ICCA
INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION

The ICCA–IBA Roadmap to Data Protection in International Arbitration

Public Consultation Draft
February 2020 – Not for Citation

Annexes

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

The ICCA Reports No. 7

TABLE OF CONTENTS

GENERAL ANNEXES

ANNEX 1

Glossary[1]

A

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

- **'Annexes'** refers to the present set of annexes to the Roadmap.

- **'Arbitral Participants'** is used in this Roadmap to refer to parties, their legal counsel, the arbitral institutions and the arbitrators (only). However, data protection principles also apply to those who work for them (or with them) during an arbitration, including tribunal secretaries, experts, vendors and service providers (such as e-discovery experts, information technology professionals, court reporters, translation services, etc.).

C

- **'California Consumer Privacy Act' or 'CCPA'** designates 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 he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (GDPR Art. 4(11)).

- **'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)).

- **'culling'** means filtering data.

[1] The glossary refers mainly to the GDPR. However, throughout the text of the Roadmap references are provided to similar concepts used in other modern data protection laws.

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 reveal information about his or her health status (GDPR Art. 4(15)).

- **'data minimisation'** is a principle established by the GDPR 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 his or her personal data is being processed and the purpose of the processing. The notice must comply with the requirements set out in GDPR Arts. 12-14 of the GDPR.

- **'Data Protection Directive'** designates 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 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.

- **'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 very 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 Rec. 22).

- **'European Data Protection Board' or 'EDPB'** designates the entity that has replaced the EU Working Party under the GDPR (*see* 'EU Working Party'). It is empowered to issue guidelines, recommendations and best practices to encourage consistent application of the GDPR and the setting of administrative fines.

- **'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.

- **'European Union' or 'EU'** designates 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. Moreover, although the UK is no longer a member of the EU or EEA, the rules described herein apply in the UK during a yet to be defined withdrawal period lasting until at least 31 December 2020.

- **'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.

F

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

G

- **'General Data Protection Regulation' or 'GDPR'** designates 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

- **'Indian Act'** designates the India Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011.

- **'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).

L

- '**lawful basis**' refers to one of the six possible lawful bases, one of which must apply whenever processing personal data (Article 6 GDPR).

- **'legitimate interests'** of 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); GDPR-Specific Annex 6). The GDPR does not define what constitutes "legitimate" interests and a wide range of interests may be legitimate interests. It could be the data controller's legitimate interests in the processing or it could include the legitimate interests of any third party. When legitimate interests are relied upon as a basis for processing, a legitimate interest assessment should be undertaken. (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'** designates the Brazilian General Data Protection Act (Statute 13709/18).

P

- **'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)).

- **'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)).

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

- **'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, 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'** designates 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 is some cases by a supervisory authority), which if entered into allow data to be transferred outside the EU in the absence of an adequacy decision (GDPR Art. 46).

- **'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 authorized to process personal data (GDPR Art. 4(10) GDPR).

- **'transfer out'** means any transfer – no matter the size, format, means of transmission or frequency – of personal data to countries outside the EEA (European Economic Area).

ANNEX 2

Overview of Data Protection Principles and Practice Tips in International Arbitration

Practice Tips

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

2. **Lawful Basis -** Arbitral Participants should identify and document at the outset of proceedings what data will need to be processed for the arbitration and the lawful basis that will be relied upon for the processing of any personal data, sensitive data or data related to children, and further how any data relating to criminal convictions, offences or related security measures can be processed. Some data protection laws have established a specific legal basis for data processing of personal data and/or sensitive data for arbitration. This is the case in Brazil, and for sensitive data under the GDPR, where there is a legal basis in the context of making or defending legal claims, which is likely to apply to arbitration. In other cases, where a legitimate interest is relied upon as a lawful basis for the processing of personal data, a legitimate interests assessment should be undertaken (as is the case for personal data under the GDPR). **[Annex 5].** Reliance on consent should be avoided altogether when another lawful basis is available, but may be required in jurisdictions where the system is primarily based on consent, like India.

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

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

5 Information Security – Arbitral Participants should apply a proportionate, risk-based approach to information security. They should consider agreeing whether additional information security measures are required for the arbitration in addition to those already employed by the Arbitral Participants in their ordinary course of business, potentially as part of a Data protection protocol, to help manage risk. Reference may be made to the ICCA/NY City Bar/CPR Cybersecurity Protocol for International Arbitration (2020 Edition) **[Link]** and the IBA Cybersecurity Guidelines (2018) **[Link]** where appropriate.

