# ASA BULLETIN

**Founder:** Professor Pierre LALIVE
**Editor in Chief:** Matthias SCHERER

**Published by:**
Kluwer Law International
PO Box 316
2400 AH Alphen aan den Rijn
The Netherlands
e-mail: lrs-sales@wolterskluwer.com

## Aims & Scope

Switzerland is generally regarded as one of the World's leading place for arbitration proceedings. The membership of the Swiss Arbitration Association (ASA) is graced by many of the world's best-known arbitration practitioners. The Statistical Report of the International Chamber of Commerce (ICC) has repeatedly ranked Switzerland first for place of arbitration, origin of arbitrators and applicable law.

The ASA Bulletin is the official quarterly journal of this prestigious association. Since its inception in 1983 the Bulletin has carved a unique niche with its focus on arbitration case law and practice worldwide as well as its judicious selection of scholarly and practical writing in the field. Its regular contents include:

- Articles
- Leading cases of the Swiss Federal Supreme Court
- Leading cases of other Swiss Courts
- Selected landmark cases from foreign jurisdictions worldwide
- Arbitral awards and orders under various auspices including ICC, ICSID and the Swiss Chambers of Commerce ("Swiss Rules")
- Notices of publications and reviews

Each case and article is usually published in its original language with a comprehensive head note in English, French and German.

### Books and journals for Review

Books related to the topics discussed in the Bulletin may be sent for review to the Editor (Matthias Scherer, LALIVE, P.O. Box 6569, 1211 Geneva 6, Switzerland).

## ASA Secretariat


4, Boulevard du Théâtre, P.O.Box 5429, CH-1204 Geneva,
Tel.: +41 22 310 74 30, Fax: +41 22 310 37 31;
info@arbitration-ch.org, www.arbitration-ch.org

**CORRESPONDENCE**

**ASA Bulletin**
Matthias SCHERER
Rue de la Mairie 35, CP 6569, CH-1211 Genève 6
Tel: +41 58 105 2000 – Fax: +41 58 105 2060
mscherer@lalive.law

(For address changes please contact
info@arbitration-ch.org/tel +41 22 310 74 30)

Published by Kluwer Law International
P.O. Box 316
2400 AH Alphen aan den Rijn
The Netherlands

Sold and distributed in North, Central and South America by Aspen Publishers, Inc.
7201 McKinney Circle
Frederick, MD 21704
United States of America

Sold and distributed in all other countries by Air Business Subscriptions
Rockwood House
Haywards Heath
West Sussex
RH16 3DH
United Kingdom
Email: international-customerservice@wolterskluwer.com

ISSN 1010-9153


This journal should be cited as ASA Bull. 4/2019

The ASA Bulletin is published four times per year.
Subscription prices for 2020 [Volume 38, Numbers 1 through 4] including postage and handling: 2020 Print Subscription Price Starting at EUR 391/ USD 518/ GBP 287.

This journal is also available online at www.kluwerlawonline.com.
Sample copies and other information are available at lrus.wolterskluwer.com

For further information please contact our sales department at +31 (0) 172 641562 or at international-sales@wolterskluwer.com.

For Marketing Opportunities please contact international-marketing@wolterskluwer.com



Printed on acid-free paper

# Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance

DAVID ROSENTHAL[1]

*Arbitration – Arbitral Tribunal – Arbitrator – Data Protection – General Data Protection Regulation – GDPR – Data Protection Act – Privacy – Confidentiality – DPA*

## Introduction

Arbitration professionals are usually unaware of data protection and data protection specialists usually do not know much about international arbitration. It thus comes as no surprise that there is hardly any real practical guidance on how to combine the two, in particular in view of the EU General Data Protection Regulation (GDPR),[2] although there are some efforts in the community to change this.[3] This article will hopefully contribute to this change, as it is written on the basis of practical experience in both fields. It comes with a template as a practical example on how to implement the recommendations herein.[4] The article focusses on basic data protection compliance under the GDPR (excluding EEA Member State law[5]) and how to achieve it, at least on the face of it. While the level of data protection is not bad in international arbitration in our experience, everybody should be clear: Full

1 lic. iur., david@rosenthal.ch, Counsel at Homburger, Switzerland (until November 2019).
The author wishes to thank Stefanie Pfisterer, Wolfgang Junge, Gabrielle Nater-Bass, Felix Dasser, Barbara Epprecht and David Vasella for their contributions to this article and the template.

2 See, for instance, N 80 et seqq. of the ICC "Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration" (https://bit.ly/2K4bpNa) and the DIS "FAQ Datenschutz für DIS-Schiedsverfahren" (https://bit.ly/2NTTzxA, in German).

3 See, e.g., the ICCA-IBA Joint Task Force on Data Protection in International Arbitration Proceedings (https://bit.ly/34Lrtv7).

4 Under the free Creative Commons "Attribution 4.0 International (CC BY 4.0)" license; see www.rosenthal.ch/downloads/ArbitrationDPA.docx or www.homburger.ch/dataprotection for an electronic version and updates.

5 In various areas of the GDPR, Member States are permitted to provide for additional exceptions and other provisions on data protection that may be relevant for arbitration. In Germany, see for example §§ 24, 29, 32 and 33 BDSG.

compliance with the GDPR is not possible. Nobody fully complies with it, not even the data protection authorities do. Also, the likelihood that one of them will intervene is not high in international arbitration. There are many areas of higher priority. That said, we believe that with the GDPR and the threat of heavy sanctions everybody in arbitration should use their best efforts to comply with its concepts and have the paperwork in place to document it. Both is not too difficult and will not really change how we handle arbitration proceedings.

