ICCA
INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION

the global voice of the legal profession®

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

Roadmap to Data Protection in International Arbitration

28 February 2019

Introduction

This ICCA/IBA Roadmap to Data Protection in International Arbitration seeks to provide a framework for arbitration professionals to better understand how data protection and privacy principles may affect their activities and what obligations they may have in the context of an arbitration.

While the details of data protection regulation are complex, the underlying principles are not and arbitration professionals and parties should be aware of those principles and to manage each arbitration in a manner that is consistent with them.

The goal of data protection legislation is to protect the privacy of individuals by reducing the volume of personal data that is processed, including in arbitration, and by ensuring that only necessary personal data is processed in a secure manner, during as limited a time frame as possible in light of the purpose of the processing.

This Roadmap aims at fostering a better understanding of data protection principles within the arbitration community in a user-friendly manner with references to checklists and source materials in the Annexes, and with further detail on the main concepts in the Explanatory Notes.

a. Why should you care?

Every participant in an arbitration who has access to personal data (including the parties, their counsel, arbitral institutions, arbitrators, experts, vendors and service providers (e-discovery experts, information technology professionals, court reporters, translation services, etc.) referred to as "**Arbitral Participants**") should consider for each individual case whether any data protection laws may apply and if so, what that means for them and for the conduct of the arbitration.

It goes beyond the scope of this Roadmap to survey the hundreds of data protection laws in force around the world today. Instead, the General Data Protection Regulation[1] ("**GDPR**") is used in this Roadmap as the reference to explain how data protection may have an impact on an arbitration. We chose the GDPR because:

- it is the most comprehensive and most onerous data protection regulation in force to date;
- the European approach is widely drawn upon by jurisdictions outside the EU as a basis for their laws, and, as a result, is quickly becoming a global standard;
- it is likely to apply to you either as matter of law or contract whenever you are involved in an arbitration with *any* EU nexus (whether through the parties, the institution, other arbitrators, witnesses, experts or otherwise);
- when it does apply, the GDPR applies broadly to virtually every action (or inaction) in a typical arbitration; and
- it imposes serious potential fines, civil liability (which may be joint and several), criminal penalties, and should also be taken into account for the purposes of ensuring that an arbitral award is enforceable.

[1] 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, p. 1.

For your reference, Annex 8 contains a table including a non-exhaustive list of references to some of the national and regional data protection laws of importance to arbitration.

b. What does data protection mean for arbitration?

Although many of the principles underlying the GDPR regime previously applied both in the EU and to arbitration under the Data Protection Directive, the entry into force of the GDPR in May 2018 has put a spotlight on the importance of data protection in arbitration [*see Explanatory Note 1*].

As a result, the users and providers of arbitration services are becoming increasingly aware of their obligations, and data subjects of their rights, whenever personal data is processed, including in the context of arbitrations. This increased awareness comes with increased risk of enforcement and supervision efforts of the regulatory authorities, with potential for non-compliance can add up to 4% of global gross revenue or EUR 20 million, whichever is higher [*see Explanatory Note 1*].

The need for compliance with the GDPR has led companies, which are the primary users of arbitration services, throughout the EU and elsewhere to review their data collection, retention, processing and security policies. For the same reason, all arbitration professionals need to do the same and consider what data they process, where, by what means, with which data security measures, and for how long.

Arbitration plays a major role in the administration of justice in cross-border disputes. Moreover, the processing of personal data (by means of communication, as well as documentary and witness evidence) is an essential component of the arbitral process. The consensual nature of arbitration, the independence of arbitral decision-making and the secrecy of deliberations are fundamental tenets of the arbitration process. Applying the GDPR to arbitration therefore requires balancing the rights and obligations contained in the GDPR with the fundamental rights of defence and due process at stake in every arbitration (Art. 24).

Each arbitration case is different in nature and the application of the GDPR to an arbitration and its participants depends on numerous factors, including (among others) where the Arbitral Participants are established, whether they engage in targeting EU data subjects, where the relevant data is located, where the administering institution is based, and whether the applicable national data protection law(s) contain any relevant exemption or derogation.

The fact-specific application of the GDPR to an arbitration makes it impossible for this Roadmap to provide one-size-fits all solutions. It is the responsibility of every individual Arbitral Participant to ascertain in relation to each arbitration in which he/she is involved what data protection obligations apply and what measures should be taken to comply with those obligations and what risks they face if they don't comply. These are individual responsibilities with individual liability. GDPR violations may result in exposure to administrative fines, civil and/or criminal liability and further sanctions and may even put the enforceability of an award at risk.

c. The structure and limitations of the Roadmap

None of the EU institutions, supervisory authorities or courts have directly addressed the application of the GDPR to arbitration. This Roadmap attempts to fill the void by identifying the issues that may arise when the GDPR's provisions are applied in the arbitration context. This Roadmap identifies solutions that may be considered to ensure that the processing of personal data in arbitration is undertaken in a manner that is consistent with both the GDPR and the parties' fundamental due process rights.

The main source of guidance referred to in this Roadmap are the provisions of the GDPR itself, as well as its recitals. While there is no specific guidance about how data protection applies in arbitration, the European Data Protection Board (the "EDPB") and its predecessor, the Article 29 Working Party (the "Working Party"), have provided useful general guidance about the privacy principles addressed in this Roadmap, which is also referred to herein. Moreover, recent ECJ decisions are important reminders that the ECJ interprets EU data protection laws very broadly, which is worth bearing in mind when applying the GDPR in concrete cases.[2]

This Roadmap is intended to serve as a concise reference to foster Arbitral Participants' understanding of the application of data protection principles in arbitration. The Roadmap is accompanied by:

- a set of Annexes, providing practical information, a glossary, checklists and references aimed at enabling Arbitral Participants to apply data protection principles in the practice of arbitration; and
- a set of Explanatory Notes, providing greater detail on the issues identified in the Roadmap and examples with references to resources the Arbitral Participants may want to refer to.

The entirety of the Roadmap, its Annexes and Explanatory Notes will necessarily be a living document. On the date of publication of its first edition [**month**] 2019, there simply is no regulatory guidance or EU case law on the question as to whether and how the GDPR applies in arbitration. It is hoped that over time the supervising authorities and courts will provide clarity on the implications of the GDPR for each category of Arbitral Participants and for the arbitral process as a whole.

It bears noting that the Roadmap consistently refers to the EU, while the scope of application of the GDPR extends to the European Economic Area (EEA), which encompasses in addition to the EU Member States also Iceland, Liechtenstein and Norway. However, as the EU is a notion that is commonly understood worldwide, this Roadmap refers to the EU instead of the EEA, but read EEA.

Lastly, nothing in this Roadmap, its Annexes or the Explanatory Notes can be taken as legal advice. This Roadmap provides information and resources to enable Arbitral Participants to more easily understand their obligations. However, compliance with the applicable data protection regulations in a particular case remains the responsibility of each individual Arbitral Participant. Arbitral Participants should seek legal advice with respect to their compliance with data protection law in the specific circumstances of their data processing, where appropriate.

