider and determine as a general matter what data protection law(s) apply to them, if any. If the institution is subject to the GDPR or a similar data protection regime, and is not exempted, it will typically become a controller of the data set included in the claimant's request for arbitration and the subsequent filings, at least for certain purposes. From that point onwards, when processing personal data, the arbitral institution must comply with the applicable data protection law, as described in Section I.

In this regard, institutions need to consider their potential data protection obligations at the time of the receipt of a request for arbitration; the registration and/or administration of arbitrations; the appointment of arbitrators; the receipt of advances and fundholding for arbitration and administration costs; the disclosure of data to parties, their legal counsel and arbitrators; the processing of data during the arbitral process; any challenge decisions of the institution; the scrutiny, approval, issuance or publication of awards or excerpts thereof; and data retention or deletion policies (including retention for archiving purposes).

In practice, where the GDPR applies, for example, the institution will need to have a lawful basis for the processing of personal data and any transfer outside the EU, appropriate data security measures, a system for the exercise of data subject rights and to maintain adequate records, as well as data breach and data retention policies. These obligations may affect the manner in which institutions are able to publish awards and decisions and to archive personal data.

77. In the case of arbitrations administered by an international organisation, *see* fn. 6.

If the institution is covered by the GDPR, for example, all these aspects of processing should be included in its privacy notice, which must comply with GDPR Articles 13 and 14. It is good practice to post and update the arbitral institution's privacy notice on its website. Data protection may also be addressed in the arbitration rules and specific explanatory notes that institutions publish from time to time for reference by parties, counsel and arbitrators.

Annex 9A contains an example of a notice that arbitral institutions subject to GDPR or a similar law (that are not an international organisation) may consider, and many of the issues addressed therein will also be relevant to non-EU based institutions.

Example: An arbitral institution in the EU sends the name and contact details of an arbitrator to a potential claimant in Egypt. Egypt is not the subject of an EU adequacy decision and the institution does not have any standard contractual clauses (or any of the other permitted appropriate safeguards) in place with the potential claimant. Because the transfer contains personal data, the transfer would need to be justified under one of the permitted derogations, for example, because the transfer of personal data is "necessary for the establishment, exercise or defence of legal claims".

2. Appointment of Arbitrators

When selecting arbitrators for cases in which the GDPR or other relevant data protection law(s) may apply, best practice is for those making the appointment to consider how it will implicate the application of the relevant data protection laws. Where the potential arbitrator is not subject to the same data protection obligations as the other Arbitral Participants, it would be prudent to consider how this will be managed during the arbitration and whether steps should be taken as part of the appointment to ensure that data can freely be transferred during the proceedings (for example through standard contractual clauses).

Potential arbitrators will also have to process the personal data of parties, legal counsel, and other arbitrators. They will do so when, for example, carrying out conflict checks and making any disclosures relevant to their impartiality and independence as may be required by applicable procedural rules and their legal professional obligations. If appointed, data processing will be carried out on an ongoing basis during the arbitration.

Before an arbitral appointment is made, personal data is often exchanged about potential arbitrators by arbitral institutions, international organisations, parties and their legal

counsel. Most of this data is obtained from the public domain, and some may be based on word of mouth or other sources.

The general privacy notices of Arbitral Participants (like institutions) who possess, use, disclose and transfer the personal data of potential arbitrators should put potential arbitrators on notice that their personal data may be processed and transferred during the selection and appointment process and indicate the legal basis for such processing. Institutions may consider including specific notices as part of any procedure for potential arbitrators to be considered for appointment, for example when lists are employed.

In addition to any standard notice, once an arbitrator is otherwise made aware they are being considered for appointment, it is best practice to put them on express notice that their personal data is being processed for this purpose, especially in cases of third-country data transfers. Note that this is a mere notice, not consent. Asking arbitrators to consent to data processing and transfer triggers risks associated with relying on consent that will be further discussed below (*see* **Section II.B.3.c(1)**). If it is decided that an appointment will be made, as mentioned above, consideration should be given to whether the use of standard contractual clauses should be raised.

3. Documenting Data Protection Compliance

a. First Procedural/Case Management Conference (referred to collectively as "CMC")

Once the arbitration is underway, Arbitral Participants should promptly consider and attempt to agree how data protection compliance during the proceedings will be addressed. The earlier the existence of, and the allocation of, responsibilities for compliance with data protection obligations is settled or decided, the lower the data protection risks and the impact on the proceedings.

In order to ensure the orderly conduct of the arbitration and compliance with applicable data protection laws, the tribunal and the parties will need to address some, if not all, of the issues addressed in Section I at the CMC. This is required or recommended by the rules of most major international organisations (including for example, the LCIA and the ICDR) and the most recent version of the IBA Rules on the Taking of Evidence, which was adopted in 2020 ("**IBA Rules**"). The IBA Rules provide that the parties should consult on evidentiary issues, including the "treatment of any issues of cybersecurity and data protection" early in the process. The Commentary on the IBA Rules expressly suggests that parties and tribunals may want to consult this Roadmap and the ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitration (2022 Edition) ("**Cybersecurity Protocol**") when considering these issues.

In cases where data protection laws may apply to one or more Arbitral Participants, which is often the case, data protection compliance should be put on the agenda of the CMC. As a practical matter, arbitrators that are not themselves bound by any data protection regime (for example those based in the parts of the United States where no such general regime is in place) may be inclined to avoid a discussion of data protection at the CMC if it is not raised by the parties. This is inadvisable as a matter of sound case management because, for example, a party could decide as a strategic matter not to raise data protection concerns during the first procedural conference but may later raise data protection issues in the context of the production of documents or other obligations during the arbitration, at which point it may be more difficult to manage such issues.

b. Data Protection Protocol/Procedural Order 1/Terms of Reference Directions

In the interest of compliance with data protection laws, as well as time and cost efficiency of the arbitration, data protection issues are best addressed and managed from the outset at the first CMC and then set forth either in a procedural order, terms of reference, or in a data protection protocol (referred to collectively as "**Data Protection Directions**").

The term "**Data Protection Protocol**" refers to a document agreeing on how data protection is to be applied in a particular context, if possible, signed by all Arbitral Participants, and potentially included by reference in the first procedural order or terms of reference (*see* Annex 8 for sample language that may be considered). To the extent permissible under the applicable law(s), the Arbitral Participants may wish to allocate roles and responsibilities in relation to data protection compliance, recorded in a data protection protocol. These types of agreements are widely used to ensure compliance among controllers with parallel and interlinked obligations, as is the case in arbitration. A data protection protocol is required by the GDPR where some or all of the Arbitral Participants are joint controllers.

Where a data protection protocol is not employed, another possibility is to set data protection compliance standards in a procedural order or terms of reference. Although this is highly case and fact specific, Annex 7 provides sample language that may be considered for inclusion in a procedural order or terms of reference using the GDPR as an example (and this language may also form part of a data protection protocol). A procedural order may also be used by the arbitral tribunal to issue Data Protection Directions, all with the underlying goal of enabling the data protection rules to be applied in an orderly manner and preventing parties from using them to delay or disrupt the proceedings.

The question as to whether data protection should be addressed in a procedural order, terms of reference, or in a data protection protocol is case specific. Many cases do not have terms of reference. Furthermore, a signed data protection protocol may be unachievable

in practice and may not be justified in smaller cases or where data protection is unlikely to be a major issue. On the other hand, in other cases, even small ones, a data protection protocol may be required (for example by joint controllers in the EU).

Regardless of the size of the case or the type of Data Protection Directions employed, such directions assist in resolving issues that may subsequently arise about how data protection compliance may impact the proceedings.

Annex 7 includes sample language for Data Protection Directions when the GDPR applies and Annex 8 contains a sample data protection protocol, and Annex 3 contains a checklist of items to be considered for data protection compliance during an arbitration.

c. Issues for Data Protection Directions

This Section will briefly consider the most important data protection issues to be considered at the CMC and recorded in Data Protection Directions from the perspective of compliance and ensuring orderly proceedings, including: (1) lawful basis for processing; (2) lawful basis for data transfer; (3) disclosure or production of documents; (4) data security and data breach protocols; (5) managing data subject rights; (6) notification; (7) documenting data protection compliance; and (8) any use of online case management platforms to assist with compliance. This is not an exhaustive list, and some of these issues may be more important than others in specific cases. However, these are issues which if not addressed early can create problems down the road either from a compliance or case management perspective. Although this is highly case and fact specific, Annex 7 provides sample language addressing each of these issues that may be considered for inclusion in Data Protection Directions using the GDPR as an example.

(1) Lawful Basis for Personal Data Processing

Arbitral Participants should identify and document at the outset of proceedings what data will need to be processed for the arbitration and the lawful basis that will be relied upon for the processing of any personal data, sensitive data, and criminal offence data during the arbitration. Arbitral Participants should be aware that a specific identified purpose is required for the processing of personal data and the use of catch-all provisions referring to numerous alternative bases is generally not allowed.

As discussed below, the lawful basis may vary depending on the relevant data protection law that is applicable. Some data protection laws have established a specific lawful basis for data processing of personal data and/or sensitive data and/or criminal offence data for arbitration. This is the case in Brazil. It is also the case under the GDPR with respect to sensitive data and for some EU Member States with respect to criminal offence data,

where there is a lawful basis in relation to making or defending legal claims (which is likely to apply to arbitration). In other cases, where a legitimate interest is relied upon as a lawful basis for the processing of personal data, a Legitimate Interests Assessment should generally be undertaken and documented (as is recommended for personal data under the GDPR) (*see* Annex 5).

In most jurisdictions, the lawful basis for data processing can be met by obtaining the consent of a data subject. However, under the GDPR and many other EU-style data protection laws, this needs to be informed consent in the case of general personal data processing and explicit consent in the case of sensitive data. Consent can always be withdrawn.[78]

Moreover, although the arbitration community frequently relies on consent for other purposes, the EU Working Party has referred to consent as a "false good solution".[79] It is not recommended to rely upon consent as a lawful basis for the processing or transfer of personal data in an arbitration where the GDPR applies because:

- In order to be valid, consent must be specific, informed and freely given;
- Consent must be obtained from the data subjects themselves rather than the Arbitral Participant who provides the personal data, including each data subject identified or identifiable from the submissions or evidence (not only the parties and the witnesses);
- In an employment context, consent is likely to be an invalid legal basis for the processing of personal data; and
- Processing on the basis of consent may need to be stopped if consent is withdrawn or refused, and it is difficult to then rely on another lawful basis for processing.[80]

Due to the inherent risk that consent is refused or withdrawn at some point, it is therefore strongly preferred to rely on other legal bases. This is not to say that consent should never be employed under the GDPR, but rather that it should only be used as a basis for

78. "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them (GDPR Art. 4(11)). A similar definition is found in Art. 5(XII) of the Brazil Act.
79. EU Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995", WP 114, 25 November 2005, at 11.
80. In the EU, for example, the European Data Protection Board has stated that processing on another basis is not permitted if consent is withdrawn. European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679, paras. 121-123.

processing when all these considerations are acceptable under the circumstances. By contrast, in other countries like India, consent is the primary basis for data processing.[81]

Some data protection laws have created a specific legal basis to allow the processing of data in arbitral proceedings. According to the Brazil Act, for example, processing of personal data, including sensitive data, is expressly authorised "for the regular exercise of rights in judicial, administrative or arbitration procedures".[82] This is similar to the legal claims exemption in the GDPR, which applies to special category data processing and third-country transfers, but not to general personal data processing (and does not refer expressly to arbitration although its coverage is broad enough to include arbitration).

Where the GDPR applies, the following bases are generally best suited to data processing in the context of international arbitration:[83]

- **Personal Data.** The processing of personal data is lawful when it is necessary for the purposes of the legitimate interests of the data controller (in this case one or more Arbitral Participants) or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring protection of their personal data.[84] For example, the data subject's rights might override the legitimate interest in processing if the processing could raise significant risks to a data subject's professional or personal life and the personal data is not likely to be determinative for the parties' dispute. When relying upon legitimate interests for processing of personal data, the EU Working Party has taken a view that a Legitimate Interests Assessment should be undertaken and recorded (*see* Annex 5 for a checklist), which is to be updated if events occur that might affect the original assessment.[85] If issues are raised about the processing of personal data during the arbitration, it will be helpful to be able to show the competent authority that a Legitimate Interests Assessment was undertaken contemporaneously.

81. *See* India Act.
82. Brazil Act, Arts 7(VI) and 11(II, d).
83. Note that there are other bases for lawful processing, but we only mention those that are most likely to be the suited to arbitration, taking into account the circumstances.
84. A "Legitimate Interests Assessment" refers to an analysis undertaken to identify the particular interests being relied upon when a data controller uses "legitimate interests" as the lawful basis for processing (*see* Annex 5).
85. EU Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", 844/14/EN, WP 217, 9 April 2014; EDPB, "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects", 8 October 2019.

- **Sensitive (Special Category) Data.** The processing of sensitive (special category) data is lawful when it is "necessary for the establishment, exercise or defence of legal claims", which we refer to as the "legal claims derogation".[86] The legal claims derogation will often be the preferred basis for processing sensitive data. It may apply to allow data processing where, for example, the processing of the sensitive data is likely to have a significant impact on a claimant or respondent's case. Personal data of children is also given special consideration.[87]
- **Criminal Convictions and Offences, or Related Security Measures.** In addition to requiring a lawful basis for the processing of data,[88] the processing of personal data relating to "criminal convictions and offences or related security measures" shall be "carried out only under the control of official authority or when the processing is authorised by Union or *Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*."[89] Deciding whether the data falls under this provision is fact specific, and the CJEU has recently said that the objective of Article 10 should be kept in mind in making this determination, which it said is "to protect the data subject from processing that could risk leading to serious interference with his or her private or professional life, for example ... social disapproval or stigmatisation of the data subject."[90] However, not all data regarding suspected criminal offences is covered as the data should be sufficiently specific and related to the potential offence.[91] When it is determined that the data in

86. GDPR Art. 9(2)(f).
87. In the event that an arbitration involves the processing of special category data on a large scale, as well as in other circumstances likely to create a high risk to the rights and freedoms of individuals, a data protection impact assessment is required under the GDPR prior to processing (GDPR Art. 35(1), (3)).
88. GDPR Art. 9(2)(f).
89. GDPR Art. 10 (emphasis added).
90. Judgment of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504.
91. In Sweden, for example, the data must be concrete to a certain degree to qualify as personal data relating to criminal offences, which it is if it concerns a certain crime or category of crime or if data is compiled in such a way that the data corresponds to the objective criteria in a penal provision. If the purpose of the processing is wholly or partly to process data related to criminal offences, this indicates that the data is covered by the scope of Article 10 of the GDPR. Regulatory statement of the Swedish Authority for Privacy Protection (IMY) (8 December 2021); *see* Magnusson Law, "Processing of personal data relating to criminal offences in Sweden – New regulatory guidance on the interpretation of Article 10 of the GDPR", available at https://www.magnussonlaw.com/news/processing-of-personal-data-relating-to-criminal-offences-in-sweden-new-regulatory-guidance-on-the-interpretation-of-article-10-of-the-gdpr/.

question is criminal offence data, whether it can be processed in an arbitration, either commercial or investor-State, will typically turn on whether processing is allowed under *Member State law*, which law may apply to the legal claims derogation to criminal offence data, and raises the question as to which Member State law should be applied. This all requires careful consideration in the context of the specific case.

After considering these factors, the Data Protection Directions should set forth the lawful basis for the processing of personal data during the arbitration proceeding. This will preclude, for example, parties potentially using lack of consent or the withdrawal of consent as a basis to resist the processing of personal data during the arbitration.

(2) Lawful Basis for Personal Data Transfer

Arbitral Participants should identify and document at the outset of the proceedings any applicable restrictions on third-country transfer of personal data and what steps will be taken to transfer personal data in compliance with the restrictions. This includes any applicable data localisation laws which might impact the conduct of proceedings. Compliance with these laws during an arbitration can impact the process and requires advance planning.

Each Arbitral Participant that is required to make transfers to other jurisdictions in the context of an arbitration is required to comply with the data transfer restrictions applicable to them. However, to make this workable in the context of the arbitration proceedings, the rules applicable to transfer should be harmonised where possible. Under the GDPR, for example, the following criteria apply:

- Does an adequacy decision apply to the country to which transfer would be made? For example, at the time of publication, data transfers from the EU to a party in Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay are lawful because they have been declared to be adequate jurisdictions.
- If not, is it feasible to put appropriate safeguards in place? For example, data transfers from the EU to third countries can be based on standard contractual clauses, which can be agreed by the Arbitral Participants. Standard contractual clauses require those entering into them to follow a light version of the GDPR. EU guidance suggests that standard contractual clauses or another adequate safeguard should be put in place where feasible, which also means that, provided they are complied with, it is not necessary to take additional

safeguards in advance of transfer because the presumption is that the personal data will be sufficiently protected after transfer.

- Where standard contractual clauses or other adequate safeguard cannot feasibly be put in place for a justifiable reason, is it possible to rely on an express derogation? In the context of an arbitration, this is most likely to be the legal claims derogation which, in the context of the transfer of personal data, requires the third-country transfers to be "occasional" and "necessary for the establishment, exercise or defence of legal claims." Moreover, advice from the EU Working Party suggests that additional safeguards should be put in place in advance of transfer, including that the personal data should be minimised (including culling for relevance, and potentially redaction or pseudonymisation of personal data), and confidentiality provisions should be entered into.[92]
- If not, is there a compelling legitimate interest in the data being transferred? In such a case both the data subjects *and* the supervisory authority must be notified. In practice, this derogation is unlikely to be applied because notifying both the data subjects and the supervisory authority in advance of transfer may prejudice a party's case, jeopardise attorney-client privilege or compromise the confidentiality of the arbitration.

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

After considering these factors, the Data Protection Directions should set forth the lawful basis for the transfer of personal data during the arbitration proceedings. Where they can be agreed, standard contractual clauses are the legally preferred means of legitimising a data transfer and do not require additional safeguards, which may facilitate document production. Where this is not feasible and the legal claims derogation is relied upon, it is advisable to state that the transfers will be occasional, that they are considered to be necessary for the establishment, exercise or defence of legal claims in the arbitration, that they will be treated confidentially, and how the data transferred will be minimised in advance of the transfer, including culling for relevance and possible redaction or pseudonymisation of personal data (although this will not always be necessary). Adding this language in the Data Protection Directions reduces the chances that data protection will be relied on as a basis to avoid data transfers in the context of the arbitration, most likely during disclosure.

---

92. EU Working Party, "Working Document 1/2009 on pre-trial discovery for cross border civil litigation", WP 158, 11 February 2009 ("Document Disclosure Guidance"), at 10-11.

(3) Disclosure or Production of Documents

Document disclosure is an important part of the international arbitration process, and the impact of data protection laws should be specifically considered in the context of document production. To the extent required by the applicable laws, third-country transfers may need to be limited and the information disclosed may need to be minimised, for example by culling for relevance and materiality, the application of search terms and artificial intelligence during review, or redacting or pseudonymising personal data prior to disclosure, and otherwise limiting the personal data produced to that which is necessary for the resolution of the dispute in line with the applicable lawful basis for processing.

The IBA Rules will often be applied as guidance to document disclosure. Under the IBA Rules, the parties should first attempt to agree on disclosure, followed by tribunal decision when agreement is not possible. Where the data protection laws apply, one aspect of that agreement should be to consider how the data protection laws will impact the disclosure process.