## Topic No. 1: Applicability of the GDPR

### 1. Challenge

The first topic to assess in every international arbitration is whether the GDPR will apply. There is no general exemption for arbitral proceedings, except for certain non-electronic processing of data.[6] The seat of the arbitration is usually not relevant to determine whether the GDPR will apply. Therefore, the question has to be answered with regard to each person involved in the arbitration separately, *i.e.* for every arbitrator[7], party, counsel, witness, expert and other individual or organization involved. For example, it is possible that only one of three arbitrators is subject to the GDPR. Likewise, it is possible that the parties to the arbitration are not subject to the GDPR but their counsel or other relevant persons are. As a rule of thumb, each person with its *seat or domicile in the European Economic Area* (EEA) is subject to the GDPR.[8] This is why the ICC in Paris is so interested in GDPR compliance: It is always subject to the GDPR. As opposed to that, the Swiss Chambers' Arbitration Institution is never subject to the GDPR. Individuals and organizations located *outside the EEA* may become subject to the GDPR under certain conditions, as well, but they are usually not triggered in international arbitration; they concern companies that create profiles of individuals in the EEA by tracking them or that target *individuals* (as opposed to companies) in the EEA for providing them with goods or services.[9]

Hence, in most arbitrations there will be at least some stakeholders who are subject to the GDPR. Under the GDPR, they are required to ensure

---

6 Art. 2(1) GDPR.

7 This may be the individual as such (where acting as a "private" arbitrator, as typically arbitrators using a barrister's or judge's chamber) or his or her law firm (where acting for its law firm, even under an *ad personam* mandate).

8 Art. 3(1) GDPR.

9 Art. 3(2) GDPR; for instance, the GDPR will not apply if a Swiss attorney upon request accepts a mandate as counsel or arbitrator in a dispute involving a private client in the EEA; however, if the Swiss attorney had advertised himself in the EEA for assignments by EEA private clients, the GDPR may apply.

that any processing of personal data under their control complies with the GDPR. In data protection, the term "processing" means any activity involving personal data[10] and "personal data" any information about an identified or identifiable individual.[11] Hence, any handling of e-mails, letters, contracts or other documents or piece of data that contains the name, an e-mail-address or other information that allows a reader to identify the individual mentioned (who is referred to as the "data subject") is subject to the GDPR. For instance, if only one arbitrator on a panel of three is subject to the provisions of the GDPR for those in the EEA, the jointly controlled processing activities of all three co-arbitrators have to comply with the GDPR, as the one arbitrator located in the EEA could otherwise be fined or face civil claims from data subjects. This joint liability will be further discussed under Topic No. 2.

## 2. Solution

There are two possible solutions to the applicability of the GDPR. The first one is to avoid it altogether. If the parties to a contract are themselves not subject to the GDPR, they can "escape" from the GDPR by agreeing on arbitrators and party counsel who are not subject to the GDPR. If they choose counsel and arbitrators from Switzerland and other non-EEA countries, the GDPR does not apply to their processing of personal data (witnesses, experts, party affiliates and the arbitral institution in the EEA may nevertheless be subject to it). If the seat of the arbitral tribunal is in Switzerland, then they may be able to avoid even the Swiss DPA in the future: Switzerland is currently revising the DPA along similar lines as the GDPR. However, contrary to the GDPR, the Federal Council has suggested that the scope of the current draft bill[12] should be interpreted to exclude proceedings of arbitral tribunals with their seat in Switzerland.[13] Hence, from a data protection point of view Switzerland will become even more attractive for international arbitration.

The second solution to the applicability of the GDPR to an arbitration is to have all core stakeholders, *i.e.* arbitrators, parties and their counsel, agree on a minimum standard of data protection where their activities overlap, for

---

10 For example, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 Nr. 2 GDPR).

11 Art. 4 Nr. 1 GDPR.

12 Art. 2 para. 3 Draft Swiss DPA (as per the September 2019).

13 BBl 2017 7013; the rationale of this is that, instead, the applicable procedural rules would (have to) ensure an adequate level of data protection.

instance by entering into a data protection agreement.[14] In fact, as shown under Topic No. 2 and No. 3, such an agreement is mandatory where even only participant in an arbitration is subject to the GDPR.

## Topic No. 2: Joint Controllership

### 1. Challenge

Under the GDPR, the primary responsibility for complying with it is upon the person having *control* over a particular processing of personal data. This person is the "controller". Control is defined as deciding over the purpose of a processing activity or its essential means,[15] *i.e.* the aspects of a data processing activity that are relevant from data protection point of view. Such aspects are, for example, the kind of data to be processed, how this is to be done, for how long and by whom, and with whom it may be shared with.[16] In practice, such control is often shared among various people or organizations. Where this is the case, they become "joint controllers". It is not necessary that all decisions are taken together to become a joint controller. Even if a party has no access to the personal data at issue, but contributes to certain decisions concerning its processing, it is likely a joint controller. The European Court of Justice (ECJ) has issued various decisions on this point and has been quick in assuming joint controllership.[17]

The consequences of being a joint controller are two-fold: First, a joint controller is jointly liable with all other joint controllers for violations of the GDPR, even if the other joint controllers themselves may not be subject to the GDPR[18], unless the joint controller can show that it had no influence on the

---

14 For instance, if a stakeholder is from a non-European country that has a data protection law of its own, the other stakeholder may be likewise be required to ensure that the arbitral proceeding complies with it. For instance, if a stakeholder is from Switzerland, but the arbitral tribunal does not have its seat in Switzerland, such stakeholder is required to comply with Swiss data protection law, and other stakeholders in the arbitration contributing to its processing activities may become jointly liable.

15 Art. 4 Nr. 7 GDPR.

16 David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019 (www.jusletter.ch), N 33.

17 See, ECJ Decision of June 5, 2018 (C-210/16, "Facebook-Fanpage"), ECJ Decision Juli 10, 2018 (C-25/17, "Jehovah's Witnesses"), ECJ Decision of Juli 29, 2019 (C-40/17, "Fashion ID"); for a discussion of the two former decisions, see Rosenthal (op. cit.), N 71 et seq., N 76 et seq. See also the Article 29 Data Protection Working Party "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)" (WP128), discussed in Rosenthal (op. cit.), N 90 et seq.

18 Art. 26(3) GDPR.

breach whatsoever.[19] Second, Art. 26 GDPR expressly requires that all joint controllers enter into an agreement among them that determines their individual responsibilities for compliance with the GDPR.[20] Moreover, the essence of this arrangement needs to be shared with any data subject who asks for it.[21] Being a joint controller is, thus, not very attractive.

In order to apply this in practice, one needs to determine the persons in control of each processing activity of a typical arbitration. The most important activity is the keeping and management of the *arbitration file*. Despite a copy of the file (containing the parties submissions, exhibits, witness statements and other documents issued) is maintained by each party, counsel and arbitrator (and the arbitral institution) itself, the *decisions* over its purpose and essential means (what is to be included in it, how long it should be kept, who may contribute to it in which manner, etc.) is usually a joint decision by *all* stakeholders, *i.e.* each arbitrator individually, the parties and their counsel. There have been authors in the arbitration community who have held that only the arbitrators or the sole arbitrator decide over the purpose and the essential aspects of the arbitral file and other aspects of an arbitration.[22] It is argued that the arbitrators are to run the proceedings in an independent manner and have the power to issue procedural orders, which is why the other stakeholders should be regarded as controllers of their own, with no joint liability.