---

[2] *See* Case C-210/16 Wirtschaftsakademie Schleswig-Holstein ; Case C-25/17 Tietosuojavaltuutettu ; *CJEU rules on joint controllership – what does this mean for companies?*

TABLE OF CONTENTS

I. GDPR FOR ARBITRATION IN A NUTSHELL

a. Broad Territorial Scope

The GDPR applies to the processing of personal data:

(i) in the context of the activities of an establishment of a controller or a processor in the EU; or

(ii) where the processing activities are related to the offering of goods or services *in* the EU (regardless of residence or citizenship) (Art. 3)[3].

Where even one Arbitral Participant is established in the EU or targets data subjects in the EU, regard must be had to the GDPR by all other Arbitral Participants.

An establishment implies stable arrangements, therefore, in deciding whether the data processing takes places within the context of an EU establishment, the first question is whether the data processor or controller undertakes activities in the EU through stable arrangements, and, if so, whether the data processing activities at issue are being carried out in the "*context*" of those activities. If the answer to both questions is affirmative, those data processing activities are covered by the GDPR wherever they take place in the world.

Where the data processing does not taken place in the context of an EU establishment, the second question is whether it "relates" to the offering of a service that was targeted to EU data subjects. If that test is met, the data processing and all related data processing is also subject to the GDPR.

Lastly, even where the GDPR does not apply as a matter of law, its main provisions may still apply as a matter of agreement, which agreement is required before data can be transferred outside the EU to entities or individuals who are not subject to the GDPR. This leads to significant scope creep, even beyond the already broad territorial reach of the GDPR.

b. Broad Subject Matter Scope

The GDPR applies whenever:

(i) "personal data" is

(ii) "processed"

during activities falling within its broad territorial scope or as a matter of agreement. Both of these concepts are broadly defined and would cover most activities in the context of a typical arbitration.

"Personal data" under the GDPR means any information relating to a natural person who can be directly or indirectly identified from that information (Art. 4). It is irrelevant to the GDPR's application that the personal data is contained in a business-related document (such as work

[3] Unless otherwise stated, all references to Articles and Recitals are to the GDPR.

files, emails, lab notebooks, agreements, construction logs, etc.). Information that is clearly *about* someone is also likely to constitute personal data. That includes opinions or assessments (for example, as to their credibility as a witness), whether subjective or objective, true or false. The notion of personal data under the GDPR is much wider than the US concept of Personally Identifiable Information (PII), and a substantial portion of information exchanged during a typical international arbitration contains data that qualifies as personal data in the sense of the GDPR [see Explanatory Note 5].

Understanding the concept of "*personal data*" is key to understanding how the GDPR operates in practice because each individual "*data subject*" is granted significant rights, which rights potentially apply to everyone who is identified or could be identified from the documents and evidence submitted in an arbitration. It is then the obligation of virtually everyone who has access to that personal data not only to comply with the GDPR, but also to be able to demonstrate compliance [see Explanatory Notes 15 - 17].

The GDPR imposes a set of rules and other obligations that must be complied with whenever personal data is "*processed*." "*Data processing*" is defined broadly in the GDPR to include not only active steps such as collecting, using and disseminating data, but also passive operations such as receiving, holding, organising and storing data. The GDPR equally applies to electronically processed information, as well as to the manually processed data of paper files (Rec. 15). Most activities undertaken in a typical arbitration constitute processing [see Explanatory Note 6].

The GDPR thus attaches serious rights and obligations to information that may not traditionally have been thought of in arbitration as confidential or sensitive and to a broad range of activities encompassing most of what occurs during a typical arbitration.

As a result, whether or not the GDPR applies and what its effect is in a specific case is something that should systematically be addressed and considered in any arbitration with any EU nexus at all, even if ultimately, it is determined that the GDPR has no application in that particular case.

c. Compliance Standards

The GDPR imposes different obligations on Arbitral Participants, depending on whether they qualify as a (1) data controller, (2) data processor or (3) joint controller. [Link EN 13]

1. Primary Responsibility of Data Controller

The primary obligation for compliance and for demonstrating compliance with the GDPR rests on the controller of the personal data, which is defined by the GDPR as "*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*" (Art. 4(7)).

A data controller is the person who decides *why and how personal data is processed*. The Working Party illustrated the point by reference to the following hypothetical:

> A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. *However, this mandate is not focused on*

processing data but on representation in court, for which activity such professionals traditionally have their own legal basis. Therefore, that barrister is to be regarded as an independent '*controller'* when processing data in the course of the legal representation of his/her client.

The data protection supervisory authority for the United Kingdom, the Information Commissioner's Office ("ICO"), similarly concluded that solicitors who determine how data will be processed, qualify as data controllers. [Link EN 13]

It is expected that the same approach would be applied to most Arbitral Participants, with the possible exception of data analysts.

2. Delegation to Data Processor

Data controllers can delegate the processing of data under their control to a data processor, which is defined as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*" (Art. 4(8)).

Under the GDPR, data controllers can only engage data processors who commit to comply with its terms in an enforceable agreement established in accordance with the GDPR (Art. 28).

A data processor has independent responsibility (and attendant liability) for compliance with the GDPR's requirements for data security and data transfer and for notifying the data controller in the case of data breach.

In determining whether an Arbitral Participant can be classified as a data processor, the question will be whether the Arbitral Participant:

(1) acts under the instruction of a data controller in undertaking their tasks;
(2) does not decide the purpose of the data processing; and
(3) is retained under a GDPR-compliant data processing agreement.

Whether this standard is met, for example, by data analysts and other e-discovery professionals will depend on who takes the decisions with respect the purpose and means of any and all processing and will be influenced by number of factors, such as whether a GDPR-compliant data processing agreement has been entered into and to whom in their contractual relationship the decision-making power is allocated as to the purpose of the processing.

[Link EN 13]

3. Joint Controllers

In addition to data controllers and data processors, there is the third category of joint controllers, in which Arbitral Participants may potentially find themselves. Joint controllers are those who jointly determine the "purpose and means" of the data processing.

Joint controllership may arise without formal agreement both between independent data controllers and between data processors and data controllers if they are considered to determine jointly the "*purpose and means*" of processing.

Under the GDPR, each of the joint controllers is responsible for protection of data and they are jointly and severally liable for any data protection violation. Data subjects have the right to seek compensation from joint controllers in the same way as from any independent controller. Each joint controller is liable *vis-à-vis* the data subject for the entire damage caused by the processing, unless they can prove that they are not in any way responsible for the event giving rise to the damage. The arrangement made between controllers is irrelevant in relation to the data subject, although it may allow the joint controller to seek compensation from the other joint controller(s). In addition, joint controllers are each fully accountable to the regulatory authorities for any failure to comply with their responsibilities.

Whether Arbitral Participants can be considered joint controllers involves a factual assessment, which turns on whether they can properly be considered to determine jointly the "*purpose and means*" of processing. It appears from recent ECJ case law that the notion of joint controllership is broadly interpreted.