This means that, where possible, the impact of the data protection rules on the document production process should be addressed in the Data Protection Directions, to avoid these arguments being raised later and to reduce cost and time. Issues to be addressed may include: (1) limiting disclosure/data minimisation (taking into account the IBA Rules where applicable); (2) redaction/pseudonymisation in light of the applicable data protection standard; (3) entering into confidentiality provisions/protective orders; and (4) entering into standard contractual clauses or another adequate safeguard for third-country data transfers so that additional safeguards are not required, or where that is not feasible, employing a derogation when possible.

In deciding what data protection measures to adopt, Arbitral Participants should consider the scope of the necessary compliance requirements and the importance of the data for the arbitration. This may be complicated in the event that only one of the parties is subject to strict data protection obligations, which may lead to issues concerning equality of treatment. In cases where the IBA Rules are applied, relevant data protection restrictions will need to be considered and applied in conjunction with the standards applied by the IBA Rules, with the data protection rules being mandatory.

The impact of data protection laws on document disclosure, with specific reference to the GDPR and the IBA Rules, is considered in more detail the following Section.

(4) Data Security and Data Breach Protocols

(a) Data Security

Arbitral Participants should apply a proportionate, risk-based approach to data security. Data security should be addressed at the CMC, which is required or recommended by many institutional arbitration rules (including for example the LCIA and the ICDR).

In terms of what should be considered, the GDPR provides that "appropriate" technical and organisational measures should be put in place. Deciding what security measures are "appropriate" requires consideration of the potential risk to data subjects, the existing information security measures of the Arbitral Participants, and what physical and technical measures are appropriate given the risks to the data subjects, and includes, as pertinent:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[93]

In assessing the appropriate level of security under the GDPR, account shall be taken of the risks that are presented by the processing,[94] in particular from:

- Accidental or unlawful destruction;
- Loss;
- Alteration;
- Unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[95]

---

93. GDPR Art. 32(1).
94. Under Art. 42 of the Brazil Act, processing of personal data shall provide the level of security that a data subject can expect, considering the relevant circumstances (such as the risks that one can reasonably expect and the available techniques for processing personal data). Under Indian law, there are certain measures that an entity can take to comply with this requirement, one of which includes obtaining an IS/ISO/IEC 27001 certification, compliance with which would also be relevant to compliance with the GDPR.
95. GDPR Art. 32(2).

Applying data security standards in an arbitration will depend on many factors, including the Arbitral Participants' existing information security measures and their function in the proceedings, the size and types of organisations involved (including number of employees, their premises and data systems), the type of processing being undertaken and whether external service providers are used. Information security also depends on the types of data being processed, including how valuable, sensitive or confidential it is, and the damage or distress that may be caused to the data subject if the personal or sensitive data were to be compromised. In international arbitration practice these issues are increasingly being addressed through the use of secure platforms for the exchange of written submissions and evidence.

The fact that there is no one-size-fits-all solution to information security is stressed in the Cybersecurity Protocol (2022 Edition) and the IBA Cybersecurity Guidelines (2018). While these initiatives are not directed at data protection compliance, they provide a useful resource for the reasonableness test in relation to information security and how information security may be addressed in international arbitration**.**

The data security obligations of Arbitral Participants are inter-linked, and a breach of security by one will have an impact on all. In this respect, all Arbitral Participants should:

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

In deciding what should be included in the Data Protection Directions concerning data security to help manage risks, Arbitral Participants should consider whether additional information security measures are required for the arbitration in addition to those already employed by the Arbitral Participants in their ordinary course of business. Reference may be made to the Cybersecurity Protocol (2022 Edition) and the IBA Cybersecurity Guidelines (2018) where appropriate.

(b) Personal Data Breach Protocols

Where data security measures in place fail to prevent a data breach, EU-style data protection laws impose strict notification requirements.

Personal data breach is defined by the GDPR, for example, as a breach of security "leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed for purposes of the arbitration" (GDPR Art. 4 (2)). Under the GDPR, there are three types of data breaches:

- "Confidentiality breach" means an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" means an unauthorised or accidental alteration of personal data.
- "Availability breach" means an accidental or unauthorised loss of access to, or destruction of, personal data.

Under the GDPR, not all data breaches require notification, but they must all be recorded. Where the GDPR applies, Arbitral Participants are required to:

- Notify the supervisory authorities in case of a data breach unless it can be shown that it is not "likely to result in a risk for the rights and freedoms of the data subject." They must also notify the data subjects themselves of the breach without undue delay if the risk to personal data and data subjects from a breach is considered to be "high" (*e.g.*, GDPR Art. 34).[96] The burden of proving the absence of risk in a data breach rests on the data controller (*e.g.*, GDPR Arts. 33-34).
- Where notification is required, it must be made without undue delay and, where feasible, not later than 72 hours after becoming "aware" of the breach (*e.g.*, GDPR Arts. 33-34). The EU Working Party has indicated that a data controller is deemed to become aware of a breach when it has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised".[97] With respect to content, a breach notification must include the cause and nature of the breach (if known) and recommendations as to how the potentially affected individuals can mitigate the risks of the breach.

96. Art. 48, Para.1 of the Brazil Act requires a notification "within a reasonable period of time".
97. EU Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679', WP250rev.01, 3 October 2017 (last revised and adopted 6 February 2018), at 11 ("Data Breach Guidelines").

– In all cases, a record of the breach must be kept.

Given these obligations, when a personal data breach occurs or is suspected, it is important for Arbitral Participants to determine quickly whether mandatory reporting requirements may be triggered and by whom. A data breach may impact personal data provided in the context of the arbitration by the parties, the arbitral tribunal and/or any arbitral institution, each of whom may have legal or ethical obligations arising out of that data breach, including notification. In most cases, a party or its counsel will have collected the personal data processed during an arbitration, exchanged that personal data with the other party(ies) and their counsel, and potentially submitted the personal data to the tribunal and the institution. A personal data breach suffered by any of these Arbitral Participants may trigger a requirement that any or all of them notify relevant authorities and potentially the data subjects.

Given the risks associated with data breaches and the short time allowed to address them, it is therefore advisable that the Data Protection Directions include a data breach protocol to be applied amongst those involved in the proceedings. This should cover (1) what will constitute a data breach; (2) the procedure that will be followed if a breach occurs; (3) what information shall be provided about a data breach; (4) who will be notified and when, including that Arbitral Participants shall be obligated to inform each other of a data breach without undue delay; and (5) duties to provide information and to cooperate with respect to notification.

Note that a personal data breach protocol adopted for an arbitration typically would not seek to address the individual reporting obligations of individual Arbitral Participants, but rather seek to ensure that all participants are made aware in a timely fashion of incidents that may trigger obligations under EU-style data protection laws and to define how they should address such breaches vis-à-vis each other when they impact arbitral data and to require cooperation and communication amongst them with respect to notification.[98] Arbitral Participants governed by the GDPR may refer to useful guidance issued by the European Commission in terms of when notification is required and what needs to be done.[99]

In order to assist Arbitral Participants, Schedule D-1 of the Cybersecurity Protocol (2022 Edition) includes a sample personal data breach protocol, which is drafted taking the GDPR requirements into consideration. Annexes 7 and 8 of this Roadmap also include

98. *See* Schedule D-1 of the Cybersecurity Protocol (2022 Edition) for a sample personal data breach protocol based on the GDPR.
99. *See* Data Breach Guidelines and the recently issued Guidelines 01/2021 on Examples regarding Personal Data Breach Notification Adopted on 14 December 2021 Version 2.0.

general language that may be employed to address data breaches, preferably with reference to a personal data breach protocol, such as that found in Schedule D-1 of the Cybersecurity Protocol (2022 Edition).

(5) Managing Data Subject Rights

The Data Protection Directions should include measures to comply with data subject rights, including data subject access requests, update and correction requests.

Arbitral Participants may receive requests from data subjects seeking to exercise their rights during the arbitration process. These requests may come from any individual whose personal data is handled during the arbitration process, including, but not limited to, individual parties, witnesses, experts or even persons not directly involved in the proceedings but about whom personal data may have been adduced (*e.g.*, an employee of a party, who is not involved in the proceedings directly, or an employee of a third party, who is not a party to the arbitration), and who believes that their data is being processed. These data subject requests will need to be addressed within a prescribed time frame (under the GDPR this is "without undue delay and in any event within one month"). It is therefore important to consider procedures for doing so in advance.

In the arbitration context, data subject access requests may be aimed either at preventing data from being used in the arbitration or at obtaining access to processed data, both of which may trigger issues of confidentiality and privilege. The GDPR and the Brazil Act, for example, provide that the data subject has the right to obtain from the controller (in this case an Arbitral Participant) confirmation as to whether or not their personal data is being processed, and, if that is the case, the right of access, which should include electronic access, to a broad range of information about that processing, as well as a copy of the data processed, provided that the provision of a copy does not interfere with the rights and freedoms of others.[100]

Upon receipt of a valid data subject access request, Arbitral Participants are required to provide the data subject with electronic access to the personal data they hold about them or a copy thereof, provided the provision of electronic access or a copy does "not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software".[101] Furthermore, in some EU Member States, including Germany, a client's right to secrecy may prevail over the data subject's right of access. However, the GDPR provides expressly that "the

100. *See* GDPR Recital 63 and Art. 15(4).
101. *Ibid.*

result of those considerations should not be a refusal to provide all information to the data subject".[102]

When acceding to a data subject access request, each Arbitral Participant should carefully consider the impact that meeting the request might have on its own legal and ethical obligations and those of others (both Arbitral Participants and third parties) and identify and implement measures to reduce any potential adverse impact. For example, Arbitral Participants might redact personal data relating to individuals that are not relevant to the dispute or restrict access to those documents or portions thereof that are strictly necessary to meet the exact terms of the data subject's request rather than adopting a blanket (and likely less time consuming) approach. National courts have also suggested that striking a balance between different stakeholders' interests might involve obtaining undertakings from the data subject to restrict the onward transfer of any information disclosed in response to the data subject access request.[103]

Data Protection Directions should provide the mechanisms for complying with data subject rights, including data subject access requests, update and correction requests. This should include who is responsible for addressing the request in the first instance. For example, it is usually preferable for the party who initially collected the personal data to address the request, or the party who presented the personal data in the arbitration, depending on the circumstances. In any case, it is generally advisable to provide that the arbitrators will not be required to respond to data subject right requests unless and until other means of responding have been exhausted.

(6) Notification

Arbitral Participants who are data controllers or joint controllers are responsible for ensuring that data subjects are put on notice that their personal data is being processed for the purposes of the arbitration and are informed of other details about the data processing. However, in the case of a confidential arbitration, providing such notices could compromise the confidentiality of the arbitration. Moreover, in the absence of a relationship with the data subject, arbitrators and institutions may have no realistic means of providing notice.

The requirement to give notice applies to each data controller, of which there will be many in an arbitration. Given that any arbitration involves multiple data controllers, this could lead to one data subject receiving multiple notices.

---

102. GDPR Recital 63.
103. *B v. General Medical Council* [2018] EWCA Civ 1497, 28 June 2018 (UK).

Many of the data controllers in an arbitration will not have originally collected the personal data from the data subjects. In order to avoid overlapping notices, the GDPR, for example, provides significant exemptions from the notice requirements for data controllers who did not originally collect the data from the data subject. Many of those exceptions are potentially applicable to processing by Arbitral Participants who did not directly collect data from individuals (like the arbitrators, the institution and the opposing party/counsel), which means that they would not be required to provide an additional notice.[104]

However, each Arbitral Participant will need to determine their notification obligations on a case-by-case basis. These obligations may differ based on where the Arbitral Participant is established, where the personal data was collected, where the data subjects are located and where the personal data is processed.

In order to ensure notice is given without overburdening the arbitration process, the Data Protection Directions may be employed to place the burden to provide notice either on the Arbitral Participant that collected the personal data for purposes of the arbitration or the one that originally collected the data, depending on the circumstances.

(7) Documenting Data Protection Compliance

Accountability requires data controllers to take personal responsibility for data protection compliance and to record the measures they take to comply with their data protection obligations. Under the GDPR, for example, data controllers are expected to be able to "demonstrate compliance" with the data protection principles it establishes as they are

---

104. Under the GDPR Art. 14(5) and Recital 62, where the data controller did not originally collect the personal data, they are not required to provide notice, *inter alia*, where:
    1. The individual data subject already has the required information on the processing of his or her personal data;
    2. Providing information on the processing of personal data to the individual would be impossible;
    3. Providing such information to the individual would involve a disproportionate effort;
    4. Providing such information to the individual would render impossible or seriously impair the achievement of the objectives of the processing; or
    5. The data controller is subject to an obligation of professional secrecy regulated by EU or EU Member State law that covers the personal data.
    6. In the cases mentioned in the second, third and fourth bullet points above, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

implemented throughout the GDPR.[105] Adequate records should be kept of what compliance measures were taken and why, in a manner that they can be shown to the competent authorities if compliance issues were to arise.[106]

In the context of an arbitration, particularly a confidential arbitration, it will be important to document in the Data Protection Directions who is responsible for documenting compliance, the form of such documentation and that when requested by a data protection authority, it can be provided.

(8) Use of Online Case Management Platforms to assist with Compliance

Online case management platforms can assist with discrete data protection obligations during the course of the proceedings, taking into account that use of the platform will itself constitute data processing and need to comply with applicable data protection laws.

The use of AI tools on the platform (particularly through unsupervised learning, which may help to cluster documents that appear to have personal data within them), may facilitate compliance with data minimisation obligations. Using a platform can also help to ensure (through agreement at the outset of the setup process) that data will be deleted and destroyed once the purpose for which it was being processed has ended (*i.e.*, normally within an agreed period of time following completion of the arbitration and receipt of the award by the parties).

Compliance with transparency and accountability obligations can also be facilitated by using online case management platforms. Data controllers and processors are required to keep a record of their data protection compliance efforts in order to demonstrate compliance, respond to data subjects' requests for information regarding the processing of their personal data, notifying data subjects when their personal data is being processed, etc. A platform can help provide an audit trail of data flows, which can make it simpler and more cost effective to respond to such queries and demonstrate compliance. Setting formulaic "on-platform" processes that must be complied with enables a more efficient and accurate tracking of data flows than can readily be achieved manually at similar costs.[107]

Use of an online case management platform during the course of the proceedings should be discussed at the CMC and potentially included in the Data Protection Directions particularly when the platform is used to assist in managing an Arbitral Participant's data

105. GDPR Art. 5(2); see also GDPR Art. 24(1).
106. Organisations with more than 250 employees must document compliance in accordance with GDPR Article 30, which provides a list of record-keeping obligations.
107. *See* Online Platform Protocol.

protection obligations during the course of the proceedings, or otherwise impacts data protection compliance.

(9) Conclusion on Documenting Data Protection Compliance

The key to avoiding data protection compliance from becoming an issue during the proceedings is to address and document the means adopted to address data protection from the outset:

- Data protection should be on the agenda for the initial CMC. This Section of the Roadmap has addressed the most important issues to be addressed and potential solutions for each of them using the GDPR as an example.
- Whenever possible, agreement should be reached, but where agreement is impossible, the tribunal can issue directions after hearing the parties.
- Data Protection Directions, whether agreed or ordered, should then be documented through a data protection protocol (*see* Annex 8) or through language included in the terms of reference or procedural order (*see* Annex 7), which should indicate where agreement was reached.
- Although this is highly case and fact specific, Annex 7 provides sample language addressing each of these issues that may be considered for inclusion in Data Protection Directions using the GDPR as an example and Annex 8 provides sample language for a Data Protection Protocol when appropriate.

4. When Data Protection Issues Arise During the Proceedings

Data protection issues may arise during the course of the proceedings. The most common source of data protection issues is the document disclosure process, which has become an important part of both international commercial arbitration and investor-State arbitration. Data breaches and data subject rights requests are also possible during an arbitration and will need to be managed to avoid potential disruptions.

Document Production. The document production process involves the collection, review, transfer to counsel, production of the documents to the other party, and potential presentation as evidence to the tribunal. It is important to recall that anything that is used or produced during an arbitration that allows an individual to be identified is personal data of that individual (emails, texts, WhatsApp messages), and that each of these activities is an activity of processing personal data. Therefore, the data protection laws apply to the document production process from start to finish and that process typically involves the processing, often including cross border transfers, of significant amounts of personal data.

Among other things, issues that may be raised under data protection laws may concern:

- Lawful basis for the processing;
- Lawful basis for the transfer;
- Data minimisation including any need for redaction/pseudonymisation; and
- Whether the data subjects (especially third parties) are on notice of the processing.

Using the EU data protection laws as an example, this Section considers the data protection principles applicable to document disclosure, and how these principles may be applied generally and taking into account the IBA Rules.

Data Protection Principles Applicable to Document Disclosure. The obligation to minimise data, which is found in most data protection laws, is particularly relevant to document disclosure. Although data minimisation is a general obligation,[108] there is no guidance as to how this should be applied in the arbitral process generally or during the document disclosure/production phase in particular.

Using the EU data protection laws as an example, the EU Working Party has provided guidance on the application of the EU Data Protection Directive to data transfer for purposes of discovery for US litigation, which guidance remains applicable. The EU Working Party suggested that data minimisation is likely to require: (1) culling the documents to be disclosed for relevance; (2) redacting unnecessary personal data; (3) entering into confidentiality provisions/protective orders; and (4) putting adequate safeguards in place for third-country transfer.[109] Similar principles would be expected to apply under the GDPR in the context of an arbitration.

The approach taken by the Working Party suggests the application of a three-step process aimed at minimising the personal data disclosed, followed by considerations of confidentiality and third-country transfer:

1. Limiting the data disclosed to what is relevant to the dispute and non-duplicative (often referred to as "culling");
2. Where justified by the risk posed, identifying and redacting or pseudonymising unnecessary personal data.

---

108. The EDPB has stated that "the principle of data minimization … emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which [it is] processed." Data Transfer Guidance, at 13.
109. Document Disclosure Guidance, at 10-11.

In considering how these principles apply to international arbitration, culling for relevance is a measure already used in practice in arbitration to reduce the volume of data processed and disclosed. However, different approaches are taken to the extent to which culling is required and allowed, and at what stage it is undertaken. Moreover, redaction of personal data is not yet common practice and is not always required.

Application of Data Protection Principles in Practice, Including in Conjunction with the IBA Rules. The IBA Rules are widely applied to the disclosure of documents in international arbitration. Given the prevalence of the IBA Rules, it is useful to consider how data protection requirements may impact disclosure under the IBA Rules, keeping in mind that data protection requirements are legally required and therefore must be applied to supplement the IBA Rules or any other standard generally applied to disclosure in international arbitration.

The IBA Rules provide that the parties may agree on the disclosure of documents, and where agreement is not possible, the parties may petition the tribunal to order disclosure. Even where the IBA Rules are not applied to the process, a similar process is likely to be applied.

As described above, the best place to address data protection compliance during the disclosure process is through agreed Data Protection Directions. However, even where Data Protection Directions are given, issues may arise in interpreting those directions. In other cases, there will not be any Data Protection Directions or they will not have addressed disclosure, in which case, these issues will be addressed by the tribunal for the first time when making decisions on document requests.

Under the IBA Rules, the standard to be applied by the tribunal in deciding on a document request is whether the document "is relevant to the case and material to its outcome". This standard is consistent with the concept of data minimisation and the guidance given by the EU Working Party. Article 9(2) of the IBA Rules empowers the tribunal to exclude from evidence or production a document for a number of reasons, including "legal impediment or privilege under the legal or ethical rules determined by the Arbitral Tribunal to be applicable"[110] and "grounds of commercial or technical confidentiality that the Arbitral Tribunal determines to be compelling."[111] The Commentary on the IBA Rules identifies that personal data protection considerations under the GDPR

110. IBA Rules Art. 9(2)(b).
111. IBA Rules Art. 9(2)(e). IBA Task Force for the Revision of the IBA Rules on the Taking of Evidence in International Arbitration, "Commentary on the revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration" (January 2021) https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D, at 29.

and similar national legislation may come under the limb of "commercial or technical confidentiality", and consideration should also be given to whether it constitutes a "legal impediment".