This is, of course, the outcome that many in the arbitration community would wish for. However, in our view it does not consider the legal framework nor reality in international arbitration. First of all, many arbitration laws and arbitration rules provide that the parties determine the procedure, and that the arbitral tribunal is only empowered to do so in the absence of an agreement by the parties.[23] Moreover, controllership by the arbitrators only does also not reflect reality in international arbitration – and, as the ECJ has made clear, only *reality* counts in these questions:[24] In our experience, there is hardly an arbitral tribunal that decides alone on the arbitral file.[25] Where parties and arbitrators

---

19 Rosenthal (op. cit), N 78, with a further reference.

20 Art. 26(1) GDPR.

21 Art. 26(2) GDPR.

22 See Martin Zahariev, Data Protection in Commercial Arbitration: In the light of GDPR, Riga/Latvia 2019, and his blog report "GDPR Issues in Commercial Arbitration and How to Mitigate Them", Kluwer Arbitration Blog, September 7, 2019 (https://bit.ly/32tgF3m); see also DIS "FAQ Datenschutz für DIS-Schiedsverfahren" (https://bit.ly/2NTTzxA, in German), item 10.

23 Cf. e.g. Art. 182 of the Swiss Private International Law Act.

24 See footnote 17; Rosenthal (op. cit.), N 25, N 71 et seqq.

25 Which term shall include all submissions made by the parties, including evidence, witness statements, expert reports, transcripts, document productions and other communications.

agree on Terms of Reference, they most of the time take joint decisions about key aspects of the arbitral file from a data protection point of view, such as the stakeholders involved in the processing of the data (*e.g.*, counsel), where copies of the file will be processed, how long they are to be kept or what measures need to be taken to protect them. Further joint decisions are made with the first procedural order, which usually sets out how submissions are to be made by whom, including evidence, witness statements and expert reports, the rules for document productions and other aspects of that involve the processing of personal data such as hearings or the redaction of certain content. Other joint decisions may occur during the proceedings, for example where a *Redfern* schedule is used.[26] While the arbitral tribunal may have the final word in many areas, it will usually consult with the parties and decide on the basis of what they submit or agree upon. If the parties reasonably agree on a particular aspect with regard to the processing of personal data, an arbitral tribunal will usually comply. This kind of involvement of each party goes well beyond what cause data protection authorities and courts to assume joint control.[27] Based on their standards, one will actually even have to consider counsel being in joint control, given that they are the ones who often take the lead in making the relevant decisions, even if acting under instruction of their clients. Among data protection specialists, it is already well established that attorneys-at-law are in most cases considered (joint-)controllers for their other client work.[28]

Hence, it has to be reasonably assumed that the parties, their counsel as well as each individual arbitrator or sole arbitrator will be regarded as joint controllers with regard to the arbitral file.[29] The fact that each stakeholder holds its own copy of the file is irrelevant, because it remains within the group who decides on the purpose and essential means of the processing. The same should be assumed for the processing of personal data to take place during any hearings. As opposed to that, the two areas of a typical arbitration proceeding most likely controlled by the arbitrators alone are the proceeding's procedural administration (apart from the administration done by the arbitral institution) and the drafting of the award, but it is also possible to consider the entire proceeding (i.e. all four areas) as a jointly controlled processing of personal

---

[26] Which is considered to be part of the processing activity herein referred to as the "arbitral file".

[27] See the footnote 17, in particular the SWIFT case, where banks influenced SWIFT decision through various committees and where, therefore, considered joint controllers (Rosenthal, op. cit., N 92).

[28] This is because they themselves decide on how to process the data for fulfilling their mandate, even if the client sets the purpose and eventually becomes a joint controller with them (Rosenthal, op. cit., N 28 et seq.).

[29] Cf. also Rosenthal (op. cit.), Annex.

data. As opposed to that, the arbitral institutions are typically processing personal data as sole and not as joint controllers.

## 2. Solution

The safe solution for the parties, their counsel and the arbitrators is to enter into a data protection agreement that fulfills the requirements of Art. 26 GDPR. Attached to this article is a template for such agreement. Our template has been drafted with the purpose of being minimally invasive to the arbitral proceedings. A procedural order will not be sufficient because it is not legally binding and enforceable upon the parties, let alone upon counsel and the arbitrators, who need to be bound as well. While it is possible to have the agreement included in Terms of Reference, we recommend a separate agreement to be concluded at the same time or as soon as possible thereafter.

The agreement can, of course, not protect joint controllers from claims for violation of the GDPR; they remain jointly liable.[30] The lack of an agreement is, however, itself a violation of the GDPR and can be fined.[31] Furthermore, the agreement may protect a joint controller from fines and other actions by the supervisory authorities for GDPR breaches by other joint controllers[32] and may serve as a legal basis for recourse. We did on purpose not include any clauses on liability or indemnification in the template, but they can be added as needed. Note that Terms of Reference often already contain indemnifications and liability limitations in favor of the arbitrators.[33]

Since there will be resistance in the arbitration community to accept that joint controllership extends beyond the arbitrators, each stakeholder will have to assess the "risks" of entering into such an agreement. If a stakeholder is subject to the GDPR, we believe the agreement will, in any event, provide protection because the acts and omissions of the other players[34] can result in data protection claims regardless of whether they are a sole or joint controller. This is why data protection agreements are commonplace even in the absence of joint controllership. Complying with the GDPR's transborder data flow requirements is another reason for having the agreement (see Topic No. 3 below).

If a stakeholder is not subject to the GDPR (or similar data protection laws), entering into a data protection agreement will force it to comply with data protection provisions that would otherwise not apply to it. However, having an

---

30 Art. 26(3) GDPR.

31 Art. 83(4) GDPR.

32 Rosenthal (op. cit.), N 79, with further references.

33 However, the Terms of Reference are usually not entered into in the name of counsel itself, whereas the data protection agreement usually should include counsel as a party to it.