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

7. Transparency – Arbitral Participants should determine what transparency requirements apply to them: (1) generally, including the publication of adequate data privacy notices; (2) when preparing to issue proceedings (in the case of the claimant and its legal counsel); (3) at the outset of proceedings; and (4) as proceedings progress and new personal data is processed or used for a different purpose. Arbitral Participants should consider issuing (or updating pre-existing) privacy notices to meet those requirements.

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

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

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

11. Data Collection and Review – When preparing their cases, parties and their legal counsel should identify and document the: (1) relevant data subjects or categories thereof (2) categories of personal data, sensitive data, personal data of children and any data related to criminal proceedings that are likely to be processed and whether it is primarily low risk business correspondence and documentation; (3) likely impact of that processing on the relevant individuals;(4) lawful basis for processing that data for the arbitration; (5) how applicable transparency obligations have been, or can be, complied with, including whether it is feasible to provide additional notices without infringing on the parties' rights or the integrity of proceedings; and (6) steps to minimise the processing of personal data to that which 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.).

12. Arbitrator Selection – When selecting an arbitrator in a case where a party, arbitrator or institution is aware, or should be aware, that any of the parties or the institution is bound by a data protection law, the Arbitral Participant making the selection should take steps to ensure that personal data may be processed by (including transferred to) the arbitrator in accordance any applicable data protection law.

13. Planning – Any Arbitral Participant that considers itself bound by a data protection law in relation to the proceedings should inform the other Arbitral Participants as soon as practicable so that appropriate measures can be undertaken to ensure that the arbitration is conducted in accordance with the law. Data protection should be included on the agenda of the first procedural conference to give the Arbitral Participants the opportunity to discuss applicable data protection laws and how they can be complied with in a proportionate manner. **[Annexes 3 and 4]**

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

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

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

17. Awards – Before the award is rendered, Arbitral Participants should consider the extent to which personal data should be included in the award and steps that might be taken to minimise the inclusion of personal data in the Award and to ensure its confidentiality when described by the parties.

18. 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

Data Protection Checklist

This checklist contains a non-exhaustive list of data protection considerations that may impact Arbitral Participants.

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 a modern data protection law applies, careful consideration should be given to these issues during the proceedings and when considering Data Protection Protocols, Procedural Orders, and Terms of Reference. 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 under the GDPR

Are you covered by the GDPR?

Establishment

⇒ Consider whether you are established in the EU through stable arrangements.

⇒ Does the processing occur "in the context of the activities" of that EU establishment?

⇒ If so, subject to certain exceptions (e.g. household information), all your personal data processing activities are covered worldwide

Targeting

⇒ If you decide you are not established in the EU, consider whether you have targeted EU data subjects for purposes of this arbitration.

⇒ If so, your processing and related processing for that arbitration are covered, but not your activities generally

Am I data controller, processor or joint controller?

⇒ Consider whether 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.

⇒ If you process personal data but do not control the purpose and means of the data processing, then you may be a data processor, for which you would require a GDPR-compliant data processing agreement. This may be the case, for example, for e-discovery firms, court reporters, and interpretation and translation services in certain contexts.

⇒ Consider whether you jointly control the purpose and means of the processing, 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

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 ⇒ Note that relying on legitimate interests requires a documented legitimate interest 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. This means that consent is not recommended as a lawful basis in the arbitration context and is only appropriate in limited circumstances.
What is my lawful basis for processing special category data or of a child?
⇒ Consider your lawful basis for the processing of any special category data or data relating to a child ⇒ Is the processing of any special category data necessary to establish, exercise or defend a legal claim? What is the basis for processing any data related to a child?
Can I process any data related to criminal activity?
⇒ Consider whether you can process personal data relating to criminal activity, which must be done under a supervising authority's control or as authorized by Union or Member State law.
What is my lawful basis for transferring any data outside the EU?
⇒ Transfer is allowed to countries or international organisations with an adequacy decision, or where appropriate safeguards including standard contractual clauses have been put in place, or where a derogation applies. ⇒ Consider whether third country data transfers are required (including to international organisations) ⇒ Determine whether any countries to which transferred will be made have adequacy decisions ⇒ Consider entering into standard contractual clauses ⇒ Where that is not feasible, consider whether a derogation permitting transfer applies. ⇒ Third country data transfers are permissible, e.g., where necessary to establish, exercise or defend legal claims. This may require that the personal data has been minimised, the transfers are "occasional" and means are put in place to protect the personal data after transfer.

Preparing for a Case

Arbitration Agreement and Arbitrator Selection

⇒ Does the arbitration clause expressly address data protection or information security?

⇒ Is any likely Arbitral Participant governed by a data protection law or regulation that may impact the arbitration?