The IBA Rules do not address the possibility of redacting and/or pseudonymising unnecessary personal data, although the redaction and/or pseudonymising of personal data is not inconsistent with their principles when necessary for data protection compliance.

The question as to whether data protection considerations may limit document disclosure generally, or whether, if production is allowed, redaction and/or pseudonymising of personal data is necessary (and if so, the extent to which it is required, and the method to be applied), is highly case specific, and the parties may disagree. Considerations to be taken into account by the tribunal in deciding these issues may include:

- Has the party objecting to disclosure and/or arguing that redaction and/or pseudonymising is necessary, established to the satisfaction of the tribunal that this is required by applicable data protection laws?
- Is third-country data transfer required, and if so, can effective safeguards be put in place? For example, where cross border disclosure of documents including personal data is contemplated, this would favour putting in place standard contractual clauses or another safeguard where feasible, rather than relying on a derogation (like the legal claims derogation).
- Are alternatives available allowing the documents to be produced (or to be produced without redaction and/or pseudonymising) – for example, if third-country data transfer is an obstacle, could standard contractual clauses be employed or could the documents initially be reviewed locally?
- How extensive is the document disclosure being sought from the tribunal?
- Have reasonable measures been agreed to cull for relevance/materiality and lack of duplication?
- To what extent would a decision to allow the document disclosure with or without redaction affect the rights of interests of the data subjects identified in the documents? This may be impacted by what type of personal data is likely to be included, and whether it is likely to contain sensitive or criminal offence data. For example, in a case where the documents being disclosed contain a limited set of documents that were exchanged during the course of a business relationship by those involved in the facts at issue, this may be considered in deciding the extent to which the production should be allowed and/or redaction/pseudonymising be required.
- To what extent would a refusal to allow the disputed document disclosure impact the rights of a party to be heard?

– Are confidentiality/protective orders in place covering the documents to be disclosed either through entering into standard contractual clauses or other means?

A blanket refusal to disclose documents in light of applicable data protection restrictions is not justified. In most situations, the entire document will not be considered personal data, but only the words, phrases or parts of the document relating to the data subject. This distinction is important in relation to document production, as data protection requirements would rarely justify withholding an entire document, but may justify redaction.

However, the tribunal will need to consider what means should be put in place to ensure reasonable data protection compliance and at the same time allowing the necessary disclosure to ensure justice is served. As discussed above in **Section II.B.3.c(3)**, technology, including artificial intelligence, may assist in both culling the data for relevance and in redacting personal data through the use of an online case management platform or otherwise. However, it should be recalled that these measures themselves constitute data processing and can be costly and time consuming, especially with large amounts of data.

Under the GDPR, for example, given the broad definition of personal data,[112] a practical approach may need to be applied to whether, and if so the extent to which, redaction is required, taking the concept of proportionality into consideration. As discussed in Section I, a data subject has a mandatory right to have their personal data protected, but that right is not absolute. Similarly, the parties to an arbitration have a right to be heard, but that right does not include unfettered disclosure, and by agreeing to arbitration they agree to a process that needs to comply with data protection laws. Therefore, these rights need to be balanced and the data protection laws applied in proportion to the risk to the data subject posed by the document disclosure, keeping in mind the important role that arbitration plays in the administration of justice but in all cases, the rights of the data subject must be adequately protected.

Data Breach. Security incidents are becoming increasingly common and Arbitral Participants are no exception. This stresses the importance of including a data breach protocol in the Data Protection Directions, so if a security incident occurs everyone knows what to do and when.

112. The CJEU held for example that "the term personal data … undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies", Judgment of 6 November 2003, *Lindqvist*, C-101/01, 2003 I-12971, para. 24.

Whenever a personal data breach occurs in a case where an EU-style data protection laws applies, Arbitral Participants will need to notify each other without undue delay that a personal data breach has occurred that may impact personal data being processed for the arbitration, as discussed in **Section II.B.3.c(4)** above.

This will allow each Arbitral Participant to decide whether a notification is required applying the principles discussed in the preceding Section. This has to happen quickly because, for example, when an Arbitral Participant experiences a personal data breach falling within the notification requirements of the GDPR, the data controller will be required to make a notification without undue delay (and where possible within 72 hours) unless the data controller can establish that the data breach is not "likely to result in a risk for the rights and freedoms of the data subject." Moreover, notification may impact the arbitration and the other Arbitral Participants, and as more than one Arbitral Participant may be required to notify, it is important to stress communication and cooperation amongst the Arbitral Participants with respect to any notifications.

Data Subject Rights Requests. As discussed in **Section II.B.3.c(5)** above with respect to Data Protection Directions, another issue that may arise during an arbitration is that a data subject may seek to enforce its rights to have access to their personal data (or another right) from an Arbitral Participant. This can be a genuine request or an attempt to derail the process.

Regardless of whether Data Protection Directions are in place, when a data subject right request is received concerning arbitral data, the Arbitral Participant receiving the request should usually inform the other Arbitral Participants of the request. The issue then arises as to who should address the request. Where possible, given the nature of the arbitral process, it is usually advisable for the Arbitral Participant that collected the personal data from the data subject to address the request in the first instance and to inform the data subject. This is especially the case when the request is directed at an arbitrator.

5. Remote Hearings

During the COVID-19 pandemic, it has become the norm to hold remote hearings. Moving forward, conducting remote hearings, and partially remote hearings, will continue to occur regularly.

When it is decided to hold a remote hearing, it will be important to establish a protocol for the hearing, not least because the remote hearing platform provider may be considered as a processor of personal data. For example, the IBA Rules address remote hearings in Article 8.2 and suggest that the tribunal must consult with the parties to establish a remote hearing protocol that addresses several issues, including: (1) the technology to

be used; (2) advanced testing of the technology or training; (3) starting and ending times, considering varying time zones; (4) how documents may be placed before a witness; and (5) measures to ensure that witnesses giving testimony are not distracted or improperly influenced.

It will also be important that any data protection and data security issues posed by a remote hearing are also addressed in the protocol. There are many examples of such protocols. However, many remote hearing protocols do not address the data protection issues that may be faced. Annex 7 includes sample language that may be included in the Data Protection Directions when the GDPR or a similar EU-style data protection law applies, and similar language should be considered for inclusion in any remote hearing protocol that may be issued or agreed.

6. Arbitral Awards and Other Decisions

Arbitral tribunals process personal data (including potentially sensitive data and criminal offence data) when preparing, drafting and rendering their orders, decisions and awards, while arbitration institutions process personal data when constituting tribunals, dealing with applications of the parties, rendering challenge decisions, overseeing the proceedings, scrutinising and notifying awards, etc.

Even in confidential arbitrations, the award may become public if it is enforced in a country where awards (or parts thereof) become public in the enforcement process. Moreover, in investment and treaty-based arbitrations, awards are often published and commercial institutions are increasingly considering the publication of awards if the parties do not object and subject to possible redaction, and (excerpts of) challenge decisions.

Before the award is rendered, Arbitral Participants should consider the extent to which personal data should be included in the award and any steps that might be taken to minimise the inclusion of personal data in the award and to ensure its confidentiality when applicable. For example, while reference may be made to the evidence of a certain witness and that witness's role for weighing the evidence, it may not be necessary to provide any further personal data about that witness in the award. Further, even where the personal data has been minimised, it remains personal data, and before publishing awards, consideration should be given to the impact this has on data protection compliance.

In this framework, arbitrators and institutions should consider the basis and necessity for the inclusion of personal data in awards and decisions and whether they wish to raise this issue with the parties before rendering an award or decision. In some EU countries, for example, it is standard practice to redact personal data from court decisions. It is important to bear in mind that even where personal information about a witness has been minimised, the references in the award remain their personal data because they are still

identifiable from the remainder of the award or related materials, and therefore the data in the award must be processed in compliance with data protection laws.

C. AFTER THE ARBITRATION

Arbitral Participants should consider how long to retain personal data connected with proceedings and the time after which such personal data and/or the documents containing it should be destroyed or permanently deleted.

Both data retention and deletion are considered data processing under many EU-style data protection laws. The GDPR, for example, provides that personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed" (GDPR Art. 5(1)(e)).[113]

This principle ensures that personal data is only stored for as long as necessary for the purpose for which it is being processed. This requires controllers to consider, document and be able to justify the duration of storage. Moreover, the personal data being stored should periodically be reviewed, and securely erased or anonymised when it is no longer required. Personal data may be retained for longer intervals for public interest archiving, scientific or historical research, or statistical purposes (which is an important driver for data retention by arbitral institutions).

Arbitral Participants will be required to store personal data for a certain period after a case is completed. They will each need to consider what data retention period is reasonable in light of the purpose of the processing, including the arbitration itself and the enforcement of any award, as well as any attendant processing in light of, for example, future conflict checks and legal and regulatory compliance (for example, for income tax and audit purposes). In this regard, the purpose limitation principle also applies to the storage of personal data (*see* **Section I.F.4**). Arbitral Participants should bear in mind that potential use in other legal proceedings may not be a sufficient basis to retain data beyond an otherwise reasonable period of time.

Arbitral Participants, like all data controllers, should consider how long to retain personal data connected with proceedings and the time after which such personal data and/

113. Similarly, under Articles 15 and 16 of the Brazil Act, the processing of personal data shall be terminated as soon as its purpose has been achieved. Further, unless there is a legal basis for keeping personal data, it shall be deleted following the termination of the processing of the data. Under Indian law, sensitive personal data of an individual should not be stored or retained for longer than is necessary to fulfil the purpose for which it is collected.

or the documents containing it should be destroyed or permanently deleted. This means that they should:

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

CONCLUSION

When an Arbitral Participant is subject to a data protection law, compliance is legally required. In practice, this means that data protection principles need to be applied during the arbitration to supplement the applicable laws, the arbitration rules, and soft law instruments (including the IBA Rules). The aim of this Roadmap is to enable Arbitral Participants to identify and effectively address data protection issues in the context of arbitral proceedings.

Sensible solutions exist permitting data protection laws to be applied during the arbitral process, which is facilitated when: (1) Arbitral Participants adopt a reasonable, cooperative, and proportionate approach to data protection compliance; (2) data protection is addressed at the initial case management conference; (3) Data Protection Directions are employed; and (4) compliance efforts are documented in a manner that can be shared with data protection authorities, if requested.

ANNEXES

All views expressed in these Annexes are those of the Task Force and not those of ICCA, the IBA, their governing bodies, or members. These Annexes are the result of the collective efforts of the Task Force, the views expressed are not attributable to any particular Task Force member and all Task Force members served in their individual capacity.

ANNEX 1
Glossary[1]

A

"adequacy decision" refers to a decision made by the European Commission that a third country's data protection laws are considered to be adequate and therefore data can be transferred outside the EU/EEA or to an international organisation without any further authorisation or notice because adequate protections apply as a matter of law (GDPR Art. 45(1)).

"Annexes" refers to the present set of annexes to the Roadmap.

"Arbitral Participants" is defined in the Roadmap as, and limited to, the parties, their legal counsel, the arbitrators and arbitral institutions.[2] While it is not explicitly addressed to them, the guidance provided in the Roadmap is also relevant to those working for or with Arbitral Participants during an arbitration, such as tribunal secretaries, experts and service providers (*e.g.*, e-discovery experts, information technology professionals, transcribers, translation services, online case management platform providers, remote hearing platform providers, etc.).

C

"California Act" or **"CCPA"** means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq.

"consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them (GDPR Art. 4(11)).

---

1. The glossary refers mainly to the GDPR. However, throughout the text of the Roadmap references are provided to similar concepts used in other EU-style data protection laws.
2. In the case of arbitrations administered by an international organisation, determining whether any relevant privileges and immunities will impact the application of data protection laws turns on the breadth and scope of the relevant privileges and immunities both in terms of whether data protection laws would come within their scope, and, if so, which Arbitral Participants would be covered by them. This is an institution-specific enquiry.

"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (GDPR Art. 4(7)).

"Controller/Processor Opinion" means the Opinion 1/2010 on the Concepts of "Controller" and "Processor", EU Working Party, 00264/10/EN WP 169, 2010.

"**criminal offence data"** means data relating to criminal convictions and offences or related security measures (GDPR Art. 10).

"culling" means filtering data, including in the context of data minimisation (for example, during the disclosure process).

"Cybersecurity Protocol" means the ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitration (2022 Edition).

D

"data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (GDPR Art. 4(12)).

"data controller" – *see "controller"* above.

"data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about their health status (GDPR Art. 4(15)).

"data minimisation" is a principle established by the GDPR and other data protection laws according to which the processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed (GDPR Art. 5(1)(c)).

"data processor" is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (*e.g.*, GDPR Art. 4(8)).

"data protection authority" or "DPA" – *see "supervisory authority"* below.

"data privacy notice" or "data protection notice" refers to a document whereby the controller notifies the data subject in a concise and accessible form that their personal data is being processed and the purpose of the processing (*e.g.*, GDPR Arts. 12-14).

"Data Protection Directions" are procedural directions issued by an arbitral tribunal in the form of a procedural order, terms of reference, or a data protection protocol setting out how data protection will be addressed during the arbitration. They may be issued on an agreed basis or ordered by the arbitral tribunal.

"Data Protection Directive" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281/31 (24/10/1995).

"Data Protection Protocol" refers to a document in which the roles and responsibilities of data controllers and processors vis-à-vis the processing of personal data are identified and agreed.

"data subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person **(**GDPR Art. 4(1)). Legal entities are not data subjects.

"data transfer" refers to transfers of data, which is broadly defined by the EU.

"Data Transfer Guidance" refers to the EDPB "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679" dated 6 February 2018.

"Document Disclosure Guidance" refers to the EU Working Party "Working Document 1/2009 on pre-trial discovery for cross border civil litigation", WP 158, dated 11 February 2009.

E

"establishment" implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect (GDPR Recital 22).

"European Data Protection Board" or "EDPB" is a body of representatives of national data protection authorities, the entity empowered to issue guidelines, recommendations and best practices to encourage consistent application of the GDPR and the setting of administrative fines (replaced the EU Working Party).

"European Economic Area" or "EEA" encompasses the twenty-seven EU Member States and three additional states: Iceland, Liechtenstein and Norway. The scope of application of the GDPR extends to the EEA, therefore, for ease of reference, the term **"EU"** as used in the Roadmap includes the EEA countries as well.

"European Union" or "EU" means the twenty-seven EU Member States: Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the Netherlands. The term EU as used in the Roadmap includes the EEA countries as well.

"EU Working Party" was a body of representatives of national data protection authorities, established under Article 29 of the EU Data Protection Directive, the GDPR's predecessor. The EU Working Party was tasked with providing guidance on the application of data protection rules under the previous EU Data Protection Directive. The advice rendered by the EU Working Party remains valid until replaced, amended or abrogated by the EDPB, which performs a similar function under the GDPR.

F

"filing system" means any structured set of personal data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (GDPR Art. 4(6)).

G

"General Data Protection Regulation" or "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

I

"IBA Rules" means the IBA Rules on the Taking of Evidence in International Arbitration (International Bar Association, revised in 2020).

"Indian Act" means the India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011. India has not yet passed a comprehensive data protection law.

"international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries (GDPR Art. 4(26)).

"ICO" means the UK Information Commissioner's Office.

J

"joint controller" – refers to the situation where two or more controllers jointly determine the purposes and means of processing (GDPR Art. 26). Joint controllers are jointly responsible for compliance with the GDPR and jointly and severally liable for noncompliance.

L

"**lawful basis**" refers to one of the six possible lawful bases for the processing of personal data under the GDPR, one of which must apply whenever processing personal data (GDPR Art. 6).

"legitimate interests" is one of the lawful bases for data processing, and can be applied except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (GDPR Art. 6(1)(f); *see* Annex 5). The GDPR does not define what constitutes "legitimate" interests and a wide range of interests may be considered to be legitimate interests, including those of the data controller and third parties. When legitimate interests are relied upon as a basis for processing, a Legitimate Interests Assessment should be considered (*see* Annex 5).

"Legitimate Interests Assessment" refers to an analysis undertaken to identify the particular interests being relied upon when a data controller uses "legitimate interests" as the lawful basis for processing (*see* Annex 5).

"LGPD" or "Brazil Act" means the Brazilian General Data Protection Act (Statute 13709/18).

O

"Online Platform Protocol" means the Protocol for Online Case Management in International Arbitration, Working Group on LegalTech Adoption in International Arbitration (2020).

P

"personal data" means any information relating to a "data subject" (GDPR Art. 4(1)). *See "data subject"* above.

"personal data breach" – *see "data breach"* above.

"personal data of a child" is given special protection under the GDPR. Where personal data of a child is processed based on consent and the child is below the age of 16 years, such processing shall be lawful when the consent is provided by the holder of parental responsibility over the child. Member States may provide by law for a lower age provided that such lower age is not below 13 years (GDPR Art. 4(2)).

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR Art. 4(2)).

"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller (GDPR Art. 4(8)).

"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (for example, a coding system) provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. It is similar to redaction but requires that the data subject not be identifiable without additional measures (GDPR Art. 4(5)).

R

"Roadmap" refers to this ICCA-IBA Roadmap to Data Protection in International Arbitration.

S

"sensitive data"– *see "special category data"* below.

"special category data" is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data

concerning health or data concerning a natural person's sex life or sexual orientation. (GDPR Art. 9(1) and 9(2)(f)).

"standard contractual clauses" refers to clauses that have been adopted by the European Commission (or in some cases by a supervisory authority), which if entered into allow data to be transferred outside the EU in the absence of an adequacy decision (GDPR Art. 46). *See* Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) C/2021/3972 OJ L 199, 7.6.2021, 31–61. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

"supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51 GDPR (GDPR Art. 4(21)). It is also referred to as a **"data protection authority"** or **"DPA"**.

T

"targeting" is the term used to refer to activities whereby an individual or entity that is not "established" in the EU nevertheless comes within the jurisdictional scope of the GDPR, including when they (1) offer of goods or services to data subjects in the EU or (2) monitor the behaviour of data subjects in the EU (GDPR Art. 3(2), Recs. 23-24). The EDPB has published "Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3)" providing further guidance on when data processing activities will be considered to constitute targeting for the purposes of the application of the GDPR.

"third country" means any country outside of the European Union and EEA.

"third country data transfer(s)" refers to data transfers of personal data outside of the EU or to an international organisation (GDPR Arts. 45, 46(1), 49).

"third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (GDPR Art. 4(10) GDPR).