34 Such as a document containing personal data submitted in violation of the GDPR.

agreement will help to establish a level playing field among the parties and thus prevent arguments of an opposing party not to produce certain documents for data protection reasons. An agreement will also provide additional protection for those not subject to the GDPR, in particular if the arbitrators happen to violate the GDPR and were, therefore, to raise indemnification claims against both parties. Should one stakeholder refuse to sign the agreement, it can still make sense for the others to sign it, as they can document their efforts to comply and do so at least with the other stakeholders. We would expect that at one point of time, arbitrators and arbitral institutions will require parties to sign data protection agreements of some kind.

## Topic No. 3: International Data Transfers

### 1. Challenge

Under the GDPR and other data protection laws, it is normally not permitted to make available personal data to recipients outside the EEA countries if they are not subject to an adequate level of data protection.[35] Transfers within Europe and among a selected number of countries with comparable data protection laws are usually no issue.[36] However, in an international arbitration, documents and other forms of personal data are often shared with recipients in other countries, such as the U.S.,[37] Singapore, India or China. This may eventually also include the UK in the case of a "hard" Brexit pending an adequacy decision.[38]

In these cases, there are basically two ways forward: The first way is for the sender (*e.g.*, the counsel, who wishes to send a submission to an arbitrator in Hong Kong) to require the recipient (*e.g.*, the arbitrator) to enter into a special kind of data protection agreement provided for by the European Commission[39] and known as the "EU Model Clauses" or "Standard Contractual Clauses".[40] Under the GDPR, they have to be used as they are, with no changes. Although

---

35 Art. 44 et seq. GDPR.

36 See https://bit.ly/2PXE9el for a list of countries considered having adequate data protection laws from a GDPR perspective.

37 Insofar the recipient is not self-certified under the "Privacy Shield" framework, a scheme provided for by the EU and Switzerland with the US to allow certain US companies to be considered as recipients acting under an adequate level of data protection once they have self-certified that they will comply with basic principles of data protection (https://www.privacyshield.gov/).

38 I.e. the European Commission formally declaring that the UK is considered a country with an adequate level of data protection (see also https://bit.ly/34WMG5h).

39 Art. 46(2) GDPR.

40 https://bit.ly/32sPO7n.

the EU Model Clauses are today widely accepted, we consider them as too complicated for most situations of an international arbitration. We would use them primarily in cases where service providers are to be retained, for instance in the case of a court reporter mandated by the parties.

The second way forward is provided for by Art. 49(1)(e) GDPR. It permits transfers of personal data to countries without an adequate level of data protection insofar they are "necessary for the establishment, exercise or defense of legal claims". In our view, this is the preferred legal basis for sharing personal data among parties, counsel and arbitrators across borders and to provide personal data to witnesses, experts and other persons appearing in an international arbitration. The Swiss DPA has a similar provision.[41] It is regularly relied on also when producing personal data in foreign state court litigations, for example in connection with pre-trial discovery productions in the U.S. However, in order to be able to rely on this provision, it is necessary that (a) only personal data that is necessary for the proceedings is disclosed, (b) the recipient keeps it confidential, and (c) the recipient will not use it for any purpose other than the proceeding (and related actions, such as an appeal).

## 2. Solution

All three conditions required by Art. 49(1)(e) GDPR can be easily accommodated for with a suitable data protection agreement to be entered into by the parties, their counsel and the arbitrators. The agreement shall provide for the obligation that each party should only submit personal data that is necessary for the proceedings, to keep such personal data confidential, and use it only for the arbitration and related purposes.[42] Because the agreement is only entered into by the parties, their counsel and each arbitrator, these obligations have to be extended to anybody who will be granted access to personal data during the proceedings. This includes, for example, witnesses and party-appointed experts. We have included a sample confidentiality statement in our template, too. We recommend that everybody signs it, not only those in countries without an adequate level of statutory data protection.

At least witnesses are not regularly asked today to sign confidentiality undertakings in arbitrations. To the contrary, in the U.S. it is quite common to do so in connection with what is referred to as "protective orders", *i.e.* confidentiality agreements entered into by the parties to a litigation and so ordered upon them by the court. In order to safeguard personal data from

---

41 Art. 6(2)(d) DPA.

42 Technically, only the stakeholders in countries without an adequate level of data protection need to be contractually bound by these obligations, but distinguishing the various cases may not be practical and raise additional questions.

Europe, these protective orders are usually expanded to apply not only to business secrets (which was their original purpose), but also to any kind of personal data.[43] In U.S. arbitrations, a similar format is used. These protective orders usually require witnesses to sign similar confidentiality declarations.

We have included provisions relating to the three requirements under Art. 49(1)(e) GDPR. In particular, we have also included confidentiality obligations in our template as a standard element because confidentiality is sometimes not provided for in international arbitration in an enforceable manner or only partly. Again, it is not sufficient for the arbitral tribunal to rule on this aspect in a procedural order,[44] given that such decisions are not legally binding upon the parties and even less on other persons involved in an arbitration. Yet, in the context of Art. 49(1)(e) GDPR, confidentiality is required only with regard to personal data, not data in general. Hence, documents submitted by a party are not subject to confidentiality insofar they do not contain personal data or such personal data has been redacted.

## Topic No. 4: How Personal Data may be processed

### 1. Challenge

The GDPR provides for various principles to be complied with when collecting, using, storing or otherwise processing personal data. At least from a European point of view, these rules are intuitive and complied with automatically when processing personal data of others in a considerate manner. These principles are the "core" of data protection, as they shall ensure that nobody feels "too" bad if data about him or her is processed, or at least understands why this is necessary. Notably, they have been in place for decades – the GDPR has not changed them.

According to these basic rules, personal data should only be processed for the purpose for which it was collected, which should be transparent to the data subject, and, of course, legitimate and reasonably acceptable to the data subject.[45] As a special requirement under the GDPR, each processing needs to have a "legal basis", *i.e.* a sufficiently good reason why the personal data is to be processed. The GDPR defines which legal grounds are acceptable depending on the sensitivity of the data at issue.[46] For normal data, the four legal grounds

---

43 The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition), including a Model U.S. Federal Court Protective Order covering data protection (for more information, see https://bit.ly/2qE2zyE).