⇒ Have any of the Arbitral Participants issued data privacy notices? What do they say?

⇒ 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? Are they willing to enter into standard contractual clauses if necessary?

Document Collection and Review

⇒ What kind of personal data is likely to be processed during the arbitration?

⇒ Does it include sensitive data?

⇒ Where is the (i) personal and (ii) sensitive data (if any) 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.

⇒ How will the (i) personal and (ii) sensitive data (if any) be collected and by whom?

⇒ What is the lawful basis for the collection and use of the (i) personal and (ii) sensitive data for a potential arbitral claim or defense under the relevant data protection law(s)?

⇒ Can data related to criminal convictions and offences or related security measures be processed for the arbitration? Personal data of a child?

⇒ Is any relevant data located in a country with a localisation regime (possibly Russia or China)? How will this be managed?

⇒ Is the amount of data being collected fair and proportionate to the claim?

⇒ Have efforts been made to minimize 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?

⇒ 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)?

⇒ 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?

During the Arbitration

Case Management

⇒ When should data protection be addressed during the proceeding? Who should raise it and when?

⇒ What methodology should be used to address data protection during the proceedings?

- Should data protection be addressed by agreement of the parties or order of the tribunal?
- Can a signed data protection protocol agreed between the parties and the tribunal be used to manage data protection compliance for the arbitration covering the issues set out in this Checklist (see Annex 4)?
- If this is not possible, will these issues be addressed in the Terms of Reference or Procedural Order 1?

Lawful basis

⇒ Are the Arbitral Participants satisfied that they have a lawful basis for the processing of any (1) personal data and (2) any sensitive data during the arbitration?

⇒ Have legitimate interests been considered as a basis for the processing of personal data during the arbitration?

⇒ If legitimate interests will be relied upon for the processing of personal data, have the Arbitral Participants undertaken a legitimate interests assessment (see Annex 5)?

⇒ Can data related to criminal convictions and offences or related security measures be processed for the arbitration? Personal data of a child?

Third Country Transfer

⇒ Will any personal or sensitive data be transferred to third countries for purposes of the arbitration?

⇒ If so, what is the lawful basis for the third country transfer under the applicable data protection law?

⇒ If the GDPR applies:

- Do the third countries have adequacy decisions?
- Should consideration be given to entering into Standard Contractual Clauses?
- Are the data transfers necessary to establish, exercise or defend legal claims?
  - Has consideration been given to minimising the personal data through culling and/or pseudonymisation/redaction?
  - Are the transfers "occasional"?
  - What measures will be put in place after the transfer addressing compliance with data protection principles?

Notices

⇒ What notification has been provided to data subjects about the processing of their personal or sensitive data?

⇒ Is the processing of their data for the arbitration compatible with the notification?

⇒ Is it necessary to send a further data privacy notice informing data subjects that their data will be processed in the arbitration? ⇒ What impact would further notification have on any confidentiality of the proceedings?
Data Minimisation
⇒ What efforts will be taken to minimise the personal and sensitive data processed for the arbitration? ⇒ Has consideration been given to culling the data set for relevance and the possibility of redaction and pseudonymisation of personal data and sensitive data where necessary under the applicable data protection law?
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 Subject Rights Requests
⇒ Have the Arbitral Participants identified what steps will be undertaken if a data subject enforces its data subject rights, including data subject access requests, during the arbitration?
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? ⇒ Has consideration been given to what constitutes a data breach?
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?
Indemnities and insurance
⇒ Should any indemnities related to data protection compliance be given, and, if so, by whom and how? ⇒ Have Arbitral Participants considered obtaining insurance in relation to data protection violations or data breaches?
Award
⇒ Do relevant data protection laws and regulations impact the arbitral tribunal's ability to include personal data in the award? ⇒ Should this be addressed with the Arbitral Participants? Has consideration been given to agreeing in advance what personal data and sensitive data will be included in the award?

GDPR-SPECIFIC ANNEXES

ANNEX 4

GDPR Language for Possible Use in Terms of Reference/Procedural Orders/Data Protection Protocols

This language contains possible wording that could be considered for inclusion in a Data Protection Protocol, Procedural Order, or Terms of Reference, where a relevant data protection law applies to one or more Arbitral Participants. Where possible, preferred practice would be to enter to a signed Data protection protocol. The wording is geared around 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.

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 shall 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, including processing prior to its being sent to the Tribunal or otherwise used in this Arbitration;

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 aware of how their data is being processed for the arbitration and any other required information (save where: (a) such personal data will not be obtained directly from those data subjects; and (b) to do so would be impossible or involve disproportionate effort);

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; 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.