ANNEX 2
Data Protection Practice Tips

Before the Arbitration
1. Applicability – Arbitral Participants (defined to include the parties, counsel, arbitrators and the arbitral institution) should consider at the outset of the arbitration (or prior to issuing proceedings in the case of parties and their legal counsel) what data protection laws will apply during the arbitration, keeping in mind that data protection laws are mandatory and apply alongside the applicable arbitration law, arbitration rules, and any soft law such as the IBA Rules, to both commercial and investor-State arbitration.
2. Proportionality – Data protection laws should be applied in a proportionate manner, taking into consideration the rights and interests of the data subject (considering, for example, the nature and amount of data being processed and the circumstances), the rights and interests of third parties, including the parties to the arbitration and the need for fair and efficient administration of justice, provided that the rights and interests of the data subject must always be adequately protected.
3. Data Collection and Review – When preparing for a case, parties and their legal counsel should identify and document: (1) the types of personal data, sensitive data, personal data of children and any personal data related to criminal proceedings that is likely to be processed; (2) the lawful basis for processing that data for the arbitration; (3) what data transfers will likely need to be made and the lawful basis for them; (4) what notices have been or will need to be given to the data subjects; (5) what adequate security measures will be put in place to protect the data; and (6) any steps to be taken to minimise the processing of personal data (including any use of online case management tools to assist in that process, *e.g.*, by limiting data collection to specific custodians, data ranges or applying search terms, redaction, pseudonymisation, etc.).
4. Service Providers – When engaging third parties to assist with an arbitration (experts, transcribers, translators, online case management platform providers, remote hearing platform providers etc.), Arbitral Participants should consider what is required to comply with data protection laws in those relationships, including whether a data processing agreement is necessary.
5. Arbitrator Selection – How an arbitrator's appointment will impact the application of data protection laws to the arbitration should be considered and steps taken

to ensure that personal data may be processed by and transferred to the arbitrator in accordance with any applicable data protection law, including the possibility of entering into standard contractual clauses for data transfers, where necessary.

During the Arbitration

6. Initial Case Management Conference (CMC) – Data protection issues should be put on the agenda and addressed at the initial CMC.

7. Data Protection Directions – In order to facilitate compliance with data protection laws and the orderly conduct of proceedings, the following data protection issues should be considered for inclusion in the first procedural order, terms of reference, or, where appropriate, in a data protection protocol (referred to as "Data Protection Directions"): (1) lawful basis for processing; (2) lawful basis for data transfer; (3) disclosure or production of documents; (4) data security and data breach protocols; (5) managing data subject rights; (6) notification; (7) documenting data protection compliance; and (8) any use of online case management platforms to assist with compliance. This is not an exhaustive list, and some of these issues may be more important than others in specific cases. However, these are issues which if not addressed early can create problems down the road either from a compliance or case management perspective.

8. During the Proceedings – Three important data protection issues that may arise in the course of the proceedings are: (1) data protection in document disclosure; (2) potential data breaches; and (3) possible data subject rights requests.

- **Document Disclosure –** Data protection laws may impact the means and amount of data to be processed and transferred to third countries for purposes of disclosure. In addition to having a lawful basis for processing and transfer, data minimisation obligations may require the culling of the documents to be produced, and/or redacting or pseudonymising personal data prior to disclosure, and otherwise limiting the personal data produced to that which is necessary for the resolution of the dispute in line with the applicable lawful basis for processing.
- **Data Breach Notification –** Given the short deadlines for data breach notification, Arbitral Participants should document in advance what will constitute a data breach, the procedure within the arbitration that will be followed if a breach occurs, who will be notified, and that they will communicate and cooperate with respect to notification. In any case, Arbitral Participants

should inform each other whenever a data breach occurs impacting arbitral data so that they can comply with any notification requirements.

- **Data Subject Rights –** Arbitral Participants should set out in advance the mechanisms that will be used to address compliance with data subject rights, including data subject access requests.

9. Award. Before the award is rendered, Arbitral Participants should consider the extent to which personal data should be included in the award and steps that might be taken to minimise the inclusion of personal data in the award and to ensure its confidentiality where applicable.

After the Arbitration

10. Data Retention – Arbitral Participants should consider how long to retain personal data connected with proceedings and the time after which such personal data and/or the documents containing it should be destroyed or permanently deleted.

ANNEX 3
Checklist: Data Protection Considerations

Introductory Remarks

This checklist contains a non-exhaustive list of data protection considerations that may impact Arbitral Participants when the GDPR or another EU-style data protection law applies.

Caution: Use of this checklist does not ensure compliance with any data protection law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Where an EU-style data protection law applies, careful consideration should be given to these issues during the proceedings and when considering Data Protection Directions. Not all of these issues arise in every arbitration and in some cases data protection issues will be raised that are not listed.

General Considerations

Are you covered by the GDPR?

Establishment

- Consider whether you are established in the EU through stable arrangements.
- Does the data processing in question occur "in the context of the activities" of that EU establishment?
- If so, subject to certain exceptions (*e.g.*, household information), all worldwide data processing activities associated with the activities of that EU establishment are covered by the GDPR.

Targeting

- If you decide you are not established in the EU, consider whether you have targeted EU data subjects for the purposes of offering services.
- If so, your data processing related to the offering of those services may be covered, but not necessarily your activities generally.

Am I data controller, processor or joint controller?

- Do you decide the purpose and means of the processing?

- If so, then you are a data controller responsible for compliance and being able to demonstrate compliance with the GDPR. Such control is generally inherent in the function of institutions, arbitrators, and legal counsel.
- Consider whether you jointly control the purpose and means of the processing with others involved in the arbitration, in which case you may be a joint controller together with the others with whom you exercise such joint control. **Caution**: joint control has been broadly defined and carries joint and several liability.
- If you process personal data but do not control the purpose and means of the data processing, then you are likely to be a data processor, for which you would require a GDPR-compliant data processing agreement with the data controller that has engaged you for the processing. This may be the case, for example, for online case management or hearing platforms, e-discovery firms, transcribers, and interpretation and translation services in certain contexts.

Preparing for a Case

Document Collection and Review: General

- Is any likely Arbitral Participant subject to a data protection law or regulation that may impact the arbitration?
- Does the arbitration agreement expressly address data protection or data security?
- Have any of the likely Arbitral Participants issued data privacy notices that may provide information about their status under data protection law or how they will treat data protection issues? What do they say?
- What kind of personal data is likely to be processed during the arbitration?
- Does it include sensitive data? Data related to a child? Criminal offence data?
- What is the lawful basis for processing the personal data in each of these categories?
- Where is the personal data in each of these categories likely to be located?
- Does the data collection and review require third country data transfer, and, if so, what is the lawful basis for the transfer? Consider mapping the data flows and putting in place standard contractual clauses.
- How will the personal data be collected and by whom?
- Is the amount of data being collected fair and proportionate to the claim?
- How has notice been provided to the data subjects identified in the data to be processed for the arbitration:

  - If notice has been provided, does it address the use of personal data for arbitration or dispute resolution?
  - If not, is data processing for the arbitration compatible with the purpose that was notified?
  - Is it necessary to send a further data privacy notice informing the individual data subjects that their personal data is being collected for use in a potential arbitration? Could this be done together with any arbitration hold that may be issued?
  - What impact would specific notification have on any confidentiality of the proceedings (that may have yet to be brought)?
- Have efforts been made to minimise the amount of data collected and reviewed? Has the data been culled? Has consideration been given to redacting or pseudonymising the personal data or sensitive data?
- Are adequate record-keeping measures in place to demonstrate compliance with data protection laws and regulations during the collection and review of data?
- What data retention and destruction policy is in place?
- Have you considered using an online case management platform to assist with data protection compliance, among other things?

What is my lawful basis for processing personal data?

- Consider the lawful basis for your processing of personal data.
- Consider whether the processing of data is necessary for the legitimate interests (of you or other Arbitral Participants), provided that the legitimate interest is not overridden by the rights and freedoms of the data subject.
- When relying on legitimate interests, consider undertaking a Legitimate Interests Assessment (*see* **Annex 5**).

Is consent a reliable lawful basis for processing personal data?

- Relying on consent creates uncertainty.
  - Consent must be obtained from each data subject, not from the parties. Employee consent is often considered to be invalid.
  - Consent may be refused or withdrawn at any time, in which case it may be difficult to rely upon another lawful basis for continued processing of the personal data. Consent is therefore not recommended as a lawful basis in the arbitration context and is only appropriate in limited circumstances, including in countries with consent-based data protection laws (like Canada under PIPEDA).

What is my lawful basis for processing special category data or personal data of a child?

- Consider your lawful basis for the processing of any special category data or personal data relating to a child.
- Is the processing of any special category data necessary to establish, exercise or defend a legal claim?

Can I process any criminal offence data?

- Consider whether you can process criminal offence data, which must be done under a supervising authority's control or as authorised by EU or Member State law.
- Member State law may allow the processing of personal data relating to criminal activity, for example, Member State law may allow processing where necessary to establish, exercise or defend a legal claim, including in arbitration.

What is my lawful basis for transferring any data outside the EU?

- Consider whether data will be transferred to third countries or international organisations.
- What is your lawful basis for the transfer of any personal data?
- Transfer is lawful to countries or international organisations: (1) where a country has been granted an adequacy decision; (2) if this is not the case, where appropriate safeguards (*e.g.*, standard contractual clauses) have been put in place; (3) if this is not feasible, a derogation can be relied upon, including where data transfers are necessary to establish, exercise or defend legal claims, provided that the personal data transfers are occasional and the personal data is minimised through culling and/or pseudonymisation/redaction, as appropriate; or (4) "compelling legitimate interests" support the transfer, which is a high threshold to meet, and also requires notification to both the data subjects and the supervisory authority.
- Standard contractual clauses should be put in place where this is feasible to do.
- Is any relevant data located in a country with a localisation regime (possibly Russia or China)? How will this be managed?

Arbitration agreement and arbitrator selection
– In reviewing potential legal counsel and/or arbitrator candidates, has consideration been given to how their appointment will impact the data protection profile of the arbitration? If located outside the EU, are they willing to enter into standard contractual clauses?
During the Arbitration
Case Management Conference
– Has data protection/data security been placed on the agenda for the initial procedural/case management conference?
Data Protection Directions
– Should data protection be addressed in the terms of reference, a procedural order, or by agreement of the parties in a data protection protocol?
Issues for potential inclusion in the Data Protection Directions
Lawful basis
– Identify the lawful basis for the processing during the arbitration process of any: (1) personal data; (2) sensitive data; (3) criminal offence data; or (4) personal data of a child.
Third country transfer
– Identify the lawful basis for the transfer of any: (1) personal data; (2) sensitive data; (3) criminal offence data; or (4) personal data of a child.
Document production
– Has consideration been give to how data protection compliance may impact document production? – Have standard contractual clauses been put in place for any third country data transfers? – What efforts will be taken to minimise the personal and sensitive data processed for the arbitration?

- Has consideration been given to the possibility of redaction and pseudonymisation of personal data, where necessary under the applicable data protection law?

Data security and data breach

Information security

- Have reasonable measures been put in place to protect the security of the information, including personal and sensitive data, to be processed in relation to the arbitration?
- Has consideration been given to the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration?
- Taking into consideration the existing information security practices of the Arbitral Participants, has consideration been given to agreeing in advance whether any additional information security measures may be required for the arbitration?

Data breach

- Has consideration been given to what constitutes a data breach?
- Have Arbitral Participants put a process in place for complying with their notification obligations if there is a data breach, taking into account the very short deadlines established in the GDPR and many other data protection laws for informing the relevant supervisory authority and/or data subjects of the data breach and the need for communication and cooperation among Arbitral Participants when notifying (*see* Cybersecurity Protocol, Schedule D-1)?

Data subject rights requests

- Have the Arbitral Participants identified what steps will be undertaken and who will be responsible for taking them if a data subject exercises their data subject rights, including data subject access requests, during the arbitration?

Notices

- Have data subjects been adequately notified of the personal data processing for the arbitration?

Record-keeping
– Have the Arbitral Participants put record-keeping measures in place to demonstrate compliance with the relevant data protection laws and regulations in a manner that can be shared with the data protection authorities if needed?
Use of on-line case management platforms
– Has consideration been given to the use of case management platforms as a means of facilitating data protection compliance during the arbitration, among other potential benefits?

ANNEX 4
Checklist: Online Case Management Platform

Introductory Remarks

Use of an Online Case Management Platform can assist Arbitral Participants to comply with their data protection and cybersecurity obligations, although it is important to recall that the use of the Platform itself constitutes data processing and must comply with applicable data protection laws. In the event that Arbitral Participants decide to use a platform, the checklist below may assist in discussions with a platform provider about compliance with data protection and cybersecurity requirements applicable to their particular arbitration.

Caution: Use of this checklist does not ensure compliance with any data protection law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. This checklist is not exhaustive of the questions that should be asked of a platform provider. Rather, it should only be considered a starting point for discussions about relevant data flows and data security arrangements. For further information on the questions to ask and practical steps to take before implementing online case management software in your arbitration, please refer to the Protocol for Online Case Management in International Arbitration.[1]

Platform Providers
Data Security
– Accountability for data security • Identify who has responsibility for the information security policy and when this was last updated. • Identify who manages and controls the operation of the platform and the physical security of the facilities in which the data is stored? • Determine if the platform relies on any external information systems or providers and their data access rights. • Identify who is responsible for managing system encryption. Determine if Arbitral Participants have (or want) the option to manage their own encryption keys.

1. https://protocol.techinarbitration.com/p/1.

- Ensure that the platform provider's staff are vetted, trained and monitored to ensure compliance with non-disclosure or confidentiality requirements.
- Identify the platform provider's data protection officer with responsibility for the tasks foreseen in GDPR and other relevant data protection laws. If located within the United Kingdom, for example, procure ICO data protection registration number and details or similar information for other jurisdictions.

– Standards the platform must meet
  - Enquire into to the information security or quality standards in relation to the services to be provided, *e.g.*, ISO 27001, ISO 27017, ISO 27018.
  - Enquire into applicable certifications for data storage, *e.g.*, SSAE 16, SOC 2, SOC 3.

– Legal aspects of the relationship with the platform provider
  - Review which information security legislation and regulatory policies have been considered in the design and operation of the platform.
  - Does the platform provider have a fully executed non-disclosure agreement for the engagement?
  - Review the platform provider's privacy policy.
  - If the platform provider develops any aspect of the platform, what is the system development lifecycle in place to support this process?
  - If the platform provider develops any mobile elements for the platform, how does it ensure this technology is appropriately secured?

– Contingency plans
  - What is the platform provider's business continuity plan? What are the results of its last business continuity test?
  - How does the platform provider protect against data leakage to ensure the continuous protection of data?
  - How does the platform provider ensure the integrity of data?
  - What is the platform provider's risk tolerance in the areas of threat and vulnerability remediation? What types of threats would it consider acceptable and what time frames does it target for remediation of those that are not acceptable?
  - How is the platform and data backed up (including frequency and the technologies in use)? How are these backups tested for recovery?

Data Storage

- Encryption and security controls
  - Is data on the platform encrypted, both in transit and at rest?
  - What are the physical security controls protecting the location where platform data would be stored (*e.g.*, physical entry arrangements - locked server cages, guarded access, video monitoring, visitor access controls etc.)?

- Jurisdictional concerns
  - What is/are the jurisdiction(s) in which data on the platform can be stored?
  - Does the platform provider have the ability to replicate and back up content in more than one jurisdiction, if needed?
  - Are there any bases on which the platform provider would seek to:
    - move or replicate data outside of the chosen region(s) without express consent from all relevant Arbitral Participants?
    - access, disclose or use platform data for any purpose beyond the services commissioned for this arbitration?

Data Privacy

- Access to data
  - Identify the employees or contractors in the platform provider who would be able to access platform data and the approval process for granting access.
  - What is the level of security applicable to remote access?
  - How would the platform provider respond to data subject access requests under applicable data protection laws?

Data Retention

- Do parties have the ability to delete permanently all or part of the information uploaded to the platform, including the ability to make permanent (*i.e.*, irreversible) redactions to documents?
- What is the platform provider's proposed retention period for platform data?
- Determine how data is destroyed when necessary.

ANNEX 5
Checklist: Legitimate Interests Assessment

Introductory Remarks

When the GDPR or another data protection law applies to an Arbitral Participant, the Arbitral Participant will be required to have a lawful basis for processing personal data during the arbitration.

When the GDPR applies, the preferred lawful basis will often be the legitimate interests of either the data controller, or a third party, or both (*see* Roadmap **Section II.B.3.c(1)**). When legitimate interests are employed as the lawful basis, the EU Working Party has taken the view that a Legitimate Interests Assessment should be performed.

This checklist contains a non-exhaustive list of considerations that should be applied in performing a Legitimate Interests Assessment.

Caution: Use of this checklist does not ensure compliance with the GDPR or any other law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Where an EU-style data protection law applies, careful consideration should be given to the lawful basis for the processing of personal data for the arbitration.

Am I relying on a legitimate interest for the processing of personal data for the arbitration?
– Controllers must have a lawful basis for processing personal data, which are set out in Article 6(1) of the GDPR. – Among other reasons, data processing is lawful where the processing is necessary for the legitimate interests of the controller or a third party, unless these interests are overridden by the individual's interests or fundamental rights. This lawful basis may be best suited for arbitration. – The EDPB has indicated that when relying on legitimate interests, a Legitimate Interests Assessment should be undertaken and documented.
What is the three-part test for applying a legitimate interest for the processing of personal data for the arbitration?
The EU Working Party has explained that there is a three-part test that should be applied when undertaking a Legitimate Interests Assessment:

- Identify the legitimate interest
- Carry out a "necessity test"
- Carry out a "balancing test"

What is my or a third party's legitimate interest?

The first step in a Legitimate Interests Assessment is to identify a legitimate interest – what is the purpose for processing the personal data and why is it important to you as a controller? In the context of an arbitration, the legitimate interest may involve the administration of justice, ensuring the parties' rights are respected and the expeditious and fair resolution of claims under the applicable arbitration rules, in addition to other interests.

The "necessity test": Is the processing necessary to achieve my or a third party's legitimate interests?

This prong of the test asks whether the processing of the personal data is necessary to achieve a party's legitimate interest. In applying this standard, Arbitral Participants might consider whether data minimisation techniques could be used to reduce the amount of personal data processed without infringing on all parties' rights to present and defend their respective cases.

The "balancing test": Have I balanced the interests?

The third prong of the test requires balancing the legitimate interest of the controller or a third party against those of the data subject and considering whether the legitimate interests of the data controller or a third party are overridden by those of the data subject. The balancing test should always be conducted fairly and must give due regard and weight to the rights and freedoms of individuals. Some factors to consider when deciding whether an individual's rights would override a controller's legitimate interest are:

- The nature of the data subject's interests;
- The potential impact of processing on the data subject's interests; and
- Any safeguards which are, or could be put, in place.

Have I documented the Legitimate Interests Assessment?

The EU Working Party has explained that the Legitimate Interests Assessment should be documented and if an issue arises, a supervisory authority is likely to review the documentation. This should therefore be done in a manner that can be disclosed on request.

ANNEX 6
Sample Standard Contractual Clauses for Controller-Controller Transfers under the GDPR

Introductory Remarks

Third country transfers by Arbitral Participants subject to the GDPR require a lawful basis. When the transfer involves a country that has not been granted an adequacy decision by the EU Commission, an "appropriate safeguard" should be put in place where feasible. In the case of arbitration, the most appropriate safeguard will likely be the "standard contractual clauses" (SCCs), which are the subject of this Annex. If entering into SCCs is not feasible, a specific derogation related to legal claims may be relied on if the conditions for doing so are considered to be met. However, the EDPB has indicated that where an appropriate safeguard can be put in place, it should be, rather than relying on a derogation.

The substantive obligations included in the SCCs impose a lightweight form of the GDPR on the data importer (i.e., the recipient of the personal data), supported by third party rights for data subjects. The precise obligations vary depending on the status of the parties to the transfer. After the CJEU decision of 2020 in *Schrems II* (Case C311/18), the European Commission put in place new, and stricter, SCCs reflecting the Court's decision and the requirements of the GDPR. The SCCs follow a modular approach, containing a set of provisions allowing draft transfers from:

- Controller to controller (Module 1);
- Controller to processor (Module 2);
- Processor to sub-processor (Module 3); and
- Processor to controller (Module 4).