44 For instance, as set forth by Art. 22(3) ICC Rules of Arbitration.

45 Art. 5(1)(a) and (b) GDPR.

46 Art. 6, 9 and 10 GDPR.

mostly relied on are the data subject's consent, conclusion or performance of a contract with the data subject, a legal obligation under EEA law or "legitimate interest". The latter requires a balancing of interest test, which means that one has to consider potential negative impacts of the data processing on the data subject and weigh them against the interests of all people in the data processing actually taking place.[47] For sensitive personal data, such as data about health, religion or sex life, more restrictive legal grounds are defined.[48] The most restrictive category of data is data about criminal convictions and offences.[49]

The other basic principles of the GDPR require that personal data is only processed in a proportionate manner, which includes collection personal data only to the extent really necessary for the purpose ("data minimization") and keeping it only for as long as necessary ("storage limitation").[50] As part of the concept, it should also only be made available to people on a "need to know" basis. Personal data processed should be correct in view of its purpose, and, if not, corrected or deleted.[51] All personal data must be protected by adequate technical and organizational measures of data security to ensure that the principles are complied with.[52]

One of the most important principles is, however, transparency. Many issues in data protection can be solved by being outright transparent to the data subject about how his or her personal data will be processed and for what purposes – allowing him or her to object or take appropriate measures. Unfortunately, the lawmakers creating the GDPR have been over the top as to transparency, defining a long list of items about which a data subject has to be informed,[53] whether it makes sense or not. This is the reason why data protection statements, informing the data subjects of the details of data processing, have become so important, even though hardly anybody reads them.

## 2. Solution

In an arbitration, much as in any other area of business, each stakeholder should within its own sphere try to comply with the foregoing principles. For example, if a party chooses to submit evidence, it should only submit documents that are necessary for making its point. The stakeholders should not retain documents for longer than necessary. And they should not gather

47 Art. 6(1)(f) GDPR.
48 Art. 9(2) GDPR.
49 Art. 10 GDPR.
50 Art. 5(1)(c) and (e) GDPR.
51 Art. 5(1)(a), (b), (e) and (f) GDPR.
52 Art. 5(1)(f) and Art. 32 GDPR.
53 Art. 13 and 14 GDPR.

evidence under false pretext or in an illegal manner. This already follows from common sense, and should not represent an issue. From a more formal or governance and liability point of view, there are, however, a few steps to be taken by the arbitrators, the parties and their counsel:

*First,* the data protection agreement referred to above should be used to impose the obligation to comply with the above principles upon those stakeholders who are not already subject to the GDPR or a similar data protection law. We have discussed this already above. Our template contains language to that end.

*Second,* the parties should not submit personal data that already by its very nature could create problems under the GDPR. Specifically, submissions in the arbitration should not include any (a) private data (*i.e.* non-business-related content in e-mails, etc.), (b) health data and other "special categories of personal data"[54] and criminal data[55], or (c) data on identifiable children, unless – of course – such data were required for the arbitration. This is already a standard procedure when submitting European documents in U.S. litigation proceedings, and usually well acceptable to both sides. Should discussions arise about redactions, it is appropriate to have the arbitral tribunal decide.

*Third,* certain special information requirements under the GDPR can be complied with by piggybacking on the confidentiality declaration presented to each witness, expert and other person to appear in the arbitration and about whom personal data is to be processed. However, as opposed to the standard approach, we have not included a lengthy privacy notice in the declaration but rather have the individual declare that he was given all the information he or she may be interested in orally by the person who provided the person with the declaration (typically counsel). The paragraph lists all the information that needs to be provided for ensuring that the data subject is adequately informed if he or she really wants. This is an unusual approach and may appear as a "shortcut" but we believe it is fair and acceptable under the GDPR. It also only covers those data subjects from which stakeholders in the arbitration collect personal data *directly*.

For those data subjects whose information is collected in the arbitration *indirectly* (*e.g.*, the employee mentioned in an e-mail that happens to be used as evidence), the party submitting the personal data may either have informed data subjects in their ordinary course of business (*e.g.*, via its website)[56] or the other stakeholders may be able to rely on a special exception provided for by the

---

54 Art. 9(1) GDPR.

55 Art. 10 GDPR.

56 Art. 14(5)(a) GDPR.

GDPR where it would require a disproportionate effort to inform data subjects[57] (certain other exceptions may also apply under very specific circumstances[58]). We believe it would be disproportionate if the arbitrators and counterparties, or even the party submitting the personal data, would have to inform each individual mentioned about the fact that his or her data is going to be used in a third party, confidential arbitration. After all, such use of his or her personal data would most likely have no effect on the individual at all, provided everything remains confidential and the data is not used for other purposes.

*Fourth,* the processing of personal data in an arbitration usually has to be based on "legitimate interest" as a legal ground under the GDPR. Given the limited impact that the processing of personal data in the context of an arbitration will usually have on the individuals to which such data relates, considering that arbitrations are often confidential and that further controls are in place to protect personal data, and given the need of the stakeholders to rely on evidence containing personal data for determining the facts in an arbitration, we believe that such use will normally be justified and can indeed be based on legitimate interest. This is further supported by the fact, that the establishment, exercise or defense of legal claims is considered a sufficient basis even for processing special categories of personal data.[59] Since the GDPR requires that the legal grounds relied upon on, including any legitimate interest analysis, needs to be documented by the controller, we have included this to our data protection agreement template (cf. Annex).

We do not recommend relying on consent as a legal basis. Unfortunately, the use of consent in data protection has become highly problematic under the GDPR. Among other reasons, this is because consent can be withdrawn by the data subject at any time. Once this happens, many believe that it is no longer permitted to use related personal data, even if another legal ground were available. Given that consent is normally not required for processing data of individuals in an arbitration in the first place, it should not be used – not even as a standard statement in a witness statement. In fact, in order to avoid problems during the arbitration, the stakeholders should agree not to obtain consent from data subjects for submitting their information, where possible.

---

57 Art. 14(5)(b) GDPR; in certain very specific occasions.

58 For instance, Art. 14(5)(c) and (d) GDPR or additional exemptions provided for by EEA Member State law (e.g., §§ 29, 32 et seq. BDSG).

59 Art. 9(2)(f) GDPR.

## Topic No. 5: Dealing with other Provisions of the GDPR

### 1. Challenge

Apart from the basic principles, the GDPR and other data protection laws provide for a number of ancillary obligations that are geared towards re-enforcing compliance with the principles or the data subject's right. The three most important rights that a data subject may exercise in an arbitration is his or her (a) right to see what each controller processes about him or her ("right of access"),[60] (b) the right to have wrong information corrected,[61] and (c) to have information deleted ("right to be forgotten").[62] Contrary to common expectation, these rights are not absolute, *i.e.* a controller may have grounds not to grant them. As a consequence, the right to be forgotten will have only very limited relevance in an arbitration – at least with regard to the evidence included in the file and necessary for the case.