The possibility of Arbitral Participants becoming jointly responsible for data protection and the risk of being exposed to joint and several liability in case of violation, emphasizes the importance of compliance with the GDPR for every Arbitral Participant subject to its terms during every arbitration in which the GDPR applies.

[Link EN 14]

d. Key Obligations

Data controllers, including during an arbitration, are required to comply with the following six principles (Art. 5 GDPR), namely to ensure that all personal data is:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ("*lawfulness, fairness and transparency*");

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("*purpose limitation*");

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("*data minimisation*");

d. accurate and, where necessary, kept up to date, meaning that every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("*accuracy*");

e. kept for no longer than is necessary for the purposes for which the personal data are processed ("*storage limitation*");

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("*integrity and confidentiality*"). [Link EN 15]

These principles are then implemented through the other provisions of the GDPR. Data controllers are required both to comply with the GDPR and to be able to demonstrate that they

have complied [Link EN 17] (Art. 24). Moreover, data controllers are instructed to apply a risk-based approach to compliance. [Link EN 16].

The following Section II of the Roadmap describes how each of these principles as implemented through the other provisions of the GDPR may apply in the arbitration context.

e. Derogations

The GDPR provides for specific areas, in respect of which Member States are expressly allowed to derogate from its terms. Some Member States have relied on these provisions to exempt certain data and data processing during out-of-court proceedings from coverage in their legislation.

Analysis of the application of data protection in the context of an arbitration may therefore require a consideration of Member State law. [Link EN 3] For example, Ireland has relied on the right to exempt "*judicial proceedings*" and "*the enforcement of civil law claims*" to also exempt out-of-court proceedings from the application of most of the data subject rights imposed by the GDPR (Art. 23). No other Member State has adopted such a broad exception for out-of-court procedures, although, the revised Swiss Data Protection Act (Switzerland being an adequacy country) purports to exempt arbitration altogether.

The GDPR also includes a broad right for Member States to derogate with respect to *employee data*, which is also likely to have an impact on international arbitration.

[Link EN 2]

f. Supervision and sanctions

The GDPR provides that in each Member State, an *independent supervisory authority* will ensure consistent application and enforcement of the GDPR in its territory, handle complaints from data subjects, conduct investigations and adopt standard contractual clauses for data transfers.

Data subjects have the right to complain to the supervisory authority of their country of residence for a rights violation by an Arbitral Participant. The Arbitral Participant can in turn request that the matter be dealt with by its lead supervisory authority. If the lead supervisory authority declines to address the matter, any competent supervisory authority has jurisdiction.

For cross-border data processing within the EU, a lead supervisory authority is entrusted with the enforcement of the GDPR on data controllers having their sole or main establishment in that country. Complaints can be raised with the lead supervisory authority or with any "*supervisory authority concerned.*" Only one decision should be reached on any issue, but which authority renders that decision depends on the circumstances, with deference typically to the lead supervisory authority, if it so requests.

The supervisory authorities also have investigative powers to carry out data protection audits, to order the controller to disclose information and notify the controller of any alleged infringements. They further have corrective powers to issue warnings and reprimands, order the controller or processor to comply with a data subject's requests, impose a temporary ban on processing, suspend data flows to third countries, and impose administrative fines (Art. 83).

In the exercise of their supervisory powers, authorities can impose administrative fines of up to the higher of EUR 20 million or 4% of an undertaking's world-wide revenue for the violation of most the GDPR's provisions (Arts. 5 to 7, 9, 12 to 22 and 44 to 49) and to the higher of EUR 10 million or 2% of an undertaking's world-wide revenue for lesser violations (Arts. 8, 11, 25 to 39, 42 and 43). It is unlikely that insurance will be available for such fines, although the position is not yet clear.

The GDPR requires Member States to impose criminal penalties for infringements of the GDPR that are not subject to administrative fines. The GDPR further provides that every individual who wants to enforce compliance or has suffered material or non-material damage from an infringement of the GDPR also has the right to bring proceedings against a controller or processor before the courts of the Member State where the data subject resides or where the controller or processor is established (Art. 79).

A data subject also has the right to a remedy before Member State courts against a supervisory authority for a decision rendered or the prolonged inactivity of a supervisory authority.

Under the GDPR data controllers no longer need to register with the supervisory authority in the place where they are established. However, in some countries, like the UK, data controllers have to identify themselves and pay an annual fee.

Furthermore, if an entity does not have an EU establishment but engages in targeting data subjects in the EU, it may need to designate in writing a representative in the EU (Art. 27). Any supervisory authority within the EU has regulatory authority over such an entity without the need to defer to a lead supervisory authority.

The GDPR exempts "*courts acting in their judicial capacity*" from the jurisdiction of the supervisory authority, in favour of supervision by the Member State courts. In Spain, the Constitutional Court held that arbitration is a "*jurisdictional equivalent*" and a similar finding was made in an old German case.[4] What that means for data protection remains to be seen, although it could be that in those countries, the processing of personal data by arbitrators, when acting in their judicial authority, could be subject to the jurisdiction of the same authority that supervises data processing by the courts (instead of the ordinary supervisory authority). [Link EN 2]

[4] *See* Judgement 1/2018, of 11 January 2018 of the Plenary of the Spanish Constitutional Court. [German case to be added].

II. APPLICATION OF THE GDPR TO ARBITRAL PROCEEDINGS

With that whistle-stop tour of the GDPR in mind, the remainder of the Roadmap considers how the GDPR may affect Arbitral Participants either before, during, or after an arbitration. It is organized around the life cycle of an arbitration case. It should be considered together with the Annexes, which contain templates for certain data protection notices and non-exhaustive checklists of issues that parties, counsel, institutions and arbitrators may want to consider in establishing whether the GDPR applies to them and the arbitration proceedings.

a. Processing outside of a specific arbitration

Like everyone else, Arbitral Participants covered by the GDPR should bear in mind that they will have general obligations under the GDPR that apply to all their data processing activities regardless of any involvement in a specific arbitration. These obligations include adopting GDPR-compliant data security measures, data breach procedures and ensuring that data transfers are lawful.

Virtually all EU-based Arbitral Participants will be data controllers with respect to at least some personal data they process. Insofar as they are data controllers, they are obliged to ensure that the data processing is lawful, and that data subjects rights are complied with. This will often include providing a publicly and easily accessible GDPR-compliant data privacy notice, for example on their website, to put data subjects on notice of the processing of their data, and putting in place a mechanism to comply with data subjects' right requests. Annex 2 provides a checklist of issues that Arbitral Participants subject to the GDPR should consider generally with respect to data protection compliance.

To avoid repetition, these issues are addressed below in the context of arbitral proceedings. However, it is important to keep in mind that they will often apply independent of specific proceedings because of the nature of Arbitral Participants' general activities.

b. Planning arbitration proceedings

Data protection should be considered from the time the arbitration agreement is drafted through to the enforcement of any award (and beyond in relation to any potential subsequent disputes). Annex 3 provides a checklist of data protection issues that parties and their counsel may want to consider prior to the commencement of an arbitration.