The Legal Basis for the Processing

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. 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 rights.

14. If either party considers that processing on this basis is not appropriate, it shall notify the Tribunal forthwith.

15. The Parties and their Legal Representatives agree that they shall not do anything contrary to the principles set forth in paragraphs 12 and 13, including but not limited to seeking data subject consent, without first raising the issue with the Tribunal and obtaining directions.

Transfer of Personal Data [outside the EEA]

16. 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, such transfers will be made to the extent necessary for the Parties to establish, exercise or defend their legal claims or where there is another lawful basis to do so.

17. In all cases of third country data transfer in the context of the proceeding, the data shall be minimized in advance and reasonable measures shall be put in place to ensure that the underlying principles established in the relevant data protection law are complied with after transfer.

Confidentiality [To be omitted in non-confidential arbitrations, but see footnote][2]

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. [A similar confidentiality obligation is contained in Article 3(13) of the IBA Rules on the Taking of Evidence in International Arbitration (as adopted on 29 May 2010) (the "**IBA Rules**"), which the Parties have agreed should be taken into account during the document production stage of the Arbitration.] **[To be included where IBA Rules apply]**

21. 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.

Data Minimisation

22. 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.

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

24. Where feasible, the Parties and their Legal Representatives 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.

[2] Note to Reader: Confidentiality of the proceedings is not required as such by the 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. For example, in the Document Disclosure Guidance, it was suggested that protective orders should be entered into whenever possible before data transfers to the US for purposes of US legal proceedings. Applying the same reasoning to arbitration would suggest that, where possible, confidentiality of the proceedings should be considered as a means of protecting the personal data (including any special categories of personal data) from being made public. Where this is not possible, for example in many investor-State cases, this does not make the processing unlawful but would argue in favour of limiting the personal data being processed.

25. 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 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]

26. 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.

27. 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.

Data Retention

28. Subject to any privacy statements of a data controller which may reflect the legitimate need to retain the personal data for different periods, all personal data processed and used in this Arbitration shall only be retained as long as, and to the extent that, it is necessary in relation to the purposes set out above and/or to fulfil any obligations under applicable laws or ethical requirements (including legal, regulatory and ethical retention obligations). Personal data will need to be retained pending the conclusion of appeals, challenges and/or enforcement of awards in any event and to ensure compliance with the legal and ethical obligations of the Arbitral Participants.

Data Subject Rights

29. Any Arbitral Participant who receives any request from any data subject in respect of the processing of his/her 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.

30. 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.

31. 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.

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

Personal Data Breach

33. 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.

34. Should any Arbitral Participant determine that a personal data breach has occurred involving the personal data processed by them in this Arbitration, they shall promptly: (i) investigate such breach and its likely impact on any relevant data subject's rights and freedoms; (ii) consider whether notification of such breach is legally required; (iii) take appropriate steps to address and mitigate the consequences of such breach and comply with applicable legal requirements; and (iv) notify the other Arbitral Participants when required to do so under the applicable arbitration rules or their ethical obligations.

ANNEX 5

Checklist for Legitimate Interest Assessment

When the GDPR or another modern 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.

For the reasons addressed in the Roadmap in many instances, 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. [Link] When legitimate interests are employed as the lawful basis, the European Data Protection Board has taken the view that a legitimate interest 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 a modern 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 EU 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 has explained that there is a three-part test that should be applied when undertaking a legitimate interest 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 interest 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, and many other interests as well.
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 my or a third party's legitimate interest. In applying this standard, Arbitral Participants, for example, might consider whether data minimisation techniques could be used to reduce the amount of personal data processed without infringing on the party's rights.
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 making a decision regarding whether an individual's rights would override a controller's legitimate interest are: • the nature of the data subject's interests; • the 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 interest assessment?
The European Data Protection Board has explained that the legitimate interest 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

Example Privacy Notices for Arbitration Proceedings for (A) Arbitral Institutions, (B) Arbitrators, and (C) Legal Counsel

EXAMPLES ONLY

Arbitral Participants covered by the GDPR or another modern data protection law should consider whether to issue a Data Privacy Notice in relation to their arbitration related activities. If they decide to do so, they then need to decide each aspect of any Data Privacy Notice that is issued because it will govern how they process data going forward.

We have prepared example Data Privacy Notices below. They are geared towards 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 example notice to add them.

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 a modern data protection law applies, careful consideration should be given to whether a Data Privacy Notice is required and if so, what its content should be. The Example 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 6A

Data Privacy Notice for Arbitral Institutions (Not International Organisations)

EXAMPLE ONLY

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.