The SCCs operate on a multi-party basis, allowing a single set of SCCs to cover transfers of personal data between a number of parties. Moreover, they include a "docking clause" allowing new parties to be added over time. This will be useful in an arbitration context.

As discussed in the Roadmap, Arbitral Participants will usually be data controllers, therefore Module 1 (controller-controller transfers) will apply. This Annex therefore provides a compiled version of the SCCs for controller-controller transfers, which includes the following obligations:

- *Transfer impact assessment:* The parties to SCCs must assess and document the impact of the transfers before they are entered into.

- *Purpose limitation:* The data importer can only use personal data for the purposes described in the SCCs, unless the processing is necessary for legal claims, which will usually be the case in arbitration.
- *Transparency:* The data importer must, directly or via the data exporter (*i.e.*, the sender), provide data subjects with certain information, including its identity and any onward transfers.
- *Other principles:* The data importer must comply with the principles of accuracy, data minimisation and limited data retention.
- *Security:* The data importer must keep the personal data secure. If there is a breach, it may need to notify the data exporter, data subjects and the supervisory authority(ies), depending on the severity of the breach.
- *Onward transfer:* There are specific controls on onward transfers to third parties outside the EU (including a third party signing up to the SCCs), unless certain conditions are met.
- *Data subject rights:* The data importer must comply with data subject rights, including data subject access rights, and rights to correct, object to processing and erase personal data where applicable.
- *Complaints mechanism:* The data importer must provide a complaints handling process for data subjects.
- *Submission to jurisdiction:* The data importer must submit to EU jurisdiction. This includes submitting to the jurisdiction of the relevant supervisory authority(ies) and the courts in which the data subjects have their residence. Data subjects will be entitled to material and non-material damages and the data exporter and the data importer will be jointly and severally liable.
- *Access by public authorities:* Notification to the data exporter and, where possible, the data subject must be made if the personal data held by the data importer is subsequently accessed by public authorities.

Note that the Appendices of the SCCs need to be completed. The SCCs provide for choices to be made in relation to certain provisions. However, in order to be valid, the SCC terms cannot be changed. The SCCs can be included in another agreement, provided that the terms remain the same.

The following is directly excerpted from Module 1 for controller-to-controller data transfers only, of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) C/2021/3972.

Disclaimer: This document was generated based on the text available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 and is provided for convenience purposes. It should not be considered an authoritative text or legal guidance

CONTROLLER-TO-CONTROLLER STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

1. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
   (i) of its identity and contact details;
   (ii) of the categories of personal data processed;
   (iii) of the right to obtain a copy of these Clauses;
   (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

---

2. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with Recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to

significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

---

3. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

Not applicable.

Clause 10
Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the

enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:
   (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
   (ii) rectify inaccurate or incomplete data concerning the data subject;
   (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
   (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
   (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

4. That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

5. The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with

Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one

of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[6]
   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

---

6. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to

document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   (ii) the data importer is in substantial or persistent breach of these Clauses; or
   (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the

country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of _____ **(*specify Member State*).**

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ **(*specify Member State*).**

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIXES

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I
A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: . . . . . .

Address: . . . . . .

Contact person's name, position and contact details: . . . . . .

Activities relevant to the data transferred under these Clauses: . . . . . .

Signature and date: . . . . . .

Role (controller/processor): . . . . . .

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: . . . . . .

Address: . . . . . .

Contact person's name, position and contact details: . . . . . .

Activities relevant to the data transferred under these Clauses: . . . . . .

Signature and date: . . . . . .

Role (controller/processor): . . . . . .

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

. . . . . .

Categories of personal data transferred

. . . . . .

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

. . . . . .

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

. . . . . .

Nature of the processing

. . . . . .

Purpose(s) of the data transfer and further processing

. . . . . .

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

. . . . . .

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

. . . . . .

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

. . . . . .

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

ANNEX III – LIST OF SUB-PROCESSORS

Not applicable.

ANNEX 7
Sample Provisions for Data Protection Directions

Introductory Remarks

This language contains possible wording that could be considered for inclusion in Data Protection Directions. The wording takes into account the GDPR, and indications are given where the GDPR is referred to.

Caution: Use of this generic language does not ensure compliance with any law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Before including any language addressing data protection issues, careful consideration should be given to what is appropriate for the specific case. This generic language therefore must be modified to reflect the circumstances of the case, the procedural context, and the instrument in which it will be recorded. For example, the language will need to be modified depending on whether it is being entered into by agreement or by order.

Responsibility for Compliance

1. The Parties and their Legal Representatives shall be responsible:

    i. To ensure that their processing of all personal data of the Arbitral Participants and other data subjects for the purpose of use in this Arbitration has been carried out in compliance with the [**GDPR**] and any other applicable data protection laws in so far as applicable;
    ii. To take steps to ensure that data subjects whose personal data may be processed in this Arbitration are provided with any legally required notice unless an exemption applies; and
    iii. To ensure that all third parties with whom they share information personal data (including sensitive/special category) obtained during the Arbitration (for example, service providers) are aware of and abide by their data protection obligations with respect to that data, including entering into a [**GDPR compliant**] data processing agreement where required.

Legal Basis for the Processing and Transfer of Personal Data

2. Personal data in this Arbitration is processed for the purpose of the legitimate interests of the Parties in resolving this dispute and to ensure that the arbitral process operates efficiently and expeditiously and that the rights of the Parties are

respected except where such interests are overridden by the interests or fundamental rights of the data subject.

3. In so far as any special category of personal data is processed it is because it is necessary for the establishment, exercise or defence of legal claims.

4. All Parties, Legal Representatives and arbitrators who are not based in the EEA or in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission, have agreed to enter into controller-to-controller standard contractual clauses as promulgated by the European Commission.

5. If a transfer of personal data is made to a recipient who is [**outside of the EEA**] and not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission and who has not entered into standard contractual clauses, such transfers will be occasional and made to the extent necessary for the Parties to establish, exercise or defend their legal claims.

6. If any Party or Legal Repetitive considers that processing and transfer on these bases is not appropriate, it shall notify the Tribunal forthwith.

7. The Parties and their Legal Representatives agree that they shall not do anything contrary to the principles set forth in paragraphs 2-6, including but not limited to seeking data subject consent, without first raising the issue with the Tribunal and obtaining directions.

Confidentiality [To be omitted in non-confidential arbitrations, but see footnote][1]

8. This Arbitration, including all communications between the Tribunal, Institution, and the Parties, shall be confidential.

9. The Parties have undertaken as a general principle to keep confidential all awards in the Arbitration, together with all materials in the Arbitration created for the purpose of the Arbitration and all other documents produced by another Party in the proceedings not otherwise in the public domain (the "**Arbitration Materials**").

1. Confidentiality of the proceedings is not required by data protection laws, but the extent to which the proceedings are confidential may be considered in deciding whether the rights of the data subjects have been adequately protected.

This obligation applies save and to the extent that disclosure may be required of a Party by legal duty, to protect or pursue a legal right, or to enforce or challenge an award in legal proceedings before a state court or other legal authority (a "**Specified Disclosure Purpose**").

10. To the extent that any Arbitral Participant needs to disclose any of the Arbitration Materials for a Specified Disclosure Purpose, such Arbitral Participant shall seek to ensure that the confidentiality of those materials is respected so far as possible under the applicable national law.

Document Disclosure

11. The Parties and their Legal Representatives agree that they shall minimise the personal data (including any sensitive/special categories of personal data) that is processed for the Arbitration including during document disclosure.

12. [Document disclosure will be pursuant to the IBA Rules to ensure focused and specific disclosure which is relevant and material to the outcome of the dispute, and documents not falling within this category shall not be processed for the Arbitration.] **[To be included where IBA Rules apply.]**

13. The Parties and their Legal Representatives will attempt to agree whether redaction or pseudonymisation is necessary and shall take such steps as are necessary to redact or otherwise remove any personal data (including any special categories of personal data) that is not relevant or necessary for the purpose of this Arbitration.

14. Parties, witnesses and data subjects who are referred to in the evidence or the pleadings in particular should be made aware by their Legal Representatives that it may be necessary to refer to their personal data (including any special categories of personal data) in an arbitral award.

Security and Cybersecurity [refer to ICCA-NYC Bar-CPR Cybersecurity Protocol for other possible measures to be considered]

15. The Parties and their Legal Representatives shall ensure that the storage and exchange of the personal data processed in this Arbitration is protected by way of appropriate technical and organisational safeguards, including through the use of secure servers and password-protected access, and taking into account the scope and risk of the processing, including the impact on data subjects, the capabilities and regulatory requirements of all those involved in the Arbitration, the costs of implementation, and the nature of the information being processed

or transferred, including the extent to which it includes personal data or sensitive commercial, proprietary or confidential information. This should include, as appropriate:

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

16. The individuals who shall have access to such personal data shall be limited to individuals based on a need-to-know basis in connection with this Arbitration.

Personal Data Breach

17. The Arbitral Participants shall monitor the security of their electronic systems and the location of any hard or soft copies of personal data in their possession which is being or has been processed in this Arbitration.

18. Should any Arbitral Participant determine that a data breach has occurred involving the personal data processed by them in this Arbitration, they shall without undue delay, and in any case within 72 hours, notify the other Arbitral Participants including all information they are aware of concerning the data breach.

19. Each Arbitral Participant shall take appropriate steps to address and mitigate the consequences of such breach and comply with applicable legal requirements.

20. To the extent that any Arbitral Participant decides to notify the data breach to a supervisory authority or to a data subject, they shall also inform the other Arbitral Participants of the notification in advance.

21. The Parties agree that they shall inform each other, and, to the extent feasible, cooperate in relation to the notification of any data breach impacting arbitral data.

Hearings

22. With respect to hearings and conferences, whether remote or in person, the Parties and their Legal Representatives shall:

i. Ensure that the processing of all personal data of the Arbitral Participants and other data subjects during the course of any hearing is carried out in compliance with the [GDPR] and any other applicable data protection laws, taking into account that the transmission of data during a remote hearing generally will constitute a data transfer.
ii. Ensure that any platform used for a remote hearing complies with the security measures set forth herein, and is protected by way of appropriate technical and organisational safeguards.
iii. Consider the impact on data protection compliance and the rights and interests of data subjects, including witnesses, of any means employed to memorialise the hearing, including the use of transcripts and recording devices.
iv. Include measures aimed at compliance with this paragraph in any protocol, directions or agreement that are adopted for the hearing.

Data Subject Rights

23. Any Arbitral Participant who receives any request from any data subject in respect of the processing of their personal data in relation to this Arbitration, shall promptly notify the other Arbitral Participants of such request unless it is prohibited from doing so by applicable law.

24. Where the Arbitral Participant who receives the data subject request did not originally collect the personal data from the data subject, the Arbitral Participant receiving the request may (but is not obliged to) consult with the data controller who originally collected the personal data to decide how best to address the data subject request within the applicable law.

25. The Arbitral Participants agree that they shall consider such requests fairly and promptly and make any necessary alteration to that data subject's personal data promptly and notify all Parties and the Tribunal of the need to do the same.

26. The Arbitral Participants agree that they shall cooperate to ensure that data subject requests are made in good faith and minimise the impact on the Arbitration of any data subject request.

Documentation of Compliance

27. It is agreed that the Tribunal shall maintain a non-confidential version of the data protection compliance efforts in this arbitration, in a form that can be shared with third parties, including supervisory authorities. It is agreed that these data protection directions together with any other documentation of compliance efforts

shall be maintained by the Tribunal and can be shared as necessary to establish compliance.

Use of Online Case Management Platform

28. The Parties have agreed to use an online case management platform to assist with information security, data protection compliance, and document production and shall agree the parameters in advance with each other, and also with the Tribunal as appropriate.

ANNEX 8
Sample Data Protection Protocol under the GDPR

Introductory Remarks

This language contains possible wording for a Data Protection Protocol where a relevant data protection law applies to one or more Arbitral Participants. Where possible, preferred practice would be to enter into a signed Data Protection Protocol and by this means to enter into the SCCs. The main difference between the Data Protection Directions found in Annex 7 and this Data Protection Protocol is that the protocol is set up as an agreement and has broader coverage. Note that where the same issue is covered by both documents, the treatment is largely the same. The wording takes into account the GDPR, and indications are given where the GDPR is referred to.

Caution: Use of this generic language does not ensure compliance with any law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Before including any language addressing data protection issues, careful consideration should be given to what is appropriate for the specific case, including a Legitimate Interest and Transfer Assessment where appropriate. This generic language therefore must be modified to reflect the circumstances of the case, the procedural context, and the instrument in which it will be recorded. For example, the language will need to be modified depending on whether it is being entered into by agreement or by order.

DATA PROTECTION PROTOCOL
Introduction
1. This protocol addresses data protection issues under the [**General Data Protection Regulation 2016** ("**GDPR**") **and other data protection laws, namely relevant national law implementing and supplementing data protection including the GDPR to the extent applicable**] ("**Data Protection Laws**") for the purpose of this Arbitration. It is subject to review and amendment as appropriate during the course of the Arbitration. 2. The definitions and meanings used [**in the GDPR**] apply to this Protocol including references to the following: "**data controller**"; "**data subject(s)**"; "**personal data**"; "**personal data breach**"; "**process/processing**"; "**processor**"; and "**special categories of personal data**".

3. The seat of this Arbitration is [**location**].

4. The following individuals and entities (and their respective individual representatives), in addition to the arbitrator(s) (the "**Tribunal**"), are or are likely to be involved in the Arbitration:

   i. The Claimant;
   ii. The Respondent (together the "**Parties**");
   iii. The legal representatives of the Claimant and Respondent namely [**LAW FIRM A**] ("**Firm A**") and [**LAW FIRM B**] ("**Firm B**") and any [**barristers/advocates**] engaged by the Parties (together the "**Legal Representatives**");
   iv. The Arbitral Institution [**insert name**] (the "**Institution**"); and
   v. (i-iv) together being the "**Arbitral Participants**."

Responsibility for Compliance

5. The Arbitral Participants are data controllers for the purposes of the Data Protection Laws.

6. Each data controller to which [**the GDPR**] applies has a responsibility to comply with [**the provisions of the GDPR**] and to be able to demonstrate compliance. Each Arbitral Participant agrees to keep adequate records of its data protection compliance activities during the course of the Arbitration in a non-confidential form which they may, at their discretion, disclose to any competent regulatory authority after informing the other Arbitral Participants.

7. Any natural or legal person involved in the Arbitration that considers itself or others acting on its behalf to be bound by a relevant data protection law or regulation shall inform the Tribunal as soon as practicable taking into consideration the orderly conduct of the proceedings. This means that, absent unusual circumstances, general data protection issues will be raised at the case management conference if not before to the extent the Parties and their Legal Representatives are aware of them. Issues coming to light later in the proceedings may be raised at that time.

8. The Tribunal may issue binding directions applying data protection principles during the Arbitration to the extent appropriate for the efficient resolution of the dispute.

9. The Parties and their Legal Representatives shall be responsible:

i. To ensure that their processing of all personal data of the Arbitral Participants and other data subjects for the purpose of use in this Arbitration has been carried out in compliance with the [**GDPR**] and any other Data Protection Laws in so far as applicable;
ii. To take steps to ensure that data subjects (including those who are not Arbitral Participants, such as those mentioned in witness statements and evidence) whose personal data may be processed in this Arbitration are provided with any legally required notice unless an exemption applies;
iii. To ensure that all third parties with whom they share personal data (including sensitive/special category) obtained during the Arbitration (for example, service providers) are aware of, and abide by, their data protection obligations with respect to that data, including entering into a [**GDPR compliant**] data processing agreement where required; and
iv. To indemnify the Tribunal and hold the Tribunal members harmless to the full extent legally allowed from any third-party claims or regulatory proceedings arising from any breach of any applicable data protection laws during the course of, or otherwise related to, the Arbitration.

Personal Data Likely to be Processed during the Arbitration

10. The following personal data may be processed during this Arbitration:

i. Personal identification information and biographical and contact information;
ii. Financial information;
iii. Information as to any legal or regulatory impediment including international sanctions;
iv. Employment related information;
v. Information concerning the events surrounding the facts of the arbitration; and
vi. Other personal information such as ethnicity, family members, medical conditions (*i.e.*, sensitive or special categories of personal data).

Personal data relating to criminal convictions or offences shall not be processed or presented to the Tribunal without advance notice and permission to do so.

How and When Such Information will be Processed

11. Personal data (including sensitive or special categories of personal data) may be processed as follows:

i. In the preparation, transmission and service of all arbitral pleadings, memorials, evidence and submissions;
ii. In the preparation, transmission and service of any witness statement or expert report;
iii. During the process of document production;
iv. During the transmission of communications, in particular e-mails, between the Tribunal and the Legal Representatives and between the Parties and the Legal Representatives;
v. In preparing and delivery of orders of the Tribunal and the preparation and delivery of any arbitral awards;
vi. In communications with the Institution; and
vii. To other third parties for the purpose of the smooth running of the Arbitration, such as transcribers and interpreters.

Legal Basis for the Processing and Third Country Transfer of Personal Data

12. Personal data in this Arbitration is processed for the purpose of the legitimate interests of the Parties in resolving this dispute and to ensure that the arbitral process operates efficiently and expeditiously and that the rights of the Parties are respected, except where such interests are overridden by the interests or fundamental rights of the data subject**. [The Tribunal has undertaken a Legitimate Interests Assessment.]** [***See*** Annex 5]

13. Insofar as any special category of personal data is processed it is because it is necessary for the establishment, exercise or defence of legal claims.

14. All Parties, Legal Representatives and arbitrators who are not based in the EEA or in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission, have agreed to enter into controller-to-controller standard contractual clauses as promulgated by the European Commission in the form attached hereto **[copy of Annex 6 with Annexes completed should be attached].**

15. If a transfer of personal data is made to a recipient who is [**outside of the EEA**] who is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Commission and who has not entered into standard contractual clauses, such transfers will be occasional, the personal data shall be minimised including redaction and/or pseudonymisation where appropriate and shall be made only to the extent necessary for the Parties to establish, exercise or defend their legal claims.

16. If any Party or Legal Representative considers that processing and transfer on these bases is not appropriate, it shall notify the Tribunal forthwith.

17. The Parties and their Legal Representatives agree that they shall not do anything contrary to the principles set forth in paragraphs 12-14, including but not limited to seeking data subject consent, without first raising the issue with the Tribunal and obtaining directions.

Confidentiality [To be omitted in non-confidential arbitrations, but see footnote][1]

18. This Arbitration, including all communications between the Tribunal, Institution, and the Parties, shall be confidential.

19. The Parties have undertaken as a general principle to keep confidential all awards in the Arbitration, together with all materials in the Arbitration created for the purpose of the Arbitration and all other documents produced by another Party in the proceedings not otherwise in the public domain (the "**Arbitration Materials**"). This obligation applies save and to the extent that disclosure may be required of a Party by legal duty, to protect or pursue a legal right, or to enforce or challenge an award in legal proceedings before a state court or other legal authority (a "**Specified Disclosure Purpose**").

20. To the extent that any Arbitral Participant needs to disclose any of the Arbitration Materials for a Specified Disclosure Purpose, such Arbitral Participant shall seek to ensure that the confidentiality of those materials is respected so far as possible under the applicable national law.

Document Production

21. The Parties and their Legal Representatives agree that they shall minimise the personal data (including any sensitive/special categories of personal data) that is processed for the Arbitration including during document disclosure.