It is important to be reminded again that whenever any Arbitral Participant is covered by the GDPR, this potentially impacts the entire arbitration. This is because anyone with an EU establishment or that targets EU data subjects will need to comply with the GDPR for their own data-related activities during the course of the arbitration, *even if no one else is covered*. Furthermore, compliance with those obligations will require them to ensure that whenever data is transferred it is subject to the main provisions of the GDPR either by law or by agreement. This stresses the importance of raising data protection early in the process. [Link to EN 13]

Arbitration Agreement. Parties should consider whether to address data protection laws expressly when drafting their arbitration agreement. This could include, for example, a general obligation to comply with applicable data protection laws, especially where some of the parties to the agreement are established in the EU but others are not. It is also worth considering specific language addressing data transfer and legitimate purposes for processing.

Choice of Institution. The choice of institution may be affected by data protection rules as the activities of institutions established in the EU are subject to the GDPR to the extent that the data processing takes place in the context of those activities, whereas institutions outside the EU or organized under international law (like the PCA and ICSID) may not be subject to the GDPR themselves, although the parties to their cases may be. This can create data transfer and other challenges. For example, when parties covered by the GDPR agree to arbitration supervised by institutions established outside the EU, they should consider how data transfer will be achieved and potentially discuss with the institution whether it would be possible to put in place standard contractual clauses should a claim arise. The same issues will arise when EU institutions assign cases to their offices outside the EU or when cases are brought before the PCA or ICSID.

Choice of Arbitrator. Like the choice of institution, the choice of arbitrator may be impacted by data protection rules because the activities of arbitrators established in the EU are subject to the GDPR, whereas those from outside the EU may not be, which can create data transfer and other challenges in transferring data to non-EU arbitrators who are not subject to the GDPR. This means that when parties subject to the GDPR select arbitrators or agree on chairs not otherwise subject to the GDPR, they should address in advance whether the arbitrators are willing to enter into standard contractual clauses as a means of facilitating data transfer. Institutions subject to the GDPR may want to do the same when making arbitral appointments.

Vendor Selection and Management. Vendors may be selected based on their location and ability to assist the Arbitral Participants in complying with their obligations under the GDPR. Vendors will typically want to put in place arrangements that are consistent with being a data processor in the sense of the GDPR, in which case the data controller engaging that vendor should be aware that it is responsible for its compliance.

Preparing the Claim. When a dispute arises, the first thing that parties and their counsel typically do is to review the facts, which requires going back through the chain of events that led to the dispute. This often involves reviewing emails and other contemporary evidence of the relevant events. This evidence, which almost always contains personal data, was typically not created for the purpose of bringing a claim but rather in the ordinary course of business. The personal data would now be collected and processed for the secondary purpose of considering a potential arbitration claim.

Under the GDPR, Arbitral Participants are required to ensure that personal data is processed in compliance with the principles of purpose limitation and data minimisation.

Purpose limitation means that Arbitral Participants who collect and process personal data only process it for specific and legitimate purposes that have been notified to the data subject. Where personal data is processed to prepare for an arbitration (or during an arbitration) by Arbitral Participants who did not originally collect the data, the processing for the arbitration should not be incompatible with the initial purpose, as notified to the data subject (Art. 5(1)(b)). This means that all Arbitral Participants should consider the original purpose of the processing, as notified to the data subject, and take a view as to whether processing for the arbitration is compatible with that original purpose. If this is not the case, an additional notice would be required notifying the data subject of the new purpose.

[Link EN 18]

Data minimisation requires that the amount and type of personal data processed is adequate, relevant and limited to what is necessary for the purpose of the processing. In the context of

arbitration, the Working Party has suggested that data minimization is likely to require the culling of data before it is used as well as the redaction thereof in order to eliminate unnecessary personal data.

[Link EN 19]

These requirements may be applied, together with the legitimate interests standard, requiring the processing of data in the context of preparing for an arbitration (or during an arbitration) to be minimized to what has been notified to the data subject and required to comply with that interest. These issues arise both in preparing the claim and in responding to disclosure requests.

Data Mapping. Data mapping in the arbitration context involves determining where the data that would form the basis for the claim (and the defence) is located and where it would need to be transferred for purposes of the arbitration. This process allows parties and their counsel to develop a strategy to minimise the necessary transfers, and to put in place appropriate safeguards. For example, where data transfer to countries without adequate safeguards is required and it is not feasible to put in place appropriate safeguards, parties and counsel may be required to review, cull and potentially redact personal data in the EU before transferring a more limited data set to parties outside the EU.

c. Data Protection Principles Applicable During Arbitral Proceedings

1. Lawfulness of the Processing of Personal Data, Sensitive Data and Data Transfers

Based on the principle that every individual has the right to decide whether to allow, and to exercise control over, the processing of his/her personal data, the GDPR prohibits the processing of personal data of any data subject, unless specifically permitted on the basis of one of the legal grounds set forth in the GDPR. [Link EN 7]

Moreover, additional requirements apply to the processing of data that is considered sensitive and to data transfers outside of the EU.

Each of these principles applies separately, so, for example, the transfer of sensitive data outside the EU must comply with three separate sets of rules – (i) personal data processing, (ii) sensitive data processing and (iii) data transfer.

Furthermore, when the requirements are met to allow data processing and transfer, the processing must then comply with the mandatory rules the GDPR establishes.

i. Lawfulness of Processing Personal Data

Every data controller, including in the arbitration context, must have a lawful basis for processing the personal data under its control, and must state in its data protection notice what the lawful basis is.

The decision as to which legal basis applies is highly fact driven and case specific. The premise of the GDPR is that the processing of personal data by a third party (including during an arbitration) is prohibited unless expressly allowed by the GDPR, which is important to an understanding of how the GDPR operates and how it applies to international arbitration.

The GDPR contains no express provision allowing processing for arbitration purposes, which means that arbitral data processing will need to be justified under one of the permissible bases set forth in the GDPR.

The decision as to which basis applies is not straightforward. It is highly fact driven and case specific.

The GDPR allows processing the processing of personal data where informed consent has been obtained, but informed consent (which would need to be from the "data subjects" themselves rather than the Arbitration Participant who provides the personal data, if different) is difficult to obtain and easy to withdraw, which makes the application of this lawful basis for processing in the context of an arbitration problematic.

The lawful basis for the processing of personal data that appears best suited to arbitration is the legitimate interest of the data controller (in this case the Arbitral Participant) in processing the personal data, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data" (Art. 6(1)(f)).

This approach has been supported by the Working Party, which has taken the view that the processing of personal data in order to establish legal claims and defenses does fall within the legitimate interest of the data controller when the processing of the personal data is necessary to make out those claims or defenses, although this is not stated in the GDPR.

Where a data controller relies upon its legitimate interest as the lawful basis for processing, including in the arbitration context, it should do a legitimate interest analysis as a basis for identifying and relying on the particular interest in the first place and update that analysis during the course of the processing to ensure that the interest in question still applies to the data processing.

ii. Lawfulness of Processing of Sensitive Data

The GDPR applies special rules for the processing of "*special category data*" which is data revealing "*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 […] a natural person's sex life or sexual orientation*" (Art. 9). For example, this may include photographs on witness statements or any health information.