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[3] 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;

[3] Note to Reader: Any time legitimate interests are relied on in the EU, relevant EU guidance suggests that there should be a documented legitimate interests' assessment (see Annex 5).

- 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 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;
- With 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.[4]

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 account legal and regulatory

[4] Note to Reader 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 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.

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 defense;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defense;
- 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 6B

Data Privacy Notice for Arbitrators

EXAMPLE ONLY

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 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[5] 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;
- 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

[5] Note to Reader: Any time legitimate interests are relied on in the EU, relevant EU guidance suggests that there should be a documented legitimate interests' assessment (see Annex 5).

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;
- With 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.[6] I make such transfers where there is a lawful basis for doing so.

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.

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 defense;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defense;
- 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:

[6] Note to Reader: 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 relevant regulatory body, I make such transfers in accordance with my legal obligations, for example where the transfers are necessary to establish, exercise or defend legal claims in the context of arbitration proceedings, or where there is another lawful basis to do so.

- 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 6C

Data Privacy Notice for Legal Counsel

EXAMPLE ONLY

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, or 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, or 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 or 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 or the firm**] may obtain the following personal data about you in the context of Dispute Resolution Proceedings in which [**I, we or the firm**] act as a legal counsel:

Institutional Representatives

- Your name, contact details, and other information you may provide to [**me, us, or the firm**] in the context of Dispute Resolution Proceedings in which [**I, we or 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, or 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, or the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I, we or 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, or 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, or the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I, we or 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, or 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, or the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I, we or 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, or 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/or the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I, we or 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 or the firm**] during Dispute Resolution Proceedings in which you provide written or oral evidence;
- Any other personal data of yours submitted to [**me, us or 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, or the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I, we or the firm**] act as a legal counsel.

Other Individuals

- Personal data of yours submitted to [**me, us or 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, or the firm**] from third parties or publicly available resources in the context of Dispute Resolution Proceedings in which [**I, we, or the firm**] act as a legal counsel.

How do [I, we or the firm] use your personal information and on what legal basis?

In the context of Dispute Resolution Proceedings in which [**I, we, or the firm**] act as a legal counsel, depending on the circumstances, [**I, we, or 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;[7]
- To maintain an informal database of potential Neutrals and tribunal secretaries as necessary to further [**my, our or 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, or 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, or 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, or 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 or the firm**] may process your personal data (only) as necessary to perform [**my, our, or the firm's**] obligations and duties under that agreement;

[7] Note to Reader: Any time legitimate interests are relied on in the EU, relevant EU guidance suggests that there should be a documented legitimate interests' assessment (see Annex 5).

- 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 Legal Compliance Obligations.

Other Individuals

- As necessary for furthering [**my/our/the firm's**] and our client's legitimate interests in resolving its dispute efficiently and expeditiously and ensuring that our client's rights are respected;
- Where necessary to meet my Legal Compliance Obligations.

How do share your personal information?

Depending on the circumstances in which [**I, we, or the firm**] process your personal data, [**I, we, or 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 you are also involved;
- [**My/Our/The firm's**] service providers such as third-party data hosting providers in order for **[me, us or the firm]** to provide services in connection with Dispute Resolution Proceedings;
- With third parties, including my colleagues, professional advisors, financial institutions, or law enforcement agencies, where necessary to perform conflict checks, to comply with [**my, our, or the firm's**] Legal Compliance Obligations, or where it is otherwise in [**my, our, or 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, or the firm**]transfer personal data to third countries in connection with the services [**I, we, or the firm**] perform for the Dispute Resolution Proceedings in which [**I, we, or the firm**] serve as a legal counsel, or as may otherwise become necessary in the course of [**my,**

our, or the firm's] operations. [8] [**I, we, or the firm**] make such transfers where there is a lawful basis for doing so.

How long do [**I, we, or the firm**] **retain your personal information?**

[**I, we, or 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, or 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, or 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 or the firm**] hold where it is incomplete or inaccurate;
- Have your personal data erased where there is no good reason for [**me, us, or the firm**] continuing to use or retain it, unless the processing is necessary to pursue a legal claim or defense;
- Request that your personal data is used only for restricted purposes, unless the processing is necessary to pursue a legal claim or defense;
- 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 [**I, we or 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, or the firm**] treat your personal data, you can contact [**me, us, or the firm**] as follows:

[8] Note to Reader: 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 relevant regulatory body, we make such transfers in accordance with our legal obligations, for example where the transfers are necessary to establish, exercise or defend legal claims in the context of Dispute Resolution Proceedings, or where there is another lawful basis to do so.