The other ancillary obligations are the obligation (1) to notify data breaches (such as e-mails sent to wrong recipients, files lost during travel, hacking) to the competent GDPR data protection authority under certain conditions,[63] (2) to maintain an overview of the processing activities,[64] (3) to document compliance with the GDPR (principle of "accountability"),[65] (4) to undertake a "data protection impact assessment" (DPIA) under certain conditions,[66] (5) to appoint a data protection officer ("DPO") and representative in the EEA under certain conditions,[67] (6) to enter into appropriate agreements with any third party used for processing personal data ("processors"),[68] and (7) the contract among joint controllers already discussed above.

### 2. Solution

In practice, most of these ancillary obligations do not represent any issue in an arbitration proceeding, because they (a) can either be dealt with when it becomes necessary, (b) can be dealt with using some "paperwork" or (c) are of practical irrelevance. To begin with the latter, an arbitration does usually neither trigger the need to appoint a DPO, nor to have a EEA representative

---

60 Art. 15 GDPR.
61 Art. 16 GDPR.
62 Art. 17 GDPR.
63 Art. 33 et seq. GDPR.
64 Art. 30 GDPR.
65 Art. 5(2) GDPR.
66 Art. 35 et seq. GDPR.
67 Art. 37 et seqq. GDPR.
68 Art. 28 GDPR.

pursuant to Art. 27 GDPR. If a party already has a DPO, it may want to involve him or her in any e-discovery work that may become necessary (*e.g.*, for obtaining the mailboxes of certain employees). A DPIA is usually not necessary for the arbitration itself. E-discovery exercises may require a DPIA but this is each party's own responsibility.

The number of data subjects who exercise their rights is increasing but in arbitration proceedings they are still not common. It is also unlikely that a data protection authority will take a deeper look into the data processing in the context of an arbitration unless being tipped off by a data subject or another person. What is more likely is that a party will want to use data protection related claims or arguments for tactical purposes, for instance, as a reason to withhold evidence. This is something to be handled on an ad-hoc basis, and while such disputes will usually have to be decided by the arbitral tribunal, it has to be aware that it itself is responsible for complying with data protection. This means that if a party is not happy with the tribunal's decision, it may raise data protection claims against the tribunal, or have a data subject do so.

In our experience, it makes sense – and is required under Art. 26 GDPR – to agree among the joint controllers on the responsibilities in handling data subject requests and the other ancillary obligations. Our data protection agreement template contains corresponding language with a view to reflect the natural split of responsibilities among the stakeholders; it is based on the GDPR as such, and does not yet take into account any GDPR goldplating EEA member states laws[69], which may have an impact on information, data subject request and other obligations. We do not believe it makes sense to go into too many details in such an agreement, as most data subject requests, data breaches and other trigger events need to be dealt with on a case-by-case basis. We have, however, included in the agreement's annex the information required for the records of processing documentation as per the GDPR. The fact that the agreement describes the obligations of the various stakeholders with regard to data protection also helps to comply with the "accountability" principle.

## Final Remarks

Many arbitration practitioners will not feel comfortable about the "red tape" that data protection appears to add to arbitration proceedings. It is true that new laws such as the GDPR increase the level of paperwork and other governance required for compliance. However, many of these issues can be addressed by having an appropriate agreement in place with no need to

[69] Various provisions of the GDPR permit member states to provide for additional exceptions or stricter provisions or regulate certain details.

materially change the manner in which an international arbitration proceeding is to be conducted. It will be interesting to see how long it will take for the arbitration community to accept these new rules and conclude that measures such as entering into data protection agreements makes sense, even if the likelihood of intervention by the data protection authorities may be low. It will also be interesting to see how non-GDPR parties will react when confronted with the challenges described in this article.

David Rosenthal, *Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance*

**Summary**

How should arbitral tribunals deal with data protection? What are the data protection obligations of the parties of an international arbitration? Since the EU General Data Protection Regulation (GDPR) is in force and provides for massive sanctions, the interest is considerable. The article discusses the five key challenges of the GDPR in an arbitration proceeding and elaborates practical solutions to overcome them: *First*, the GDPR is applicable to each arbitrator, party and counsel who has its seat or domicile in the EU. Hence, some of the stakeholders may be subject to the GDPR, some not. *Second*, because all stakeholders usually are involved in determining the purpose and other essential aspects of the arbitral file or hearings, from a GDPR perspective they are usually considered jointly responsible for data protection compliance. As a consequence, the stakeholders who are subject to the GDPR are required to enter into an agreement with the other stakeholders to govern these jointly controlled activities that involve the processing of personal data, data that relates to identified or identifiable individuals. *Third*, the GDPR prohibits personal data from being made available to countries without an adequate level of data protection unless certain conditions are met. Again, a contract is usually required to ensure that this is the case, for instance by requiring confidentiality declarations from all participants, including witnesses. *Fourth*, the GDPR provides that certain basic principles have to be complied with when processing personal data, such as limiting the use of personal data to what is necessary. *Fifth*, the GDPR provides for certain additional obligations to be taken care of such as data breach notifications, handling access right or other requests of individuals. A key part of the solution to these requirements is the conclusion of a data protection agreement among the various stakeholders, and the article comes with a template for such an agreement.

# Data Protection Agreement

---

of [■] in the [■] Case No. [■]
by and between

**[Arbitrator 1]**
and
**[Arbitrator 2]**
and
**[Arbitrator 3]**

(each individually an **Arbitrator** or collectively the **Arbitral Tribunal**)

and

**[Party 1]**
and
**[Party 2]**

(individually an **Arbitration Party** or collectively the **Arbitration Parties**)

and

**[Counsel 1]**
and
**[Counsel 2]**

(individually or collectively the **Arbitration Counsel**)

(the Arbitral Tribunal, the Arbitration Parties, the Arbitration Counsel individually **Contracting Party** or collectively the **Contracting Parties**)