The lawful processing of special category data requires a lawful basis for the processing of the personal data *plus* a separate lawful basis for the processing of the sensitive data.

Processing of special category data is allowed based on express informed consent, which is a higher bar than described above for informed consent and accordingly has even more pitfalls (Art. 9(2)(f)).

Another lawful basis for processing special category data is where "*necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity*", which is likely to be best suited for processing special category data for arbitration. [Link EN 7]

The GDPR refers in several places to processing which is "*necessary for the establishment, exercise or defence of legal claims.*" [Link EN 12] In determining what this means, it bears noting that Recital 111 of the GDPR states that the legal claim necessity is not limited to court or judicial proceedings but also applies in "*administrative or any out-of-court procedure, including procedures before regulatory bodies.*"

The notion of "*out-of-court procedure*" is not defined in the GDPR, but could be construed as encompassing arbitration and other forms of ADR. In an opinion issued in the context of transfers outside the EU, the EDPB indicated that:

> The combination of the terms "legal claim" and "procedure" implies that the relevant procedure must have a basis in law, including a formal, legally defined process, but is not necessarily limited to judicial or administrative procedures ("or any out of court procedure").[5]

According to the EDPB, the word "*necessary*" requires "*a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position*."[6] ECJ case law (on the Data Protection Directive) indicates that the concept of "*necessity*" must be given its own independent meaning in EU law, to fully reflect the objectives of data protection legislation.[7] [Link EN 12]

iii. Lawfulness of Data Transfers

The GDPR establishes rules for transfers of personal data to third countries by all Arbitral Participants (whether data processors or data controllers), which apply during the arbitration process. The EU aim of subjecting data transfers to limitations is, in general, to ensure that data is always sufficiently protected, and that the rights of data subjects in relation to their data are not prejudiced by transfer out of the EU.

Before a data processor or controller can transfer personal data outside the EU, including during an arbitration, there must be a legal basis for the data transfer in addition to the lawful basis for processing. It is important to note that transfer is broadly interpreted to include, for example, any downloading of a document or an email while outside the EU.

In the context of an arbitration, data transfer often triggers Arbitral Participants to consider data protection. Whenever any Arbitral Participant is subject to the GDPR, they will have to determine a lawful basis for transfer before sending any materials outside the EU.

The GDPR allows third country data transfers where:

- the country has been deemed by the European Commission to provide adequate data protection;
- the data controller or data processor has put in place "*appropriate safeguards*" to protect the data by one of the means expressly prescribed by the GDPR; or

---

5 Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, European Data Protection Board, (2018) ("DraftTerritorial Guidance").

6 *Id.*

7 *See* Case C-524/06 Heinz Huber v. FRG [2008] ECR I-9705.

- where one of a list of specified derogations apply, including where the processing is "*necessary for the establishment, exercise or defence of legal claims*" provided that the transfer can be considered as "*occasional*" (Arts. 45-49).

Regardless of the means employed by a party to transfer personal data outside the EU, the recipient of the data must be required by law or by agreement to apply adequate protections to the data after its transfer, including the main principles of the GDPR (Art. 44). [FN]

In the arbitration context, it is important to recall that international organisations such as the Permanent Court of Arbitration, the World Bank and the International Court of Justice, which are established under international law or by an agreement between countries, are treated as though they are outside the EU (Art. 4(26) defining international organisations, Art. 46(1) addressing transfers to international organisations). This means that transfer to such organizations will require compliance with the data transfer rules.

The Working Party has indicated that the exceptions allowing data transfers follow a cascade approach, as follows:

- First, transfer may take place if there is an adequacy decision, allowing data transfers to the relevant country;

- Second, if data is to be transferred to a country without an adequacy decision, one of the expressly listed "*adequate safeguards*" must be put in place where feasible;

- Third, in case there is no adequacy decision and adequate safeguards are not feasible either, a specific derogation can be relied on; and

- Lastly, if none of the express derogations is applicable, a party may rely on its "*compelling legitimate interests*" as a basis for transfer, but this is a high standard and requires notification to the data subjects and the supervisory authority.

The same requirements apply to "*onward transfers*" from the first recipient of a data transfer to a third party, even if the two are established in the same third country unless that country is covered by an adequacy decision (Recital 101).

This means that where feasible, the data transfer rules require Arbitral Participants to enter into appropriate safeguards before a transfer is made outside the EU to a country without an adequacy decision.

One of the appropriate safeguards are the so-called standard contractual clauses developed by the EU. These standard clauses must be adopted verbatim to provide a valid legal basis for transfer. By entering into standard contractual clauses, the non-EU entity agrees to be bound by the main provisions of the GDPR as a condition of the transfer.

Where standard contractual clauses or other appropriate safeguards are not feasible, a derogation may be relied upon for transfer if express consent has been obtained or where the transfer is "*necessary*" for establishing, exercising or defending a legal claim, as discussed in the previous Section. Transfers under the legal claims derogation must also be occasional which means that they "*may happen more than once, but not regularly, and would occur outside the*

regular course of actions."[8] The standard for occasional transfers may be hard to meet in arbitrations.

The GDPR also requires the application of all third country transfer provisions in a manner that "*ensure[s] that the level of protection of natural persons guaranteed by this Regulation is not undermined*" (Art. 44). The Working Party has reiterated that when a derogation is relied on for transfer, safeguards must be put in place to ensure that the processing is carried out with an adequate level of protection and the data subject rights are not circumscribed (Art. 44). This is not required as an additional step where standard contractual clauses are put in place because the clauses themselves accomplish this.

The application of the data transfer provisions taken as a whole support the of standard contractual clauses as a basis for data transfers in the context of arbitral proceedings, if appropriate.

[Link EN 8]

2. Cybersecurity requirements

The GDPR requires all Arbitral Participants, including both data processors and data controllers, to apply adequate physical and cyber security whenever they process personal data, failing which they risk fines and other enforcement action.

The GDPR requires data controllers and processors to implement appropriate technical and organisational measures to ensure a "*level of security appropriate to the risk*" (Art. 32). This means that whenever the GDPR applies to personal data processed in an arbitration, adequate data security is *mandatory*. However, the GDPR does not define the security measures that are required for compliance.

Article 5(1)(f) of the GDPR concerns the "*integrity and confidentiality*" of personal data. It establishes the principle that personal data shall be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*."

Article 32(1) and (2) of the GDPR provides that the following measures are required to secure all data covered by its terms:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    a. the pseudonymisation and encryption of personal data;
    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

[8] *See* Draft Territorial Guidance *supra* note 5.

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Therefore, in deciding what data security measures to apply, Arbitral Participants should apply a risk based approach.

In the context of an arbitration, each Arbitral Participant including both data controllers and data subjects are required to ensure that their own data security meets the requirements of the GDPR. The GPR imposes no obligation to police the data security measures of other Arbitral Participants, provided the other Arbitral Participants are either subject to the GDPR or have entered into appropriate safeguards as a condition of data transfer. The Standard Contractual Clauses address data security, as should any appropriate safeguards entered into for the purposes of a data transfer under a derogation.