- 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, or the firm**] act as a legal counsel, [**I, we or the firm**] suggest that you raise your concerns with that party first before contacting [**me, us, or the firm**] regarding the processing of your personal data in the context of Dispute Resolution Proceedings.

Date: [**dd mm year**]

ANNEX 7

EU Standard Contractual Clauses

EU controller to non-EU or EEA controller (see links below):

- Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ L 181, 4.7.2001, p. 19 (see Annex)

- Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004, p. 74 (see Annex)

EU controller to non-EU or EEA processor (see links below):

- Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, p. 5 (see Annex)

RESOURCE ANNEXES

ANNEX 8

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,* (Article 29 Data Protection 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,* (Article 29 Data Protection 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",* (Article 29 Data Protection Working Party, 00264/10/EN WP 169, 2010)

Data Processing

6. *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 Mar. 19, 2018)

Data Transfers

7. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679,* European Data Protection Board, (2018) [referred to as "**Data Transfer Guidance**"]

8. *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, (Article 29 Data Protection Working Party, 2093/05/EN WP 114, 2005)

9. *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

10. 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)

11. *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 (Jan. 24, 2018)

12. *Handbook on European Data Protection Law*, European Union Agency For Fundamental Rights (2018)

Joint Controller

13. Case C-210/16 Wirtschaftsakademie Schleswig-Holstein

14. Case C-25/17 Tietosuojavaltuutettu.

15. *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)

Lead Supervisory Authority

16. *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority,* (Article 29 Data Protection Working Party, 16/EN WP 244 rev. 01, 2017*)*

Personal Data

17. *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 May 31, 2018)

Proportionality

18. *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (Dec. 19, 2019)

Risk-Based Approach

19. *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks 3,* (Article 29 Data Protection Working Party, 14/EN 218 WP 169, 2014)

Territorial Scope

20. *Draft Guidelines 3/2018 on the Territorial Scope of the GDPR*, EDPB, November 2018

Transparency

21. *Guidelines on Transparency under Regulation 2016/679,* (Article 29 Data Protection Working Party, 17/EN WP 260, 2018)

Arbitration-related Materials

22. *Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration,* International Chamber of Commerce, January 1st, 2019

23. *"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)

24. *IBA Rules on the Taking of Evidence in International Arbitration* (International Bar Association, 2010)

25. *Commentary on the Revised Text of the 2010 IBA Rules on the Taking of Evidence in International Arbitration* (2010)

Cybersecurity Materials

26. *ICCA/NY Bar/CPR Consultation Draft Cybersecurity Protocol for International Arbitration*, http://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf [https://perma.cc/K52P-MHJL] (archived May 30, 2018)

27. *Cybersecurity Guidelines,* IBA Presidential Task Force on Cybersecurity (2018)

28. *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)

29. *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

30. *Cross-Border Application of EU's General Data Protection Regulation (GDPR)-A private international law study on third state implications,* Anni-Maria Taka, (2017)

31. *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.

32. *Data protection and conflict-of-laws: a challenging relationship,* Maja Brkan, Eur. Data Prot. L. Rev. 2 (2016): 324

33. *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

34. *Protection of Privacy in Private International and Procedural Law: Interim Report and Commentary*, International Law Association Sydney Conference (2018)

ANNEX 9

Compendium of Selected Data Protection Laws

Jurisdictions with EU Adequacy Decisions				
No.	**Country**	**Supervisory Authority**	**Implementing Legislation**	**Adequacy Decision**
1.	**Andorra**			Commission Decision 2010/625/EU
2.	**Argentina**	Agência de Proteção de Dados (APD) – approved by Presidential Decree but not yet created	• Data Protection Law (Law no. 22/11 of 17 June) • Electronic Communications and Information Society Services Law (Law no. 23/11, of 20 June 2011) • Protection of Information Systems and Networks Law (Law no. 7/17, of 16 February)	Commission Decision 2003/490/EC
3.	**Canada (commercial organisations)**	1. Office of the Privacy Commissioner of Canada ('PIPEDA') 2. Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta 3. Office of the Information and Privacy Commissioner for British Columbia ('PIPA BC'), and	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'),	Commission Decision 2002/2/EC

		Commission d'accès à l'information du Québec ('Quebec Privacy Act')	• 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')	
4.	**Faroe Islands**			Commission Decision 2010/146/EU
5.	**Guernsey**	• Data Protection Authority • Office of the Data Protection Authority	Data Protection (Bailiwick of Guernsey) Law 2017 (DPL 2017) (came into force on May 25, 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	Commission Decision 2008/393/EC