---

## PREAMBLE

1. The Contracting Parties are participants in the arbitration proceeding [■] Case No. [■] commenced by [Party 1] against [Party 2] through a request for arbitration submitted to the Secretariat of the [■] (the Arbitral Institution) on [■] (the Arbitration).
2. In the context of the Arbitration, the Contracting Parties process personal data as defined by Art. 4 No. 1 and 2 of 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 (General Data Protection Regulation, **GDPR**) for the purpose of resolving the dispute that is the basis for the Arbitration (the **Dispute**). Unless otherwise defined, terms in this agreement shall have the same meaning as those defined by the GDPR.
3. The Contracting Parties recognize that the GDPR as well as national laws, regulations, statutes and decisions, which regulate the processing of personal data (**Data Protection Laws**), may require some or all Contracting Parties to comply with certain requirements. For such purpose, the Contracting Parties determine their respective responsibilities concerning the processing of personal data that involves two or more Contracting Parties in the context of this Arbitration.
4. In light of the foregoing, the Contracting Parties agree as follows:

## 1. Scope

This Data Protection Agreement (the **Agreement**) governs the processing of personal data in the context of the process activities defined in Annex A to this Agreement, and applies only *inter partes* and vis-à-vis data protection supervisory authorities. It does not apply to any other processing of personal data by the Contracting Parties outside the scope of Annex A.

The provisions herein apply irrespective of whether a Contracting Party itself is subject to the GDPR or other Data Protection Laws. Nothing in this Agreement shall constitute an acknowledgement by any Contracting Party that the GDPR or certain Data Protection Laws apply to it.

In no way shall this Agreement limit, extend or otherwise change (a) the mandate or the powers of the Arbitral Tribunal under the agreement to arbitrate of the Arbitration Parties, or be considered part thereof, (b) the relationship between each Arbitration Party and its Arbitration Counsel or (c) the relationship between the Contracting Parties beyond the scope of this Agreement.

## 2. General Allocation of Responsibility

Insofar as a Contracting Party is a controller of a processing activity defined in Annex A, it shall be responsible for its compliance with regard to the GDPR and any other Data Protection Laws applicable to such activity where – pursuant to the procedure and rules of the Arbitration and orders of the Arbitral Tribunal – it is to process personal data for such processing activity. In particular, it shall take all necessary technical and organizational measures to protect the rights of data subjects, in particular pursuant to articles 12 through 22 GDPR (including applicable exemptions and other provisions under EEA member state law), and equivalent provisions under other Data Protection Laws applicable to the processing activities at issue.

## 3. Obligations of Each Contracting Party

### 3.1 Confidentiality regarding Personal Data

Each Arbitration Party and its Arbitration Counsel (each a **Receiving Party**) shall keep confidential any personal data that the other Arbitration Party, the Arbitral Tribunal or any individual appearing in this Arbitration (each a **Disclosing Party**) discloses (i) for the purpose of being included in the Arbitral Tribunal's file (the **Arbitral File**), (ii) to be considered for inclusion in the Arbitral File or (iii) otherwise to be used for a processing activity defined in Annex A (collectively the **Matter Data**).

This obligation shall not apply to (a) any Matter Data that is publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) any Matter Data that is discovered or created by the Receiving Party before disclosure by the Disclosing Party; (c) any Matter Data that is received by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; (d) any Matter Data that is disclosed by the Receiving Party with Disclosing Party's prior written approval; (e) any disclosure by the Receiving Party required under applicable law, in which case it shall, insofar permitted, inform the Disclosing Party and reasonably enable it to defend against such obligation before complying with it; (f) any disclosure by the Receiving Party to any Contracting Party or otherwise as permitted pursuant to Section 0; (g) any other disclosure by the Receiving Party necessary for the establishment, exercise or defense of legal claims in connection with this Arbitration, including any appeal or enforcement or other auxiliary actions in connection with the Arbitration through state courts.

The Receiving Party shall process the Matter Data for the sole purpose of conducting the Arbitration, including any appeal and enforcement actions or other auxiliary actions in connection with the Arbitration through state courts (the **Purpose**), except where provided otherwise by this Agreement.

The obligations of this Section shall apply *mutatis mutandis* to the Arbitral Tribunal insofar it receives any Matter Data (i) for inclusion in the Arbitral File, (ii) to be considered for its inclusion in the Arbitral File, or (i) in the context of the other processing activities pursuant to Annex A.

The confidentiality obligations of this Agreement are without prejudice to any other confidentiality obligations that may exist between Contracting Parties.

### 3.2 Legal Basis for Processing

Where possible, the Contracting Parties shall with regard to the GDPR not seek consent as a legal basis to process Matter Data or other personal data of individuals, as this may not be appropriate for use of such personal data in an arbitration. Instead, having considered their legitimate interest in being able to pursue the Arbitration on the basis of the Matter Data and the safeguards provided by this Agreement, the Contracting Parties agree that the Matter Data shall be processed on the legal basis of article 6(1)(f) GDPR (legitimate interest), article 6(1)(b) GDPR (performance of contract), **[**article 6(1)(c) GDPR (compliance with EEA law)**][**, article 6(1)(e) GDPR (public interest)**]*[adjust as applicable]*** and article 9(2)(f) GDPR (establishment, exercise or defence of legal claims), where applicable. The reason why the Contracting Parties believe that a legitimate interest exists are found in Annex A.

### 3.3 Compliance With Principles of Processing of Personal Data

Each Contracting Party shall process Matter Data and any other personal data in this Arbitration as per the principles in article 5 GDPR. In particular, it shall be processed in a lawful, fair and transparent manner and only for specified, explicit and legitimate purposes. It shall ensure that Matter Data and any other personal data in this Arbitration is correct and necessary in view of the Purpose, and is processed only to the extent needed for the Purpose and stored as personal data only for as long as needed for the Purpose (subject, however, to Section 0).

Each Contracting Party shall maintain the technical and organizational measures necessary to protect Matter Data and any other personal data in this Arbitration from any unauthorized processing and accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to it, as further detailed in article 32 GDPR. In particular, it shall undertake at least the

level of data security measures it would undertake for protecting own business secrets and in no event anything less than reasonable measures.

### 3.4 Information Duties

The Arbitration Parties shall ensure that their representatives, their witnesses, their party-appointed experts and any other individual appearing on their behalf or in their interest in the Arbitration are aware that their personal data may be processed for the Purpose, including for publication and archiving, and have either signed Annex B or otherwise received the information pursuant to article 13 et seq. GDPR and the equivalent provisions under the other applicable Data Protection Laws if and insofar required to cover the processing of their personal data as per this Agreement (not taking into account local law exemptions that may not cover the other Contracting Parties).