Important initiatives have been undertaken towards ensuring cybersecurity in international arbitration. These include the Debevoise & Plimpton Protocol to Promote Cybersecurity in International Arbitration launched in 2017, the ICCA/NY Bar/CPR Cybersecurity Framework for International Arbitration (2019) and the IBA Cybersecurity Guidelines (2018). While none of these initiatives address the data security requirements of the GDPR directly, they provide a useful resource for applying a risk-based analysis to cybersecurity, and the ICCA/NY City Bar/CPR Cybersecurity Framework for International Arbitration further provides a structure for how data protection may be addressed in international arbitration.

[Link to EN 11]

3. Notification requirements

Unless an exemption applies, the GDPR requires data privacy notices to be provided both by the data controller that originally collects the personal data from the data subject, and by those that receive the personal data subsequently. Most Arbitral Participants fall in the second category. This means that unless exempted, each of the Arbitral Participants will need to provide a notice to all data subjects whose personal data is processed during an arbitration.

Arbitral Participants who do not collect the data but receive from others, which will often be the case in an arbitration (with the exception of the parties), are not required to provide notice where:

- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;

- the data controller is required by law to obtain or disclose the personal data; or
- the data controller is subject to an obligation of professional secrecy regulated by EU or EU Member State law that covers the personal data.

[Link to EN 21]

While many of the exceptions to the notification requirement are potentially applicable to secondary processing by Arbitral Participants, especially when the arbitration is confidential, each Arbitral Participant will need to decide this on a case-by-case basis. Views may differ based on where the Arbitral Participant is established, where the personal data was collected, where the data subjects are located and where the data is processed.

One possibility, which has been implicitly supported by the Working Party would be for the Arbitral Participants to agree that the party that originally collected the data will provide the necessary information to the data subjects and that the other, secondary, processors would rely on those notices and potentially receive indemnities.[9] However, in deciding whether this is appropriate in the context of a specific arbitration, Arbitral Participants should consider that it could increase the risk of a finding of joint controllership, and that care should be taken to minimise the risk of creating a joint controllership that would not otherwise exist, given the potential of joint and several liability of the joint controllers. [Link to EN 14]

Many Arbitral Participants, including parties, law firms and institutions, will already have in place data protection policies and procedures, including data protection notices, with respect to their activities, some of which may address dispute resolution specifically. Other Arbitral Participants, for example independent arbitrators and smaller institutions, may be adopting data protection notices addressing their case work for the first time. Annex 5 provides the structure of a data protection notice for consideration by institutions, and Annex 6 for arbitrators, but notices are highly fact specific and require careful consideration and tailoring to each Arbitral Participant's activities and needs.

4. Data retention and destruction

Data retention and destruction are considered forms of processing under the GDPR. The GDPR requires data controllers, including Arbitral Participants, to notify the data subject at the time of data collection of the applicable retention periods or the basis on which those retention periods will be calculated, with the aim of reducing the period during which data is processed.

Arbitral Participants will need to consider what data retention period is reasonable in light of the purpose of the processing, including the arbitration itself and the enforcement of any award, as well as any attendant processing in light of, for example, undertaking conflict checks and complying with legal and regulatory obligations.

Parties should keep in mind that potential future use in an arbitration or other legal proceedings may not be a sufficient basis for parties to retain data beyond an otherwise reasonable period of time.

[9] The most relevant of the Working Party guidance for our subject is the *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 the "Document Disclosure Guidance").

Article 5(1)(e) of the GDPR provides that personal data be:

> [K]ept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes …('storage limitation').

To demonstrate compliance with this principle, organizations with more than 250 employees may need to establish and document standard retention periods for different categories of information held, a system for ensuring they are complied with, and for periodically reviewing retention. Smaller firms, chambers and independent arbitrators will need to be able to demonstrate compliance but will not need to comply with Article 30 (keeping records of processing activities) unless they are engaged in high risk processing. However, they will still be required to regularly review the data held, and to delete (or anonymise) any personal data no longer required for processing.

This means that when deciding how long it can be retained, Arbitral Participants should consider their stated purpose for the processing of the personal data in question. Arbitral Participants can retain personal data for as long as required for the lawful purpose relied on for processing.

Arbitral Participants should also consider whether they need to keep a record of the relationship with the individual once that relationship ends. The data controller may need to keep some information so that it can confirm that the relationship existed – and that it has ended – as well as some of its details. This could apply, for example, for future conflict checks.

Arbitral Participants should also consider any legal or regulatory requirements, for example, for income tax and audit purposes.

The bottom line is that Arbitral Participants, like all data controllers, should take a proportionate approach, balancing their needs with the impact of retention on the data subject. This means that data controllers, including Arbitral Participants, should:

- keep personal data for only as long as required;
- be able to justify how long they keep personal data, which will depend on the purposes for holding the data;
- periodically review the data held, and erase or anonymize it when they no longer need it; and
- carefully consider any challenges to their retention of data.

[Link EN 22]

5. Data breach notification

The GDPR contains strict notification requirements in the case of a data breach, which are likely to apply to all Arbitral Participants (Arts. 33-34) during the course of the arbitration, subject to any exemptions under national law.

Data controllers are required to notify the supervisory authorities of "*a data breach that is likely to result in a risk for the rights and freedoms of the data subject within 72 hours of discovery of the breach*" (Arts. 33-34).

Data subjects must also be notified of the breach without undue delay if the data breach "*presents a high risk for the rights and freedoms of individuals*." If the data breach only presents "*some risk*" for individuals, only the data protection authority will need to be notified and not the individual data subjects (Arts. 33-34). The data breach notification must include the cause and nature of the breach (if known) and recommendations as to how the potentially affected individuals can mitigate the risks of the breach. The burden to prove the absence of risk in a data breach rests on the data controller (Arts. 33-34). Even where no notification is required, a record of the breach must be kept.

A data breach is the most obvious manner in which arbitration may come to the attention of the supervisory authorities or trigger data subject claims. Considering the tight time lines and large fines, it will therefore be important for Arbitral Participants to consider in advance, before any breach occurs, exactly what will trigger a breach notification and the process for how data breach notifications will be given, by whom and to which authority. Given the impact that data breach may have on the arbitration process, it will be useful for Arbitral Participants to consider in advance how they will be addressed and whether coordination would be helpful.

[Link EN 21]

6. Insurance and indemnities

A personal data breach or other GDPR violation can be expensive. There will be costs involved in investigating and remedying the causes and, to the extent necessary, in notifying and corresponding with the supervisory authorities and affected data subjects. In the event of harm, civil liability may be incurred and damages may have to be paid. In addition, of course, there is the possibility that a regulator or court may impose a regulatory fine.

Hence, it is unsurprising that there are insurance products available, which might help Arbitral Participants mitigate relevant risk. Cover may also be available as part of, or as an add-on to, professional liability insurance of lawyers and others. At this relatively early stage and in the absence of any real claim experience, it is difficult for insurers properly to quantify the risk, and as a result, premiums may vary substantially.