22. [Document production will be pursuant to the IBA Rules to ensure focused and specific disclosure which is relevant and material to the outcome of the dispute,

1. Confidentiality of the proceedings is not required by data protection laws, but the extent to which the proceedings are confidential may be considered in deciding whether the rights of the data subjects have been adequately protected.

and documents not falling within this category shall not be processed for the Arbitration.] **[To be included where IBA Rules apply.]**

23. The Parties and their Legal Representatives will attempt to agree whether redaction or pseudonymisation is necessary and shall take such steps as are necessary to redact or otherwise remove any personal data (including any special categories of personal data) that is not relevant or necessary for the purpose of this Arbitration.

24. Parties, witnesses and data subjects who are referred to in the evidence or the pleadings in particular should be made aware by their Legal Representatives that it may be necessary to refer to their personal data (including any special categories of personal data) in an arbitral award.

Security and Cybersecurity [refer to ICCA-NYC Bar-CPR Cybersecurity Protocol for other possible measures to be considered]

25. The Parties and their Legal Representatives shall ensure that the storage and exchange of the personal data processed in this Arbitration is protected by way of appropriate technical and organisational safeguards, including through the use of secure servers and password-protected access, and taking into account the scope and risk of the processing, including the impact on data subjects, the capabilities and regulatory requirements of all those involved in the Arbitration, the costs of implementation, and the nature of the information being processed or transferred, including the extent to which it includes personal data or sensitive commercial, proprietary or confidential information. This should include, as appropriate:

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

26. The individuals who shall have access to such personal data shall be limited to individuals based on a need-to-know basis in connection with this Arbitration.

Personal Data Breach

27. The Arbitral Participants shall monitor the security of their electronic systems and the location of any hard or soft copies of personal data in their possession which is being or has been processed in this Arbitration.

28. Should any Arbitral Participant determine that a data breach has occurred involving the personal data processed by them in this Arbitration, they shall without undue delay, and in any case within 72 hours, notify the other Arbitral Participants including all information they are aware of concerning the data breach.

29. Each Arbitral Participant shall take appropriate steps to address and mitigate the consequences of such breach and comply with applicable legal requirements.

30. To the extent that any Arbitral Participant decides to notify the data breach to a supervisory authority or to a data subject, they shall also inform the other Arbitral Participants of the notification in advance.

31. The Parties agree that they shall inform each other, and to the extent feasible, cooperate in relation to the notification any data breach impacting arbitral data.

Hearings

32. With respect to hearings and conferences, whether remote or in person, the Parties and their Legal Representatives shall:

    i. Ensure that the processing of all personal data of the Arbitral Participants and other data subjects during the course of any hearing is carried out in compliance with the [GDPR] and any other applicable data protection laws, taking into account that the transmission of data during a remote hearing generally will constitute a data transfer.
    ii. Ensure that any platform used for a remote hearing complies with the security measures set forth herein, and is protected by way of appropriate technical and organisational safeguards.
    iii. Consider the impact on data protection compliance and the rights and interests of data subjects, including witnesses, of any means employed to memorialise the hearing, including the use of transcripts and recording devices.
    iv. Include measures aimed at compliance with this paragraph in any protocol, directions or agreement that are adopted for the hearing.

Data Subject Rights

33. Any Arbitral Participant who receives any request from any data subject in respect of the processing of their personal data in relation to this Arbitration, shall promptly notify the other Arbitral Participants of such request unless it is prohibited from doing so by applicable law.

34. Where the Arbitral Participant who receives the data subject request did not originally collect the personal data from the data subject, the Arbitral Participant receiving the request may (but is not obliged to) consult with the data controller who originally collected the personal data to decide how best to address the data subject request within the applicable law.

35. The Arbitral Participants agree that they shall consider such requests fairly and promptly and make any necessary alteration to that data subject's personal data promptly and notify all Parties and the Tribunal of the need to do the same.

36. The Arbitral Participants agree that they shall cooperate to ensure that data subject requests are made in good faith and minimise the impact on the Arbitration of any data subject request.

Documentation of Compliance

37. It is agreed that the Tribunal shall maintain a non-confidential version of the data protection compliance efforts in this arbitration, in a form that can be shared with third parties, including supervisory authorities. It is agreed that this data protection protocol together with any other documentation of compliance efforts shall be maintained by the Tribunal and can be shared as necessary to establish compliance.

Use of Online Case Management Platform

38. The Parties have agreed to use an online case management platform to assist with information security, data protection compliance, and document production and shall agree the parameters in advance with each other, and also with the Tribunal as appropriate.

ANNEX 9
Sample Privacy Notices

Introductory Remarks

Arbitral Participants covered by the GDPR or another EU-style data protection law should consider whether to issue a Data Privacy Notice in relation to their arbitration-related activities, and if so, the content of that notice, taking into account that their data processing practices must reflect the notice given.

We have prepared sample Data Privacy Notices below. They are based on the GDPR, although most data protection laws require similar notices.

The language suggestions below are tailored for arbitration-related activities only. Arbitral Participants should consider either issuing a separate privacy notice addressing any other data processing activities they are engaged in (for example, marketing), or modifying the sample notice to include all activities.

Caution: Use of these notices does not ensure compliance with any law or regulation. Each Arbitral Participant has individual responsibility for data protection compliance. Where an EU-style data protection law applies, careful consideration should be given to whether a Data Privacy Notice is required and if so, its content. The Sample Notices are not intended to be exhaustive and Arbitral Participants must assess and reflect their specific data processing activities. Where applicable, these considerations will impact each Arbitral Participant.

ANNEX 9A
Data Privacy Notice for Arbitral Institutions[1]

SAMPLE ONLY

SAMPLE DATA PRIVACY NOTICE FOR ARBITRAL INSTITUTIONS

Last Updated: [●]

Purpose of this Privacy Notice

The [**Name of Institution**] ("[**Name of Institution]" "we" or "us")** performs dispute resolution services and carries out other activities in relation to disputes or potential disputes, both during their pendency and after their conclusion, including under the [**Name of Institution**] Arbitration Rules (and the [**Name of Institution**] Mediation Rules] ("**[Name of Institution] Proceedings**" or "**Proceedings**").

This Privacy Notice describes how [**Name of Institution**] collects and processes personal data in the context of those services and activities. This Privacy Notice is not intended to override any other privacy-related orders or notices that may be issued in the context of [**Name of Institution**] Proceedings or that we may provide you in specific circumstances. Our privacy notice for all other activities that do not relate to [**Name of Institution**] Proceedings can be found here. [**Link**]

[**Name of Institution**] Proceedings may finally determine the rights and interests of persons (both individuals and legal entities) and must therefore be undertaken fairly and impartially. While the [**Name of Institution**] does not determine the outcome of disputes itself, we play an important role in ensuring that justice is administered in [**Name of Institution**] Proceedings, and that the parties' fundamental rights to due process, equal treatment and to present their case and to be heard are protected.

1. In the case of arbitrations administered by an international organisation, determining whether any relevant privileges and immunities will impact the application of data protection laws turns on the breadth and scope of the relevant privileges and immunities, as well as the language of the relevant data protection law, both in terms of whether data protection laws would come within their scope, and, if so, which Arbitral Participants would be covered by them. This is an institution-specific and arbitration-specific enquiry, which goes beyond the scope of this Roadmap.

The conduct of [**Name of Institution**] Proceedings requires that personal data is processed that relates to arbitrators, mediators, adjudicators, experts and others acting or potentially acting in similar roles ("**Neutrals**"), as well as tribunal secretaries, members of the [**Name of Institution**] Court, parties, their authorised representatives and legal counsel, witnesses and all other individuals that may be identified or identifiable in any information that is processed by the [**Name of Institution**] in the context of the [**Name of Institution**] Proceedings.

The [**Name of Institution**] acts as a controller of personal data for some of its activities in the context of [**Name of Institution**] Proceedings. You should be aware that others may also act as data controllers during [**Name of Institution**] Proceedings, for example, the parties, their authorised representative or legal counsel and Neutrals. The [**Name of Institution**] is the responsible entity for the data processing activities that it undertakes as an institution, but not for the activities undertaken by other data controllers in the context of [**Name of Institution**] Proceedings. Their activities are not the subject of this Privacy Notice.

Please note that when, in the context of [**Name of Institution**] Proceedings, you provide any personal data relating to an individual with whom we or the person to whom the personal data is submitted have no direct relationship, it is your duty to provide the individual data subject with adequate notice that their data is being processed for this purpose and to comply with your other applicable data protection obligations.

This Privacy Notice is in effect as of the date indicated at the end of this Privacy Notice. A footer to this Privacy Notice will be placed on all communications during [**Name of Institution**] Proceedings. If we make material changes to this Privacy Notice, we will indicate this in the footer and update this Privacy Notice on our website with a changed date at: [**Link**].

If you have any questions about this Privacy Notice, or how we treat your personal data in the context of [**Name of Institution**] Proceedings, or if you wish to exercise any of your data subject rights, please refer to the details found at the end of this Privacy Notice.

What personal data do we collect and how do we collect it?

Depending on the circumstances, we may obtain the following personal data about you:

*Neutrals/Tribunal Secretaries/Members of the [**Name of Institution**] Court*

– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and

other personal data submitted to us by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the [**Name of Institution**] Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with [**Name of Institution**] Proceedings;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Individual Parties/Party's Authorised Representatives/Legal Counsel

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to us by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the [**Name of Institution**] Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with [**Name of Institution**] Proceedings;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Fact and Expert Witnesses

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to us by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the [**Name of Institution**] Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with [**Name of Institution**] Proceedings;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment;
- Personal data you choose to include in your witness statement or expert report and any oral testimony you may give (which may be transcribed), as submitted to us during [**Name of Institution**] Proceedings in which you provide written or oral evidence;
- Any other personal data of yours submitted to us by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the [**Name of Institution**] Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with [**Name of Institution**] Proceedings in which you provide written or oral evidence.

Other Individuals

– Personal data of yours submitted to us by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a member of the [**Name of Institution**] Court, or otherwise disclosed to or collected by us from third parties or publicly available resources, in connection with [**Name of Institution**] Proceedings.

How do we use your personal information and on what legal basis?

Depending on the circumstances in which we process your personal data, we may use your personal data in the following ways and on the legal bases described below:

*Neutrals/Tribunal Secretaries/Members of the [**Name of Institution**] Court*

– To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in [**Name of Institution**] Proceedings, as necessary to further our and the parties' legitimate interests[2] in ensuring that only suitable candidates are appointed and that conflicts of interest do not arise that could undermine the actual or perceived integrity of [**Name of Institution**] Proceedings;
– To maintain a database of potential Neutrals and tribunal secretaries as necessary to further our and potential parties' legitimate interests in identifying and appointing suitable Neutrals and tribunal secretaries;
– To decide and potentially publish [**to be completed where the institution publishes arbitration-related materials**];
– To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of [**Name of Institution**] Proceedings, as necessary for the performance of our agreements with you and duties under them;
– To facilitate the general conduct of [**Name of Institution**] Proceedings, including to communicate with you, facilitate communications between arbitral participants, and to fulfil other administrative tasks in relation to [**Name of Institution**] Proceedings, as necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the [**Name of Institution**]'s interests in ensuring that the arbitral process

2. Any time legitimate interests are relied on in the EU, consideration should be given to undertaking a documented Legitimate Interests Assessment (*see* Annex 5).

operates efficiently and expeditiously and that the rights of the parties are respected;
- Where necessary to meet our legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering ("**Legal Compliance Obligations**").

Individual Parties/Party's Authorised Representative and Legal Counsel

- To provide services in relation to [**Name of Institution**] Proceedings (including remitting funds) and to communicate with you in your capacity as a party to [**Name of Institution**] Proceedings or an authorised representative or legal counsel of a party, as necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the [**Name of Institution**]'s interests in ensuring that the arbitral process operates efficiently and expeditiously and that the rights of the parties are respected;
- Where we have entered into an agreement to provide services to you as an individual in connection with [**Name of Institution**] Proceedings (for example, claims brought by individuals), we may process your personal data (only) as necessary to perform our obligations and duties under that agreement;
- Where necessary to meet our Legal Compliance Obligations.

Expert and Fact Witnesses

- To facilitate your giving of evidence in [**Name of Institution**] Proceedings, and the examination of such evidence, as necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the [**Name of Institution**]'s interests in ensuring that [**Name of Institution**] Proceedings operate efficiently and expeditiously and that the rights of the parties are respected;
- Where necessary to meet our Legal Compliance Obligations.

Other Individuals

- As necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the [**Name of Institution**]'s interests in ensuring that [**Name of Institution**] Proceedings operate efficiently and expeditiously and that the rights of the parties are respected;
- Where necessary to meet our Legal Compliance Obligations.

How do we share your personal information?

Depending on the circumstances in which we handle your personal data, we may share it with the following natural and legal persons, as necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the [**Name of Institution**]'s interests in ensuring that [**Name of Institution**] Proceedings operate efficiently and expeditiously and that the rights of the parties are respected or as otherwise set out below:

- [**Name of Institution**] Court members to further the administration of cases [**add other activities of the relevant Court**];
- Other participants in [**Name of Institution**] Proceedings in which you are involved, for example professional transcribers or other service providers;
- Our service providers such as our third-party data hosting providers in order for us to provide services in connection with [**Name of Institution**] Proceedings;
- Third parties including our professional advisors, financial institutions or law enforcement agencies, where necessary to comply with our Legal Compliance Obligations, or where it is otherwise in our or a party's legitimate interests to do so.

Where do we transfer your personal data?

From time to time we transfer personal data to third countries in connection with the services we perform in relation to [**Name of Institution**] Proceedings in which you are involved, or as may otherwise become necessary in the course of our operations. We make such transfers where there is a lawful basis for doing so.[3]

How long do we retain your personal information?

We will only keep your personal data for as long as is reasonably necessary in the circumstances. Retention periods vary depending on the category of data, taking into

3. Where the GDPR applies, consideration should be given to the following language:
   If the recipient is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the relevant regulatory body, we make such transfers in accordance with our legal obligations, for example where the standard contractual clauses or another adequacy mechanism promulgated by the European Union have been entered into, or if this is not feasible, the transfers are necessary to establish, exercise or defend legal claims in the context of [**Name of Institution**] Proceedings, or where there is another lawful basis to do so.

account legal and regulatory requirements, limitation periods for taking legal action, good practice and the lawful basis on which we process your personal data.

What rights do you have over your personal data?

Depending on the circumstances, you have a number of rights over the personal data that we process about you. These may include the right to:

- Request access to your personal data and to obtain a copy of it from us, where this would not adversely affect the rights and freedoms of others;
- Correct your personal data that we hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for us continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defence;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defence;
- Request us to stop processing your personal data when it is being processed based on your consent;
- Object to your personal data being processed if the lawful basis for processing it is either our or a third party's legitimate interests, unless there are overriding legitimate grounds for the processing;
- Require certain of your personal data to be transferred to you or a third party to the extent that the data was collected directly from you; and
- Lodge a complaint with the relevant data protection authority.

If you wish to exercise any of these rights, or if you have any questions about this notice or how we treat your personal data, you can contact us:

- By email: [**TO BE ADDED**]

- By post: [**TO BE ADDED**]

Please note that if you are an employee of, nominated or engaged by, or otherwise affiliated with a party to an [**Name of Institution**] Proceeding, we suggest that you raise your concerns with that party in the first instance before contacting the [**Name of Institution**] regarding the processing of your personal data in the context of [**Name of Institution**] Proceedings.

Date: [**dd mm year**]

ANNEX 9B
Data Privacy Notice for Arbitrators

SAMPLE ONLY

SAMPLE DATA PRIVACY NOTICE FOR ARBITRATORS

Last Updated: [●]

Purpose of this Privacy Notice

[**Name of Arbitrator**] (**"I" or "me")** acts as an arbitrator and carries out other activities in relation to disputes or potential disputes, both during the pendency of such disputes and after their conclusion ("**Arbitral Proceedings**").

This Privacy Notice describes how I collect and process personal data in the context of those services and activities. This Privacy Notice is not intended to override any other privacy-related orders or notices that either I or a tribunal of which I am a part may issue in the context of the Proceedings or that I may provide to you in specific circumstances. My privacy notice for all other activities that do not relate to my activities in relation to Arbitral Proceedings can be found here. [**Link**]

Arbitral Proceedings may finally determine the rights and interests of persons (both individuals and legal entities) and must therefore be undertaken fairly and impartially, which requires me to ensure that the parties' fundamental due process rights, rights to equal treatment and their right to present their case and to be heard are protected.

My activities as an arbitrator may require me to process personal data that relates to arbitrators, mediators, adjudicators, experts and others acting or potentially acting in similar roles ("**Neutrals**"), as well as tribunal secretaries, employees of arbitral institutions, parties, their authorised representatives and legal counsel, witnesses and other individuals that may be identified or identifiable in any information that is processed during the Arbitral Proceedings.

I act as a controller of personal data for some of my activities as an arbitrator. You should be aware that others may also act as data controllers during Arbitral Proceedings in which I act as an arbitrator, for example, the parties, their authorised

representative or legal counsel, the arbitral institution and other Neutrals. When I act as an arbitrator, I am responsible for the data processing activities that I undertake in that function, but not for the activities undertaken by other data controllers acting in the context of Arbitral Proceedings, including other Neutrals. Their activities are not the subject of this Privacy Notice.

Please note that when, in the context of Arbitral Proceedings, you provide any personal data relating to individuals with whom I or the person to whom such data is submitted has no direct relationship, it is your duty to provide the individual data subject with adequate notice that their data is being processed for this purpose and to comply with your other applicable data protection obligations.

This Privacy Notice is in effect as of the date indicated at the end of this Privacy Notice. A link to this Privacy Notice is found under the signature line of my emails. If I make material changes to this Privacy Notice, I will update this Privacy Notice on my website with a changed date at: [**Link**].

If you have any questions about this Privacy Notice or how I treat your personal data in the context of Arbitral Proceedings, or if you wish to exercise any of your data subject rights, please refer to the details found at the end of this Privacy Notice.

What personal data do I collect and how do I collect it?

Depending on the circumstances, I may obtain the following personal data about you in the context of Arbitral Proceedings in which I serve as arbitrator:

Institutional Representatives

- Your name, contact details and other information you may provide to me during the appointment process or in the context of Arbitral Proceedings, including any challenge proceedings, in which I serve as an arbitrator.

Neutrals

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator;

– Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
Tribunal Secretaries
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
Individual Parties/Party's Authorised Representatives and Legal Counsel
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.
Fact and Expert Witnesses
– Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to me by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator; – Information about whether you are subject to economic sanctions or any other legal or regulatory impediment; – Personal data you choose to include in your witness statement or expert report and any oral testimony you may give (which may be transcribed), as

submitted to me during Arbitral Proceedings in which you provide written or oral evidence;
- Any other personal data of yours submitted to me by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context of Arbitral Proceedings in which I serve as an arbitrator.

Other Individuals

- Personal data of yours submitted to me by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, me from third parties or publicly available resources in the context Arbitral Proceedings in which I serve as an arbitrator.

How do I use your personal information and on what legal basis?

In the context of Arbitral Proceedings in which I serve as an arbitrator, and depending on the circumstances, I may use your personal data in the following ways and on the legal bases described below:

Other Neutrals and Tribunal Secretaries

- To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in Arbitral Proceedings, as necessary to further the parties' and my legitimate interests[4] in ensuring that only suitable candidates are appointed and that conflicts of interest do not arise that could undermine the actual or perceived integrity of the Arbitral Proceedings;
- To maintain an informal database of potential Neutrals and tribunal secretaries as necessary to further both my and potential parties' legitimate interests in identifying and appointing suitable chair persons and tribunal secretaries;
- To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of Arbitral Proceedings, as necessary for the performance of any agreement we may have entered into and my duties under them;

4. Any time legitimate interests are relied on in the EU, consideration should be given to undertaking a documented Legitimate Interests Assessment (*see* Annex 5).