			(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.	
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.	**Switzerland**	*See above*	*See above*	Commission Decision 2000/518/EC
12.	**Uruguay**	Unidad Reguladora y de Control de Datos Personales (URCDP or Data Protection Authority)	• Data Protection Act Law No. 18.331 (August 11, 2008) • Decree No. 414/009 (August 31, 2009)	Commission Implementing Decision 2012/484/EU
13.	**United States of America (limited to the Privacy Shield framework)**	*See above for specific state laws*	*See above*	Commission Implementing Decision 2016/1250
***South Korea – adequacy talks ongoing**				

Selected Data Protection Laws of Non-EEA Jurisdictions			
	Country	**Supervising Authority(ies)**	**National Law(s)**
1.	**Brazil**	National Data Protection Authority (ANPD)	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**	1. Office of the Privacy Commissioner of Canada ('PIPEDA') 2. Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta 3. Office of the Information and Privacy Commissioner for British Columbia ('PIPA BC'), and 4. 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**	1. Cyberspace Administration of China (CAC) 2. 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 – [draft] Information Technology Act, 2000
6.	**Mexico**	1. 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). Currently subject to substantial revision (draft published September 15, 2017) expected to pass autumn 2019 – aims to align the DPA with the GDPR.

10.	**USA**[9]	No single national authority The Federal Trade Commission has authority to issue and enforce privacy regulations in specific areas	
11.	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
12.	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
13.	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*
14.	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*

[9] The list of states with data protection frameworks is not exhaustive. We refer to a select few, deemed especially relevant in arbitration.

			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*
15.	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)**
16.	**Austria**	Österreichische Datenschutzbehörde http://www.dsb.gv.at/	(i) Federal Act Amending the Data Protection Act 2000 (Data Protection Adaptation Act) 2018 (ii) Federal Law 23 (iii) Federal Law 24
17.	**Belgium**	Autorité de la protection des données)/ Gegevensbeschermingsautoriteit (APD-GBA) https://www.autoriteprotectiondonnees.be/ https://www.gegevensbeschermingsautoriteit.be/	(i) Law of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data (ii) Law of 3 December 2017 establishing the Data Protection Authority [Dutch]
18.	**Bulgaria**	Commission for Personal Data Protection https://www.cpdp.bg/	[legislation in draft] [Bulgarian]
19.	**Croatia**	Croatian Personal Data Protection Agency http://www.azop.hr/	Law on Implementation of the General Data Protection Agreement [Croatian]
20.	**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 [Greek]

21.	**Czech Republic**[10]	Office for Personal Data Protection http://www.uoou.cz/	[Act on processing of personal data in draft (amendments to herein stated sections are not expected)]
22.	**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) [Danish] https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf [English]
23.	**Estonia**	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) http://www.aki.ee/	Personal Data Protection Act 616 SE [Estonian]
24.	**Finland**	Office of the Data Protection Ombudsman http://www.tietosuoja.fi/en/	Data Protection Act (Fi: Tietosuojalaki, 1050/2018) [Finnish]
25.	**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 [French]; and - Ordinance No. 2018-1125 dated 12 December 2018 implementing Article 32 of Law No. 2018-493. *NB:* Ordinance No. 2018-1125 will enter into force no later than 1 June 2019.

[10] 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 expressively permitted by such special legal act.

			- 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 [French]
26.	**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 [English]
	Baden-Württemberg	(i) 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 [German]
	Bavaria	(ii) Bavarian Data Protection Commissioner https://www.datenschutz-bayern.de/	Bavarian Data Protection Act (Bayerisches Datenschutzgesetz) dated 15 May 2018 [German]
	Berlin	(iii) Berliner Beauftragte für Datenschutz und Informationsfreiheit https://www.datenschutz-berlin.de/	Act to Adapt Berlin Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (Gesetz zur Anpassung des Berliner Datenschutzgesetzes und weiterer Gesetze an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 13 June 2018 [German]
	Brandenburg	(iv) 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	Act on adaptation of the general data protection law to the Regulation (EU) 2016/679 and on implementation of the Directive (EU) 2016/680 (Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 8 May 2018 [German]
	Bremen	(v) 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 [German]
	Hamburg	(vi) Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz-hamburg.de/	Act to Adapt Hamburg Data Protection Act to Regulation (EU) 2016/679 (Gesetz zur Anpassung des Hamburgischen Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679) dated 18 May 2018 [German]