An important point is that there is some debate about whether regulatory fines can be insured against. That is clearly a matter for the relevant national law, but in many jurisdictions, insurance against fines is illegal, or contrary to morals or public policy. It is therefore not uncommon for policies to be sold on the basis that they will cover fines "*to the extent allowed by law*".

The application of the GDPR to arbitration creates interlinking obligations, and the potential for joint and several liability in the case of joint controllership. As a result, it is important to consider the use of indemnities to allocate and minimize those risks. While there may be arguments against the enforceability of indemnities to pay fines levied against another Arbitral Participant, it would still be prudent to have such clauses in place.

d. Applying Data Protection Principles During Arbitral Proceedings

Data protection issues can arise at any stage between the start and the conclusion of an arbitration. From the moment that a file (containing personal data) is sent to an arbitrator or institution, through documentary disclosure and the filing of witness statements and expert reports, to the eventual issuance and enforcement of an award, it will be important for tribunals and parties to consider the protection of individuals whose data is involved, however tangentially.

In an institutional arbitration or where there is an appointing authority, parties subject to the GDPR should consider raising its potential impact prior to the filing of any request for arbitration with the institution as appointing authority. This would be especially necessary in cases where the filing of the request itself raises data protection concerns, for example where data transfer is required or data security is in doubt.

After the claim is filed, the arbitral institution or appointing authority may address data protection with the parties either at the initiative of the party or at its own motion. Parties may consider informing the institution in its request for arbitration or in the response (or even beforehand) about data protection issues that may arise and indicating how those issues may have an impact on the arbitral process. For their part, institutions and/or appointing authorities may wish to consider the extent to which data protection issues arise in the context of, *inter alia,* the receipt of a request for arbitration, the registration and/or administration of arbitrations, the appointment of arbitrators, the receipt and holding of advances on the arbitration and administrative costs, and the transfer of data to parties, their counsel and arbitrators.

After the arbitral tribunal is constituted, the parties and arbitrators can also raise any data protection issues directly with each other. If data protection has not already been addressed or fully addressed, it is good practice to include the topic on the agenda of the Case Management Conference or first procedural meeting and address the relevant issues at that occasion. This will allow the parties, counsel and the tribunal (where necessary in conjunction with the institution) to consider at the outset of the proceedings how the applicable data protection regime(s) will play out in the context of that particular arbitration. Additional complications may arise with defaulting parties.

1. Risk-based approach and record-keeping

The GDPR requires data controllers, including in the context of arbitration, to apply a risk-based approach to compliance and to be able to demonstrate compliance.

The risk-based approach to compliance with the GDPR will necessarily mean balancing, in the context of an arbitration, a data subject's data protection rights with the parties' fundamental rights, including the right of defence and the right to due process (Arts. 47 and 48 of the Charter of Fundamental Rights of the European Union). The requisite balancing of interests under the GDPR emphasizes the need to consider these issues early so these rights can be catered for in the process. [Link to EN 16]

The GDPR requires that controllers of data not only comply with the GDPR, but that they also retain a record of that compliance. The obligation to document compliance is further detailed in Article 30, which does not apply to SMEs with less than 250 employees. This makes it

important that decisions on data protection issues be documented, including the rationale for the decision. [Link to EN 17]

During the arbitration process (as well as beforehand), it will be up to each Arbitral Participant to ensure that they both comply with their obligations and keep adequate records demonstrating compliance. It may be useful for Arbitral Participants to consider in advance how they will be comply with their record-keeping obligations and whether coordination would be helpful.

The remainder of this section will consider how data protection issues may arise in the context of an arbitration proceeding. Annex 4 provides a checklist of issues all Arbitral Participants should consider during the arbitration process.

2. Procedural mechanisms

After consultation with the parties, where appropriate, language addressing compliance with the applicable data protection laws may be included in:

- the terms of reference (where applicable);
- a first procedural order and/or subsequent orders;
- a data protection protocol or other agreement addressing data compliance issues affecting all Arbitral Participants who process personal data during the arbitration; and/or
- to the extent not covered in the first procedural order, the procedural orders governing the taking of evidence in general and the disclosure phase in particular.

Issues that may be addressed through such procedural mechanisms include, among other things, the necessity for data protection notices, cybersecurity measures, the impact of data protection on the taking of evidence, data breach notifications, and the allocation of roles and responsibilities with respect to compliance with data subject rights. Annex 4 contains a checklist of items to be considered in thinking about how the GDPR may impact the arbitration.

In complex cases, the Arbitral Participants may wish to consider using a data protection protocol. The decision of whether to employ a data protection protocol, and more generally, the extent to which the tribunal should be involved in the management of the Arbitral Participants' respective data protection obligations, should be evaluated taking into account all the circumstances.

In certain circumstances, it may be necessary or appropriate for the arbitral tribunal to become involved in data protection compliance mechanisms. This may also increase the efficiency of the arbitration and ease the Arbitral Participants' compliance burden. However, at the same time, these sorts of arrangements (for example allocating responsibility for providing data protection notices to certain Arbitral Participants) could increase the likelihood that Arbitral Participants are considered to be joint controllers, with attendant joint and several liability. This highlights the importance that such procedural mechanisms include appropriate indemnities, and that potential insurance options are considered.

[Link to EN 14]

3. Taking of evidence

None of the major arbitration rules address the manner in which data protection is to be handled in the context of an arbitration. Neither the 2010 version of the IBA Rules on the Taking of Evidence in International Arbitration (the "IBA Rules"), nor other guidance on the organisation of arbitration proceedings address the impact of data protection rules on the arbitral process. Conversely, data protection rules (including the GDPR) do not expressly deal with their application in international arbitration nor has any guidance been issued in their respect. The recently issued ICC "*Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration*" effective as of January 1st, 2019, does address the GDPR generally, but without any specific indication as to how its application might affect the arbitral process.

This leaves Arbitral Participants to decide in each case whether and how applicable data protection rules may limit the ways in which they can gather, process, use, transfer, and protect personal data and the means by which the rights granted to data subjects will be respected, and how those efforts should be documented. A case-by-case determination has the benefit of allowing the process to be tailored to potentially applicable data protection and other laws.

Consistent with the approach adopted in the IBA Rules on the Taking of Evidence in International Arbitration, the question whether and how data protection issues may have an impact on the taking of evidence ought to be addressed early.[10] If not addressed earlier, it is good practice to discuss the issue during the case management conference or first procedural meeting. In addition to minimizing general data protection risks and avoiding surprises, this practice fosters compliance and encourages data protection concerns to be voiced at the outset, rather than later on in the proceedings (for example in response to a disclosure request), which could cause unnecessary costs and delays.

Insofar as personal data is concerned, the GDPR may affect the volume and nature of disclosure, requiring among other things that the processing of personal data be minimized and limited to what is necessary for the purpose of the arbitration. When sensitive data is being disclosed, or insofar as data is being transferred (to a country without an adequacy decision and without appropriate safeguards), the personal data that can be processed or transferred will often be limited to that which is necessary for "*the establishment, exercise or defence of legal claims*" (Art. 17, Recital 65).