– To facilitate the general conduct of Arbitral Proceedings, including to communicate with you, facilitate communications between the tribunal and the arbitral participants more broadly, and to fulfil other administrative tasks in relation to Arbitral Proceedings, as necessary for furthering the parties' and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected; – Where necessary to meet my legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering ("**Legal Compliance Obligations**").
Individual Parties/Party's Authorised Representatives and Legal Counsel
– To facilitate the general conduct of Arbitral Proceedings, including to communicate with you, facilitate communications between the tribunal and the arbitral participants, and to fulfil other administrative tasks in relation to Arbitral Proceedings, as necessary for furthering the parties' and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected; – Where we have entered into an agreement for me to provide services to you as an individual in connection with Arbitral Proceedings (for example, claims brought by individuals), I may process your personal data (only) as necessary to perform my obligations and duties under that agreement; – Where necessary to meet my Legal Compliance Obligations.
Expert and Fact Witnesses
– To facilitate your giving of evidence in Arbitral Proceedings, and the examination of such evidence, as necessary for furthering the parties' and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected; – Where necessary to meet my Legal Compliance Obligations.
Other Individuals
– As necessary for furthering the parties' and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected; – Where necessary to meet my Legal Compliance Obligations.

How do I share your personal information?

Depending on the circumstances in which I process your personal data, I may share it with the following people as necessary for furthering the parties' and my legitimate interests in resolving the dispute between them efficiently and expeditiously and ensuring that the rights of the parties are respected, or as otherwise set out below:

- Arbitral Participants and others involved in Arbitral Proceedings in which you are also involved;
- My service providers such as third-party data hosting providers in order for me to provide services in connection with Arbitral Proceedings;
- Third parties including my professional advisors, financial institutions, or law enforcement agencies, where necessary to comply with my Legal Compliance Obligations, or where it is otherwise in my or another Arbitral Participant's legitimate interests to do so.

Where do I transfer your personal data?

From time to time I transfer personal data to third countries in connection with the Arbitral Proceedings in which I serve as an arbitrator, or as may otherwise become necessary in the course of my operations. I make such transfers where there is a lawful basis for doing so.[5]

How long do I retain your personal information?

I will only keep your personal data for as long as is reasonably necessary in the circumstances. Retention periods vary depending on the category of data, taking into account legal and regulatory requirements, limitation periods for taking legal action, good practice and the lawful basis on which I process your personal data.

5. Where the GDPR applies, consideration should be given to the following language:
   If the recipient is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Union, such transfers are made in accordance with our legal obligations, including entering into the standard contractual clauses or another adequacy mechanism promulgated by the European Union where feasible and if this is not feasible, in accordance with a derogation, for example where the transfers are necessary to establish, exercise or defend legal claims, or where there is another lawful basis to do so.

What rights do you have over your personal data?

Depending on the circumstances, you may have a number of rights over the personal data that I process about you. These may include the right to:

- Request access to your personal data and obtain a copy of it from me, where this would not adversely affect the rights and freedoms of others;
- Correct your personal data that I hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for me continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defence;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defence;
- Request me to stop processing your personal data when it is being processed based on your consent;
- Object to your personal data being processed if the lawful basis for processing it is either my or a third party's legitimate interests unless there are overriding legitimate grounds for the processing;
- Require certain of your personal data to be transferred to you or a third party to the extent that I collected the data directly from you;
- Lodge a complaint with the relevant data protection authority.

If you wish to exercise any of these rights, or if you have any questions about this notice or how I treat your personal data, you can contact me:

- By email: [**TO BE ADDED**]

- By post: [**TO BE ADDED**]

Please note that if you are an employee of, nominated or engaged by, or otherwise affiliated with a party to an Arbitral Proceeding in which I am appointed as an arbitrator, I suggest that you raise your concerns with that party first before contacting me regarding the processing of your personal data in the context of Arbitral Proceedings.

Date: [**dd mm year**]

ANNEX 9C
Data Privacy Notice for Legal Counsel

SAMPLE ONLY

SAMPLE DATA PRIVACY NOTICE FOR LEGAL COUNSEL

Last Updated: [●]

Purpose of this Privacy Notice

[Name of Legal Counsel or the law firm] [**"I", "me," "we" or the firm]** act(s) as a legal counsel and [**carry/carries**] out other activities in relation to disputes or potential disputes that are submitted to arbitration and other dispute resolution mechanisms, both during their pendency and after their conclusion. ("**Dispute Resolution Proceedings**")

This Privacy Notice describes how [**I/we/the firm**] collect and process personal data in the context of those services and activities. [**My/ the firm's**] General Privacy Notice can be found here. [**Link**]

Dispute Resolution Proceedings may finally determine the rights and interests of persons (both individuals and legal entities) and must therefore be undertaken fairly and impartially, which requires that the parties' fundamental due process rights, rights to equal treatment and their right to present their case and to be heard are protected.

[**My/The firm's**] activities as a legal counsel during Dispute Resolution Proceedings may require **[me/us/the firm]** to process personal data that relates to arbitrators, mediators, adjudicators, experts, and others acting or potentially acting in similar roles ("**Neutrals**"), as well as tribunal secretaries, employees of arbitral institutions, parties, their authorised and legal counsel, witnesses, and other individuals that may be identified or identifiable in any information that is processed during the Dispute Resolution Proceedings.

[**I/we/the firm**] acts as a controller of personal data for some of [**my/our**] activities as legal counsel. You should be aware that others may also act as data controllers during a Dispute Resolution Proceeding, for example, the parties, their authorised representatives, other legal counsel, the arbitral institution, and Neutrals. When I act

as a legal counsel, I am responsible for the data processing activities that I undertake in that function, but not for the activities undertaken by other data controllers acting in the context of Dispute Resolution Proceedings. Their activities are not the subject of this Privacy Notice.

Please note that when, in the context of Dispute Resolution Proceedings, you provide me with any personal data relating to individuals with whom I have no direct relationship, it is your duty to provide the individual data subject with adequate notice that their data is being processed for this purpose and to comply with your other applicable data protection obligations.

This Privacy Notice is in effect as of the date indicated at the end of this Privacy Notice. A link to the Privacy Notice is found under the signature line of [**my/our/the firm's**] emails. If [**I/we**] make material changes to this Privacy Notice, [**I/we**] will update this Privacy Notice on the website with a changed date at: [**Link**].

If you have any questions about this Privacy Notice, or how [**I/we/the firm**] treat your personal data in the context of Dispute Resolution Proceedings or wish to exercise any of your data subject rights, please refer to the details found at the end of this Privacy Notice.

What personal data do I collect and how do I collect it?

Depending on the circumstances, [**I/we/the firm**] may obtain the following personal data about you in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act as a legal counsel:

Institutional Representatives

- Your name, contact details, and other information you may provide to [**me/us/the firm**] in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act[**s**] as legal counsel.

Neutrals

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [**me/us/the firm**] by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [**me/us/the firm**] from third parties or publicly available resources

in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act[**s**] as legal counsel;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Tribunal Secretaries

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [**me/us/the firm**] by you, a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, a representative of the institution, or otherwise disclosed to, or collected by [**me/us/the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act[**s**] as legal counsel;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Individual Parties/Party's Authorised and Legal Counsels

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [**me/us/the firm**] by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [**me/us/the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act as a legal counsel;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment.

Fact and Expert Witnesses

- Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to [**me/us/the firm**] by you, a party, a party's authorised representative or legal counsel, another Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [**me/us/the firm**] from third parties or publicly available

resources in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act as a legal counsel;
- Information about whether you are subject to economic sanctions or any other legal or regulatory impediment;
- Personal data you choose to include in your witness statement or expert report and any oral testimony you may give (which may be transcribed), as submitted to [**me/us/the firm**] during Dispute Resolution Proceedings in which you provide written or oral evidence;
- Any other personal data of yours submitted to [**me/us/the firm**] by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [**me/us/the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act as a legal counsel.

Other Individuals

- Personal data of yours submitted to [**me/us/the firm**] by a party, a party's authorised representative or legal counsel, a Neutral, a tribunal secretary, or a representative of the institution, or that is otherwise disclosed to, or collected by, [**me/us/the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act as a legal counsel.

How do [I/we/the firm] use your personal information and on what legal basis?

In the context of Dispute Resolution Proceedings in which [**I/we/the firm**] act as a legal counsel, depending on the circumstances, [**I/we/the firm**] may use your personal data in the following ways and on the legal bases described below:

Neutrals and Tribunal Secretaries

- To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in Dispute Resolution Proceedings, as necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;[6]

6. Any time legitimate interests are relied on in the EU, relevant EU guidance suggests that consideration should be given to undertaking a documented Legitimate Interests Assessment (*see*

- To maintain an informal database of potential Neutrals and tribunal secretaries as necessary to further [**my/our/the firm's**] and potential parties' legitimate interests in identifying and appointing suitable Neutrals and tribunal secretaries;
- To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of Dispute Resolution Proceedings, as necessary for the performance of any agreement we may have entered into and [**my/our/the firm's**] duties under it;
- To facilitate the general conduct of Dispute Resolution Proceedings, as necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;
- Where necessary to meet [**my/our/the firm's**] legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering ("**Legal Compliance Obligations**").

Legal Counsel of Other Parties

- To facilitate the general conduct of Dispute Resolution Proceedings, as necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;
- Where we have entered into an agreement for me to provide services to you as an individual in connection with Dispute Resolution Proceedings (for example, claims brought by individuals), [**I/we/the firm**] may process your personal data (only) as necessary to perform [**my/our/the firm's**] obligations and duties under that agreement;
- Where necessary to meet [**my/our/the firm's**] Legal Compliance Obligations.

Expert and Fact Witnesses

- To facilitate your giving evidence in Dispute Resolution Proceedings and the examination of such evidence, as necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;
- Where necessary to meet [**my/our/the firm's**] Legal Compliance Obligations.

Annex 5).

Other Individuals

- As necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;
- Where necessary to meet [**my/our/the firm's**] Legal Compliance Obligations.

How do share your personal information?

Depending on the circumstances in which [**I/we/the firm**] process your personal data, [**I/we/the firm**] may share it with the following people, as necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected:

- Participants involved in Dispute Resolution Proceedings in which our client is also involved;
- [**My/Our/The firm's**] service providers such as third-party data hosting providers in order for **[me/us/the firm]** to provide services in connection with Dispute Resolution Proceedings;
- Third parties, including my colleagues, professional advisors, financial institutions, or law enforcement agencies, where necessary to perform conflict checks, to comply with [**my/our/the firm's**] Legal Compliance Obligations, or where it is otherwise in [**my/our/the firm's**] or another Arbitral Participant's or third party's legitimate interests to do so.

Where do I transfer your personal data?

From time to time [**I/we/the firm**] transfer personal data to third countries in connection with the services [**I/we/the firm**] perform for the Dispute Resolution Proceedings in which [**I/we/the firm**] serve as a legal counsel, or as may otherwise become necessary in the course of [**my/our/the firm's**] operations. [**I/we/the firm**] make such transfers where there is a lawful basis for doing so.[7]

7. Where the GDPR applies, consideration should consider the following language:
   If the recipient is not based in a jurisdiction providing an adequate level of protection for personal data as determined by the European Union, such transfers are made in accordance with our legal obligations, including entering into the standard contractual clauses or another adequacy mechanism promulgated by the European Union where feasible and if this is not feasible, in accordance with a derogation, for example where the transfers are necessary to establish, exercise or defend legal claims, or where there is another lawful basis to do so.

How long do [I/we/the firm] retain your personal information?

[**I/we/the firm**] will only keep your personal data for as long as is reasonably necessary in the circumstances. Retention periods vary depending on the category of data, taking into account legal and regulatory requirements, limitation periods for taking legal action, good practice and the lawful basis on which [**I/we/the firm**] process it.

What rights do you have over your personal data?

Depending on the circumstances, you may have a number of rights over the personal data that [**I/we/the firm**] process about you. These may include the right to:

- Request access to your personal data and obtain a copy of it from **[me/us/the firm]**, where this would not adversely affect the rights and freedoms of others;
- Correct your personal data that [**I/we/the firm**] hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for [**me/us/the firm**] continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defence;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defence;
- Request [**me/us/the firm**] to stop processing your personal data when it is being processed based on your consent;
- Object to your personal data being processed if the lawful basis for processing it is either [**my/our/the firm's**] or a third party's legitimate interests unless there are overriding legitimate grounds for the processing;
- Require certain of your personal data to be transferred to you or a third party to the extent that [**I/we/the firm**] collected the data directly from you; and
- Lodge a complaint with the relevant data protection authority.

If you wish to exercise any of these rights, or if you have any questions about this notice or how [**I/we/the firm**] treat your personal data, you can contact [**me/us/the firm**] as follows:

- By email: [**TO BE ADDED**]

- By post: [**TO BE ADDED**]

Please note that if you are an employee of, nominated or engaged by, or otherwise affiliated with a party to an Dispute Resolution Proceeding in which [**I/we/the firm**]

act as a legal counsel, [**I/we/the firm**] suggest that you raise your concerns with that party first before contacting [**me/us/the firm**] regarding the processing of your personal data in the context of Dispute Resolution Proceedings.

Date: [**dd mm year**]

ANNEX 10
List of Sources by Category

Data Protection Related Materials

Application of Data Protection Directive to Discovery

1. *Working Document on Pre-trial Discovery for Cross Border Civil Litigation,* EU Working Party, 00339/09/EN WP 158, 2009 (endorsed by the EPDB) (referred to as "**Document Disclosure Guidance**")

2. *The Sedona Conference: International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition),* App. D: Cross-Border Data Safeguarding Process + Transfer Protocol, Sedona Conference Working Group (2017)

3. *E-Discovery and Data Privacy: A Practical Guide,* Catrien Noorda & Stefan Hanlose eds., 2011

Consent

4. *Guidelines on Consent under Regulation 2016/679,* EU Working Party, 17/EN WP259 rev.01, as revised and adopted on 10 April 2018 (endorsed by the EPDB)

Controller versus Processor

5. *Opinion 1/2010 on the Concepts of "Controller" and "Processor",* EU Working Party, 00264/10/EN WP 169, 2010 (**"Controller/Processor Opinion"**)

Data Breach

6. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification,* EU Working Party, Version 2.0, adopted on 14 December 2021

7. *Guidelines on Personal data breach notification under Regulation 2016/679*, endorsed by the EDPB, G29 WP250 rev.1, 6 February 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Data Processing

8. *What Constitutes Data Processing?,* European Commission, https://ec.europa. eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [https://perma.cc/Q85B-NJ33] (archived 19 March 2018)

Data Transfers

9. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR,* EDPB, Version for Public Comment, 18 November 2021

10. *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* (Text with EEA relevance) C/2021/3972 OJ L 199, 7.6.2021, p. 31–61. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en (referred to as "**standard contractual clauses**")

11. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679,* EDPB, 2018 (referred to as "**Data Transfer Guidance**")

12. *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, EU Working Party, 2093/05/EN WP 114, 2005

13. *Adequacy of the protection of personal data in non-EU countries*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

General Materials

14. Daniel Cooper and Christopher Kuner, *Data Protection Law and International Dispute Resolution*, 32 Recueil des cours/ Collected Courses of the Hague Academy of International Law 9-174 (2017)

15. *Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulations as of 25 May 2018*, Communication from the Commission to the European Parliament and the Council, COM (2018) 43 (24 January 2018)

16. *Handbook on European Data Protection Law*, European Union Agency for *Fundamental* Rights (2018)

Joint Controller

17. Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* C210/16, EU:C:2018:388

18. Judgment of 10 July 2018, *Tietosuojavaltuutettu*, C25/17, EU:C:2018:551 Case C-25/17

19. *CJEU rules on joint controllership – what does this mean for companies?*, https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies (August 2018)

Legitimate Interests

20. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, EU Working Party, 844/14/EN, WP 217, 9 April 2014

21. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, EDPB, 8 October 2019

Lead Supervisory Authority

22. *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority,* EU Working Party, 16/EN WP 244 rev. 01, 2017

Personal Data

23. *What is Personal Data?*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/CJ52-ZQVB] (archived 31 May 2018)

Proportionality

24. *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (19 December 2019)

Risk-Based Approach

25. *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks 3,* EU Working Party, 14/EN 218 WP 169, 2014

Territorial Scope

26. *Guidelines 3/2018 on the Territorial Scope of the GDPR*, EDPB, 12 November 2019

Transparency

27. *Guidelines on Transparency under Regulation 2016/679,* EU Working Party, 17/EN WP 260, 2018

Arbitration-related Data Protection Materials

28. *Protocol for Online Case Management in International Arbitration,* Working Group on LegalTech Adoption in International Arbitration (2020) (referred to as "**Online Platform Protocol**")

29. *Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration,* International Chamber of Commerce (1 January 2021)

30. *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration,* Kathleen Paisley, 41 Fordham Int'l L.J. 840 (2017)

31. *IBA Rules on the Taking of Evidence in International Arbitration* (International Bar Association, revised in 2020) (referred to as "**IBA Rules**")

32. *Commentary on the Revised Text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration* (2020)

Cybersecurity Materials

33. *ICCA/NYC Bar/CPR Cybersecurity Protocol for International Arbitratio*n (2022 Edition) (referred to as "**Cybersecurity Protocol**")

34. *Cybersecurity Guidelines,* IBA Presidential Task Force on Cybersecurity (2018)

35. *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion,* Stephanie Cohen and Mark Morril, 40 Fordham Int'l L.J. 981 (2017)

36. *Debevoise & Plimpton Protocol to Promote Cybersecurity in International Arbitration* https://www.debevoise.com/~/media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf. (2017)

Applicable Law to Data Protection

37. *Cross-Border Application of EU's General Data Protection Regulation (GDPR)- A private international law study on third state implications,* Anni-Maria Taka (2017)

38. *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation,* Jiahong Chen, International Data Privacy Law 6.4 (2016): 310-323.

39. *Data protection and conflict-of-laws: a challenging relationship,* Maja Brkan, Eur. Data Prot. L. Rev. 2 (2016): 324

40. *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union,* Christian Kohler, Rivista di diritto internazionale privato e processuale (2016): 653

41. *Protection of Privacy in Private International and Procedural Law: Interim Report and Commentary*, International Law Association Sydney Conference (2018)

ANNEX 11
Compendium of Selected Data Protection Laws

The Task Force has compiled this compendium from publicly available sources and has undertaken reasonable efforts to ensure that it is current as of the date of publication of the Roadmap. It should not be relied on without independent confirmation of the current law.