	Hessen	(vii) Der Hessische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz.hessen.de//	Hessian Act on adaptation of Hessian data protection law to the Regulation (EU) 2016/679 and implementation of the Directive (EU) 2016/680 as well as freedom of information (Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit) dated 3 May 2018 [German]
	Mecklen-Vorpommern	(viii) 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 Mecklen-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 [German]
	Lower Saxony	(ix) Die Landesbeauftragte für den Datenschutz Niedersachsen https://www.lfd.niedersachsen.de/startseite/	Law on the Reform of Lower Saxony Data Protection Law (Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts) dated 16 May 2018 [German]
	North Rhine-Westphalia	(x) Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen https://www.ldi.nrw.de/	Act on the Adaption of the Data Protection Law to the Regulation (EU) 2016/679 and implementation of the Directive (EU) 2016/680 (Gesetz zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 17 May 2018 [German]
	Rheinland-Pfalz	(xi) 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 [German]
	Saarland	(xii) Unabhängiges Datenschutz Zentrum Saarland https://datenschutz.saarland.de/	Act no. 1941 on adaption of the data protection act of the Federal State Saarland to the Regulation (EU) 2016/679

			(Gesetz Nr. 1941 zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679) dated 16 May 2018 [German]
	Saxony	(xiii) Sächsischer Datenschutzbeauftragter https://www.saechsdsb.de/	Act on the Adaption of State Data Protection Law to the 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 (Gesetz zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) dated 26 April 2018 [German]
	Saxony-Anhalt	(xiv) Landesbeauftragter für den Datenschutz Sachsen-Anhalt https://datenschutz.sachsen-anhalt.de/nc/datenschutz-sachsen-anhalt/	Data Protection Law Saxony-Anhalt (Datenschutzgesetz Sachsen-Anhalt) dated 21 February 2018 [German]
	Schleswig-Holstein	(xv) Unabhängiges Landeszentrum für Datenschutz https://www.datenschutzzentrum.de/	Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 2 May 2018 [German]
	Thuringia	(xvi) Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit https://www.tlfdi.de/	Thuringia Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680) dated 6 June 2018 [German]
27.	**Greece**	Hellenic Data Protection Authority http://www.dpa.gr/	[legislation in draft] [Greek]

28.	**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 [Hungarian]
29.	**Iceland**	Persónuvernd https://www.personuvernd.is/	
30.	**Ireland**	Irish Data Protection Commission https://www.dataprotection.ie/	Data Protection Act 2018 [English]
31.	**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) [Italian]
32.	**Latvia**	Data State Inspectorate http://www.dvi.gov.lv/lv/	Personal Data Processing Law [Latvian]
33.	**Liechtenstein**	Data Protection Office, Principality of Liechtenstein https://www.datenschutzstelle.li	Liechtenstein Data Protection Law, 4 October 2018
34.	**Lithuania**	State Data Protection Inspectorate https://www.ada.lt/	Law on the Protection of Personal Data [Lithuanian]
35.	**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 [French]

36.	**Malta**	Office of the Information and Data Protection Commissioner https://idpc.org.mt/en/Pages/Home.aspx	(i) Data Protection Act (CAP 586) [English] (ii) Other Subsidiary Legislation, including: Subsidiary Legislation 586.09 Restrictions of the Data Protection (Obligations and Rights) Regulations [English]
37.	**The Netherlands**	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/nl	Law Implementing the General Data Protection Regulation [Dutch]
38.	**Norway**	Datatilsynet www.datatilsynet.no	[Draft bill published in July 2017] [Norwegian]
39.	**Poland**	Personal Data Protection Office (Urząd Ochrony Danych Osobowych) https://uodo.gov.pl/	Act of 10 May 2018 on the Protection of Personal Data [Polish]
40.	**Portugal**	Comissão Nacional de Protecção de Dados – CNPD https://www.cnpd.pt/	[Legislation in draft] [Portuguese]
41.	**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 [Romanian] https://iapp.org/media/pdf/resource_center/Romanian_Data_Protection_Law_English_Translation.pdf [unofficial English 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 [Romanian]

42.	**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*") [English]
43.	**Slovenia**	Information Commissioner of the Republic of Slovenia https://www.ip-rs.si/	[legislation in draft] [Slovenian]
44.	**Spain**	Agencia Española de Protección de Datos (AEPD) https://www.agpd.es/	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [Spanish]
45.	**Sweden**	Datainspektionen http://www.datainspektionen.se/	Law (2018:218) with additional provisions to the EU Data Protection Ordinance [Swedish] Regulation (2018: 219) with additional provisions to the EU Data Protection Ordinance [Swedish]
46.	**United Kingdom**	Information Commissioner's Office https://ico.org.uk/	Data Protection Act 2018