In the context of discovery for US litigation, the Working Party has stated that "*there is a duty upon data controllers involved in litigation to take such steps as are appropriate (in view of the sensitivity of the data in question and of alternative sources of the information) to limit the discovery of personal data to that which is objectively relevant to the issues being litigated. There are various stages to this filtering activity including determining the information that is relevant to the case, then moving on to assessing the extent to which this includes personal data. Once personal data has been identified, the data controller would need to consider whether it is necessary for all of the personal data to be processed, or for example, could it be produced in a more anonymised or redacted form.*"[11]

[10] IBA Rules on the Taking of Evidence in International Arbitration (International Bar Association) 2010; Commentary on the Revised Text of the 2010 IBA Rules on the Taking of Evidence in International Arbitration (2010).
[11] Document Disclosure Guidance, supra note 9.

When the GDPR applies to the personal data being processed during an arbitration, data minimization is mandatory (Recital 39). However, it is important to keep in mind that the GDPR is not concerned with the amount and volume of data that is exchanged, just the extent to which it includes personal data. Therefore, this would mean that personal data should be reviewed first for relevance and whether it is "*necessary*" to make out the claim. If so, the question is whether personal data that is not necessary for the arbitration (including names, email addresses, and all other data by which an individual is or could be identified) can be redacted.

The Working Party has expressed the view that parties "*have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought*"[12]. Issues to be considered by tribunals in balancing competing interests may include, among others, procedures aimed at limiting data protection exposure though data protection protocols and other risk-reducing procedures, reasonable measures to avoid unnecessary third country data transfers, the objecting party's previous treatment of data, pseudonymization where feasible, the scope of the compliance risk, and the importance of the data for the arbitration.

The Working Party and the EDPB favour redaction of personal data and encryption. Technology clearly makes both the culling and redaction of personal data feasible. However, even with technological advances, redaction measures may be expensive to apply and time consuming (and hence more costly and slower) to work with. It remains to be seen in practice, following the entry into force of the GDPR, to which extent redaction takes place earlier and becomes more widespread.

It is worth noting that the approach suggested by the Working Party is consistent with the IBA Rules,[13] but may limit the personal data likely to be disclosed by limiting the disclosure itself and requiring more extensive redaction of personal data (only) when the principles suggested by the Working Party are applied robustly. [Link EN 20]

4. Compliance with Data Subject Rights

During the arbitration process, Arbitral Participants will also be required to respect the data subjects' rights with respect to their personal data.

The GDPR requires data controllers, including Arbitral Participants, to put in place a system to address any concerns raised by data subjects and to notify them of how these rights can be exercised. Given the impact that the exercise of these rights may have on the arbitral process, it will be useful for Arbitral Participants to consider in advance how they will be addressed and whether coordination would be helpful.

Arbitral Participants may potentially receive requests from data subjects seeking to exercise their rights. These may come from any individual whose personal data is handled during the arbitration process, including but not limited to individual parties, witnesses, experts, or even persons not directly involved in the proceedings but about whom personal data has been adduced (e.g., an employee of a party but who is not involved in the proceedings directly). In order to limit potential disruption during an arbitration, Arbitral Participants may wish to discuss at the outset of the arbitration how GDPR compliant access requests will be handled.

[12] Id. at 1.
[13] See supra note 11.

The most likely rights to be enforced are the rights of access through so-called data subject access requests and the right to rectify any data that is inaccurate. These data subject rights requests may be aimed at obtaining data to be used in the arbitration and can raise important issues of confidentiality and privilege, among other things.

The GDPR provides that the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to a broad range of information about that processing. There is a risk that such requests are (ab)used to derail the arbitral process.

Arbitral Participants should be aware that upon receipt of a valid data subject access request, they must provide an individual with access to their personal data that they hold. However, the exercise of that right should not adversely affect the rights or freedoms of others (Art. 15(4)). This may include (but is not necessarily limited to) any potential adverse impact on data protection rights, trade secrets and intellectual property (*see e.g.,* Recital 63).

Therefore, when assessing a data subject access request, Arbitral Participants should consider carefully what impact meeting the request might have on others (both Arbitral Participants and third parties). This may include identifying and implementing steps to reduce any potential adverse impact. For example, where appropriate, Arbitral Participants might redact personal data relating to other individuals or ensure they restrict the documents produced to those (or portions of them) strictly necessary to meet the exact terms of the data subject's request rather than adopting a blanket (and likely less time consuming) approach to responding.

National courts have also suggested that striking a balance between different stakeholders' interests might involve obtaining undertakings to restrict the onward transfer of any information disclosed in response to the subject access request.[14] Adopting a tailored approach balancing different stakeholders' rights can be time consuming, but is the best way to ensure that competing rights are respected while allowing the Arbitral Participant to comply with a data subject access request.

Arbitral Participants should in all cases consult relevant national laws for any relevant derogations from the GDPR with respect to individual data subject rights requests. The GDPR permits derogations in this area and many national laws tailor (and curtail) the GDPR considerably in specific circumstances. For example, Ireland has adopted an exemption from certain individual rights, which covers out-of-court procedures.

Data subject right requests may be particularly problematic if aimed at gaining access to information about the deliberations or decision-making process of tribunals. Applying the balancing of interests in a concrete arbitration, a tribunal may well come to the conclusion that a data subject access request that would breach the secrecy of tribunal communications is to be rejected.

[EN 22]

[14] *B v General Medical Council [2018] EWCA Civ 1497, 28 June 2018 (UK).*

5. Arbitral awards

Arbitral awards are likely to contain personal data. Moreover, even in confidential arbitrations, there is a risk that the award will become public if it is enforced in a country where awards (or parts thereof) become public in the enforcement process. Institutions increasingly publish awards (or excerpts thereof) as a matter of course unless the parties object. Arbitrators should therefore consider the basis and necessity for including personal data in the award and may want to raise this issue with the parties. In some countries it is standard practice to redact personal data even from court decisions.

Depending on the circumstances of a particular case, the alleged failure to comply with mandatory data protection principles could also conceivably form a basis for challenging the award. In the line of cases starting with *Eco Swiss*, the ECJ has taken the view that an EU national court must refuse recognition and enforcement of an arbitral award if the tribunal failed to comply with mandatory EU rules. The ECJ has applied this principle in the competition context, certain aspects of EU agency and distribution law, and consumer protection laws. A similar approach could be taken in relation to the data protection principles enshrined in the GDPR, which find their basis in the European Charter of Fundamental Rights (Case C-126/97 Eco Swiss [1999] ECR I-3055; Case C-168/05 Mostaza Claro [2006] ECR I-10421).

Therefore, apart from the other issues raised in this Roadmap, a tribunal seeking to render an award that is enforceable should consider the potential impact of procedural decisions on, and the inclusion in the award of, personal data in a manner which complies with the applicable data protection law.

[Link EN 3]