Jurisdictions with EU Adequacy Decisions

No.	Country	Supervisory Authority	Implementing Legislation	Adequacy Decision
1	**Andorra**	l'Agència Andorrana de Protecció de Dades (APDA) https://www.apda.ad/	Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades (LQPD)	Commission Decision 2010/625/EU
2	**Argentina**	Agencia de Accesso a la Información Pública https://www.argentina.gob.ar/aaip	Ley de Protección de Datos Personales 25.326	Commission Decision 2003/490/EC
3	**Canada (commercial organisations)**	Office of the Privacy Commissioner of Canada ("PIPEDA") Office of the Information and Privacy Commissioner of Alberta ("PIPA Alberta") Office of the Information and Privacy Commissioner for British Columbia ("PIPA BC"), and Commission d'accès à l'information du Québec ("Quebec Privacy Act")	In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Canada's private sector privacy statutes: Personal Information Protection and Electronic Documents Act ("PIPEDA") Personal Information Protection Act ("PIPA Alberta") Personal Information Protection Act ("PIPA BC"), Personal Information Protection and Indentity Theft Prevention Act ("PIPITPA") (not yet in force), and An Act Respecting the Protection of Personal Information in the Private Sector ("Quebec Privacy Act")	Commission Decision 2002/2/EC
4	**Faroe Islands**			Commission Decision 2010/146/EU

No.	Country	Supervisory Authority	Implementing Legislation	Adequacy Decision
5	**Guernsey**	Data Protection Authority Office of the Data Protection Authority	Data Protection (Bailiwick of Guernsey) Law 2017 (DPL 2017) (came into force on 25 May 2018 to coincide with the GDPR)	Commission Decision 2003/821/EC
6	**Israel**	The Israel Privacy Protection Authority (PPA)	Human Dignity and Liberty, 5752 – 1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the PPL); and the guidelines of the Israel Privacy Protection Authority.	Commission Decision 2011/61/EU
7	**Isle of Man**			Commission Decision 2004/411/EC
8	**Japan**	Personal Information Protection Commission	Act on the Protection of Personal Information, as amended on 30 May 2017	EU Japan Adequacy Decision, January 2019
9	**Jersey**	Data Protection Authority Information Commissioner	Data Protection (Jersey) Law, 2018 (DPJL) and the Data Protection Authority (Jersey) Law, 2018 (DPAJL) came into force on May 25, 2018. These laws superseded the Data Protection (Jersey) Law 2005, which had been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC). This decision continues to apply pending a review of Jersey's adequacy (to be conducted under Article 45 of the European General Data Protection Regulation (GDPR)), which is expected to take place in 2020. The DPJL and DPAJL provide a broadly equivalent regime to that under the GDPR.	Commission Decision 2008/393/EC

No.	Country	Supervisory Authority	Implementing Legislation	Adequacy Decision
10	**New Zealand**	Privacy Commissioner's Office	The Privacy Act 1993 (Act) A Privacy Amendment Bill was introduced to New Zealand's parliament in 2018	Commission Implementing Decision 2013/65/EU
11	**Republic of Korea**	Personal Information Protection Commission (PIPC)	Personal Information Protection Act (PIPA), as amended on 4 February 2020	Commission Implementing Decision of 17.12.2021
12	**Switzerland**	Federal Data Protection and Information Commissioner (FDPIC)	*See below (subject to a new decision on adequacy in view of regulatory changes since 2000)*	Commission Decision 2000/518/EC
13	**Uruguay**	Unidad Reguladora y de Control de Datos Personales (URCDP or Data Protection Authority) https://www.gub.uy/unidad-reguladora-control-datos-personales/	Data Protection Act Law No. 18.331 (August 11, 2008) Decree No. 414/009 (August 31, 2009)	Commission Implementing Decision 2012/484/EU
14	**United Kingdom**	Information Commissioner's Office https://ico.org.uk/	Data Protection Act 2018	Commission Implementing Decision of 28.6.2021

Selected Data Protection Laws of Non-EEA Jurisdictions

	Country	Supervising Authority(ies)	National Law(s)
1	**Brazil**	National Data Protection Authority (ANPD) https://www.gov.br/anpd/pt-br	Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018, published on August 15, 2018. Largely aligned to the EU General Data Protection Act (GDPR)
2	**Canada**	Office of the Privacy Commissioner of Canada ("PIPEDA") Office of the Information and Privacy Commissioner of Alberta ("PIPA Alberta") Office of the Information and Privacy Commissioner for British Columbia ("PIPA BC"), and Commission d'accès à l'information du Québec ("Quebec Privacy Act")	In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Canada's private sector privacy statutes: Personal Information Protection and Electronic Documents Act ("PIPEDA") Personal Information Protection Act ("PIPA Alberta") Personal Information Protection Act ("PIPA BC"), Personal Information Protection and Identity Theft Prevention Act ("PIPITPA") (not yet in force), and An Act Respecting the Protection of Personal Information in the Private Sector ("Quebec Privacy Act")
3	**China**	Cyberspace Administration of China (CAC) Ministry of Public Security	There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal data protection and data security are part of a complex framework and are found across various laws and regulations. PRC Cybersecurity Law came into effect on June 1, 2017 and became the first national-level law to address cybersecurity and data privacy protection. However, there remains uncertainty as to how it will be applied.
4	**Hong Kong**	The Office of the Privacy Commissioner for Personal Data	The Personal Data (Privacy) Ordinance (Cap. 486) – in force since 1996, significantly amended in 2012/2013
5	**India**	[No authority]	Personal Data Protection Bill 2018 – [withdrawn] Information Technology Act, 2000 India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011

	Country	Supervising Authority(ies)	National Law(s)
6	**Mexico**	National Institute of Transparency for Access to Information and Personal Data Protection Ministry of Economy	Federal Law on the Protection of Personal Data held by Private Parties (July 6, 2010), supplemented by further regulations: The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (December 22, 2011) The Privacy Notice Guidelines (April 18, 2013) The Recommendations on Personal Data Security (November 30, 2013) The Parameters for Self-Regulation regarding personal data (May 30, 2014) The General Law for the Protection of Personal Data in Possession of Obligated Subjects (January 27, 2017)
7	**Russia**	Federal Service for Supervision of Communications, Information Technologies and Mass Media ("Roscomnadzor")	Russian Constitution establishes the right to privacy of each individual (arts. 23-24) Data Protection Act No. 152 FZ dated 27 July 2006 (DPA), amended on 22 July 2014
8	**Singapore**	Personal Data Protection Commission	Personal Data Protection Act No. 26 of 2012, enacted on October 15, 2012
9	**Switzerland**	Federal Data Protection and Information Commissioner (FDPIC)	Federal Act on Data Protection of June 19, 1992 (DPA), together with Ordinance to the Federal Act on Data Protection (DPO) and the Ordinance on Data Protection Certification (ODPC). After substantial revision, a new Federal Act on Data Protection was adopted on September 25, 2020 and should come into force on September 1, 2023 (the new Act aims to align the DPA with the GDPR).
10	**United Kingdom**	Information Commissioner's Office https://ico.org.uk/	Data Protection Act 2018
11	**USA**[1]	No single national authority The Federal Trade Commission has authority to issue and enforce privacy regulations in specific areas	

1. The list of states with data protection frameworks is not exhaustive. We refer to a select few, deemed especially relevant in arbitration.

	Country	Supervising Authority(ies)	National Law(s)
12	California		More than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020 and the California Privacy Rights Act (CPRA) – the majority of the CPRA's provisions will enter into force on Jan. 1, 2023
13	Florida		Fl Stat § 282.318 Information Technology Security Act Fl Stat § 408.051 Florida Electronic Health Records Exchange Act Fl Stat § 501.171 Security of Confidential Personal Information
14	New York		Ny Gen. Bus. Law § 899-Aa *Notification; Person Without Valid Authorization Has Acquired Private Information* Ny Gen. Bus. Law §§ 899-Aaa – 899-Bbb *Document Destruction Contractors* Ny Gen. Bus. Law § 399-Ddd *Confidentiality of Social Security Account Number* Ny Gen. Bus. Laws § 399-Ddd*2 *Disclosure of Social Security Number* Ny Gen. Bus. Law § 399-H *Disposal of Records Containing Personal Identifying Information* 23 Nycrr 500 §§ 500.00 – 500.23 *Cybersecurity Requirements for Financial Services Companies*
15	Texas		Tx Business and Commerce Code §§ 521.001 – 521.002 *Identity Theft Enforcement and Protection Act* Tx Business and Commerce Code § 521.051 *Unauthorized Use or Possession of Personal Identifying Information* Tx Business and Commerce Code § 521.052 *Business Duty to Protect Sensitive Personal Information* Tx Business and Commerce Code § 521.053 *Notification Required Following Breach of Security of Computerized Data* Tx Business and Commerce Code § 521.151 *Civil Penalty; Injunction* Tx Business and Commerce Code §§ 72.001 – 72.004 *Disposal of Certain Business Records*

	Country	Supervising Authority(ies)	National Law(s)
16	Washington DC		D.C. Code §§ 28-3851 – 3853 Consumer Security Breach Notification D.C. Code §§ 47-3151 – 3154 Use of Consumer Identification Information D.C. Code §§ 38-831.01 – 38-831.06 Protection of Students Digital Privacy D.C. Code §§ 7-241 – 7-248 Human Health Care and Safety/Data Sharing D.C. Code § 38-607 Student Health Files

EU/EEA Member State Data Protection Laws

	Country	Supervising Authority	Implementing Law(s)
1	**Austria**	**Österreichische Datenschutzbehörde** http://www.dsb.gv.at/	Federal Act Amending the Data Protection Act 2000 (Data Protection Adaptation Act) 2018 Federal Law 23 Federal Law 24
2	**Belgium**	Autorité de la protection des données)/ Gegevensbeschermingsautoriteit **(APD-GBA)** https://www.autoriteprotectiondonnees.be/ https://www.gegevensbeschermingsauto-riteit.be/	Law of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data Law of 3 December 2017 establishing the Data Protection Authority
3	**Bulgaria**	Commission for Personal Data Protection https://www.cpdp.bg/	Personal Data Protection Act
4	**Croatia**	Croatian Personal Data Protection Agency http://www.azop.hr/	Law on Implementation of the General Data Protection Agreement
5	**Cyprus**	Office of the Commissioner for Personal Data Protection http://www.dataprotection.gov.cy/	Law Providing Protection of Natural Persons against the Processing of Personal Data and the Free Movement of this Data

	Country	Supervising Authority	Implementing Law(s)
6	**Czech Republic**[2]	Office for Personal Data Protection http://www.uoou.cz/	Act No. 110/2019 Coll., on processing of personal data
7	**Denmark**	Datatilsynet http://www.datatilsynet.dk/	Law No. 502 of 23 May 2018 on Supplementary Provisions to the Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Exchange of Such Information (Data Protection Act) https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf
8	**Estonia**	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) http://www.aki.ee/	Personal Data Protection Act 616 SE
9	**Finland**	Office of the Data Protection Ombudsman http://www.tietosuoja.fi/en/	Data Protection Act (Fi: Tietosuojalaki, 1050/2018)
10	**France**	Commission Nationale de l'Informatique et des Libertés – CNIL http://www.cnil.fr/	Law No. 78-17 dated 6 January 1978 on information technology, files and freedoms, as amended by: - Law No. 2018-493 dated 20 June 2018 on the protection of personal data; and - Ordinance No. 2018-1125 dated 12 December 2018 implementing Article 32 of Law No. 2018-493. - Law No. 78-17 has been implemented by Decree No. 2005-1309 dated 20 October 2005 as amended by Decree No. 2018-687 dated 1 August 2018 - Law No. 78-17 is implemented by Decree No. 2019-536 dated 29 May 2019

2. In the Czech Republic, Act No. 216/1994 Coll., on Arbitration and Enforcement of Arbitral Awards, governs the conditions under which the state delegates its jurisdiction to private subjects – the arbitrators – the substantive and procedural framework of arbitration with regard to both *ad hoc* arbitrators and permanent arbitration courts as well as conditions under which the latter category can be established. Unlike in other Member States of the European Union, permanent arbitration courts in the Czech Republic can only be established by special legal act, or only if their establishment is expressly permitted by such special legal act..

	Country	Supervising Authority	Implementing Law(s)
11	**Germany – Federal**	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit https://www.bfdi.bund.de/DE/Home/home_node.html	German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680
	Baden-Württemberg	Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg https://www.baden-wuerttemberg.datenschutz.de/	Act to Adapt Data Protection Law to Regulation (EU) 2016/679 (Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679) dated 12 June 2018
	Bavaria	Bavarian Data Protection Commissioner https://www.datenschutz-bayern.de/	Bavarian Data Protection Act (Bayerisches Datenschutzgesetz) dated 15 May 2018
	Berlin	Berliner Beauftragte für Datenschutz und Informationsfreiheit https://www.datenschutz-berlin.de/	Berlin Data Protection Act (Berliner Datenschutzgesetz) dated 13 June 2018
	Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg https://www.lda.brandenburg.de/cms/detail.php?gsid=bb1.c.233960.de	Brandenburg Data Protection Act (Brandenburgisches Datenschutzgesetz) dated 8 May 2018 [German]
	Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit https://www.datenschutz.bremen.de/	Bremen Act on implementation of the General Data Protection Regulation (Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung) dated 8 May 2018
	Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz-hamburg.de/	Hamburg Data Protection Act (Hamburgisches Datenschutzgesetz) dated 18 May 2018
	Hesse	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz.hessen.de//	Hessian Data Protection Act and Freedom of Information Act (Hessisches Datenschutz- und Informationsfreiheitsgesetz) dated 3 May 2018

	Country	Supervising Authority	Implementing Law(s)
	Mecklen-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklen-Vorpommern https://www.datenschutz-mv.de/	Law on the Adaptation of the State Data Protection Act and other data protection regulations within the area of responsibility of the Ministry of the Interior and Europe Mecklenburg-Vorpommern to the Regulation (EU) 2016/679 and the implementation of the Direction (EU) 2016/680 (Gesetz zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 22 May 2018 (Gesetz zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 22 May 2018
	Lower Saxony	Die Landesbeauftragte für den Datenschutz Niedersachsen https://www.lfd.niedersachsen.de/startseite/	Lower Saxony Data Protection Act (Niedersächsisches Datenschutzgesetzs) dated 16 May 2018
	North Rhine-Westphalia	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen https://www.ldi.nrw.de/	North Rhine Westphalia Data Protection Act (Datenschutzgesetz Nordrhein-Westfalen) dated 17 May 2018 (Datenschutzgesetz Nordrhein-Westfalen) dated 17 May 2018
	Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz https://www.datenschutz.rlp.de/de/startseite/	State Data Protection Law (Landesdatenschutzgesetz) dated 8 May 2018
	Saarland	Unabhängiges Datenschutz Zentrum Saarland https://datenschutz.saarland.de/	Saarland Data Protection Act (Saarländisches Datenschutzgeset) dated 16 May 2018
	Saxony	Sächsischer Datenschutzbeauftragter https://www.saechsdsb.de/	Saxony Data Protection Act (Sächsisches Datenschutzgesetz) dated 25 August 2003 (last amended on 22 August 2019)

	Country	Supervising Authority	Implementing Law(s)
	Saxony-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt https://datenschutz.sachsen-anhalt.de/nc/datenschutz-sachsen-anhalt/	Saxony-Anhalt General Data Protection Regulation Implementation Act (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt) dated 18 February 2020 Saxony-Anhalt Data Protection Directive Implementation Act (Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt) dated 2 August 2019
	Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz https://www.datenschutzzentrum.de/	State Data Protection Law (Landesdatenschutzgesetz) dated 2 May 2018
	Thuringia	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit https://www.tlfdi.de/	Thuringia Data Protection Act (Thüringer Datenschutzgesetz) dated 6 June 2018 [German]
12	**Greece**	Hellenic Data Protection Authority http://www.dpa.gr/	Law No. 4624/2019
13	**Hungary**	Hungarian National Authority for Data Protection and Freedom of Information http://www.naih.hu/	Act on the Right to Information Self-Determination and Freedom of Information 2011 CXII. law for legal harmonisation
14	**Iceland**	Persónuvernd https://www.personuvernd.is/	Law no. 90/2018 on personal protection and processing of personal information
15	**Ireland**	Irish Data Protection Commission https://www.dataprotection.ie/	Data Protection Act 2018
16	**Italy**	Garante per la protezione dei dati personali (“**Garante Privacy**”) https://www.garanteprivacy.it/	Provisions for the adaptation of national legislation to the provisions of the GDPR, in particular Legislative Decree No. 101 of 10 August 2018, which amended the “Privacy Code” (Legislative Decree No. 196 of 30 June 2003)
17	**Latvia**	Data State Inspectorate http://www.dvi.gov.lv/lv/	Personal Data Processing Law

	Country	Supervising Authority	Implementing Law(s)
18	**Liechtenstein**	Data Protection Office, Principality of Liechtenstein https://www.datenschutzstelle.li	Liechtenstein Data Protection Law, 4 October 2018
19	**Lithuania**	State Data Protection Inspectorate https://www.ada.lt/	Law on the Protection of Personal Data
20	**Luxembourg**	Commission Nationale pour la protection des données http://www.cnpd.lu/	Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the General Scheme on Data Protection
21	**Malta**	Office of the Information and Data Protection Commissioner https://idpc.org.mt/en/Pages/Home.aspx	Data Protection Act (CAP 586) Other Subsidiary Legislation, including: Subsidiary Legislation 586.09 Restrictions of the Data Protection (Obligations and Rights) Regulations
22	**The Netherlands**	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/nl	Law Implementing the General Data Protection Regulation
23	**Norway**	Datatilsynet www.datatilsynet.no	The Personal Data Act
24	**Poland**	Personal Data Protection Office (Urząd Ochrony Danych Osobowych) https://uodo.gov.pl/	Act of 10 May 2018 on the Protection of Personal Data Act of 26 May 1982, Law on Advocates (Polish: Prawo o adwokaturze) Act of 6 July 1982 on Attorneys-at-law (Polish: Ustawa o radcach prawnych)
25	**Portugal**	Comissão Nacional de Protecção de Dados – CNPD https://www.cnpd.pt/	Law no. 58/2019 of 8 August 2019

	Country	Supervising Authority	Implementing Law(s)
26	**Romania**	The National Supervisory Authority for Personal Data Processing http://www.dataprotection.ro/	Law 190/2018 on measures to implement regulations of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the EU Directive 95/46 https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf [unofficial translation] Law 129/2018 amending Law 102/2005 on the creation, organization and functioning of the National Supervisory Authority for Personal Data Processing, and repealing Law 677/2001 for the protection of individuals regarding personal data processing and the free circulation of such data
27	**Slovakia**	Office for Personal Data Protection of the Slovak Republic http://www.dataprotection.gov.sk/	Act No. 18/2018 Coll., on Protection of Personal Data and on Changing and Amending of Other Acts (the "*Slovak Data Protection Act*")
28	**Slovenia**	Information Commissioner of the Republic of Slovenia https://www.ip-rs.si/	[legislation implementing the GDPR in draft]
29	**Spain**	Agencia Española de Protección de Datos (AEPD) https://www.aepd.es/es	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
30	**Sweden**	Datainspektionen http://www.datainspektionen.se/	Law (2018:218) with additional provisions to the EU Data Protection Ordinance Regulation (2018: 219) with additional provisions to the EU Data Protection Ordinance

Roadmap to Data Protection in International Arbitration

Data protection laws prescribe the rules applicable to personal data processing, including when, where and how personal data may be processed. However, they do not address how they should be applied in specific contexts, including arbitration. This ICCA-IBA Roadmap to Data Protection in International Arbitration ("Roadmap") has therefore been developed by the ICCA-IBA Task Force as a tool to assist arbitration professionals in understanding how the data protection laws may apply during international arbitration proceedings.

When an arbitral participant is subject to a data protection law, compliance is legally required. As a result, data protection principles will need to be applied to supplement the applicable laws, arbitration rules, and soft law instruments (including the IBA Rules). By reference to general data protection principles, the Roadmap aims to assist arbitral participants in identifying and addressing data protection issues, and proposes that arbitration proceedings benefit when data protection compliance is addressed early in the process and a reasonable, cooperative, and proportionate approach is adopted and documented. The Annexes provide practical guidance in the form of practice tips, check lists, references, and sample text for data protection directions/protocols, standard contractual clauses, and privacy notices.

The ICCA Reports No. 7

www.arbitration-icca.org www.ibanet.org