These obligations shall apply *mutatis mutandis* also to the Arbitral Tribunal with regard to its administrative secretary, any tribunal-appointed experts, or any other individual it invites to appear in the Arbitration.

### 3.5 Redaction of Sensitive Personal Data

Whenever an Arbitration Party submits Matter Data in the Arbitration, it shall ensure that private data (i.e. non-business-related personal data), any personal data of individuals of age 16 or below, any special categories of personal data (as defined under Art. 9 GDPR) and any personal data relating to criminal convictions and offences (as defined under Art. 10 GDPR) has been redacted to the extent reasonably possible, unless such personal data is required for the Purpose. Should an Arbitration Party dispute whether personal data has been redacted correctly by the other Arbitration Party, the two shall defer to the Arbitral Tribunal or a jointly selected third party for a good faith resolution of this dispute.

These obligations shall apply *mutatis mutandis* also to the Arbitral Tribunal with regard to any Matter Data it submits.

### 3.6 Permitted Disclosure of Personal Data to Third Parties

Unless the Arbitration Parties have agreed otherwise, or the Arbitral Tribunal has ordered otherwise in the Arbitration, and subject to the exceptions listed in Section 0, each Contracting Party may share Matter Data with any potential or actual witness, expert, administrative secretary, translator, interpreter, court reporter or other individual to appear in or be involved in the Arbitration insofar as such disclosure is deemed necessary for the Purpose, and further provided such individual has signed a declaration of confidentiality as set

out in Annex B or any other undertaking providing for a similar level of protection, unless such protection is already provided for by applicable law or a processor agreement has been entered into pursuant to Section 4.

Each Contracting Party may under this Agreement share any Matter Data with the Arbitral Institution for the Purpose without taking further steps (this shall not prejudice any additional requirements for data protection compliance as set forth by the Arbitral Institution).

### 3.7 Erasure of Personal Data

Following the completion of the Arbitration and expiration of the deadline to challenge any award, each Contracting Party shall return, permanently erase without keeping a copy, or anonymize, any Matter Data it has received from another Contracting Party and is required to keep confidential pursuant to 0, except that (a) it may retain Matter Data insofar the Contracting Party is required to do so by law or – as the case may be – by its mandate towards an Arbitration Party, or for evidentiary, scientific or historic research purposes, and (b) erasure is not required where this would impose an unreasonable effort on such Contracting Party due to the nature of the systems legitimately used. In both cases, the obligations pursuant to this Agreement shall continue to apply for as long as such personal data is retained by the Contracting Party.

## 4. Use of Processors

Where one or more Contracting Parties wish to use, for one of the processing activities in Annex A, a third party as a processor (within the meaning of article 4 GDPR) to carry out a processing of personal data on their behalf, they shall consult with the other Contracting Parties being controllers of said processing activity and enter into a processor agreement with the third party in accordance with article 28(3) GDPR and other applicable Data Protection Laws and, if such third party is in a country without an adequate level of data protection, they shall also enter into an agreement reflecting the "Standard Contractual Clauses (processors)" pursuant to the Decision 2010|87|EU (C(2010)593) of the European Commission without the Illustrative Indemnification Clause, or any clauses superseding them under the GDPR, as the case may be (the **EU Model Clauses**).

Individual interpreters and court reporters (but not legal entities) and the Arbitral Tribunal's secretary, if any, are not be considered processors but instead acting instead under the control of the relevant processor (article 29 GDPR). Hence, the provisions of Section 0 shall apply to them.

The Contracting Parties agree that Matter Data and other personal data related to the processing activities for which they are a controller may be stored with a Cloud or hosting service provider by a Contracting Party with no further consultation of the other Contracting Parties, provided that this occurs otherwise in compliance the above provisions of this Section 4.

## 5. Data Protection Governance

### 5.1 Data Subject and Supervisory Requests

Each Contracting Party who, as a controller of a processing activity defined in Annex A, receives a data subject request (including requests for access, correction, deletion or objection) or a request from data protection supervisory shall (a) without delay inform all other Contracting Parties who are also controllers of the processing activity at issue pursuant to Annex A, and (b) in good faith agree with them on how to respond to it, it being agreed that this shall not prevent a Contracting Party from complying the GDPR and other the Data Protection Laws applicable to it.

Each Contracting Party who is a controller of the processing activity at issue shall provide the other Contracting Parties who are also controllers of such processing activity any reasonably requested support allowing them to properly respond to such request pursuant to the GDPR and other Data Protection Laws applicable to such processing activity.

The Arbitral Tribunal may request that requests it has received are properly responded by the Arbitration Parties insofar they are also controllers of the processing activities at issue, even if they are not subject to the GDPR or other Data Protection Laws applicable to such processing activity.

Each Contracting Party may share the essence of this Agreement with any data subject or supervisory authority requesting it. The Contracting Parties shall beforehand agree on what the essence is, with the Arbitral Tribunal having the final decision power.

### 5.2 Data Breaches

If a Contracting Party becomes aware of a personal data breach within the meaning of article 33 GDPR that relates to a processing activity defined in Annex A, it shall (a) without delay inform all other Contracting Parties of such breach and (b) in good faith agree with them on how to respond to it, including making notifications to supervisory authorities and data subjects as required under the GDPR and other Data Protection Laws applicable to such processing

activity, it being agreed that this shall not prevent a Contracting Party from complying the GDPR and other the Data Protection Laws applicable to it.

Each Contracting Party who is a controller of the processing activity at issue shall provide the other Contracting Parties who are also controllers of such processing activity any reasonably requested support allowing them to properly respond to such data breach pursuant to the GDPR and other Data Protection Laws applicable to such processing activity.

The primary responsibility to do a data breach notification is with (a) the Contracting Party responsible for the data breach or where the breach occurred (if this can be determined and there is one), and (b) the Contracting Party being an Arbitration Party (in this order of priority).

### 5.3 Cooperation

Each Contracting Party who is a controller of a processing activity defined in Annex A shall reasonably support any other Contracting Party who is also a controller of such activity in complying with its obligations and responsibilities under this Agreement and under the GDPR and other Data Protection Laws applicable to such activity.

### 5.4 Non-Compliance

If a Contracting Party who is a controller of a processing activity defined in Annex A has indications that another Contracting Party who is also a controller of such activity is (a) not in compliance with the GDPR or other Data Protection Laws applicable to such activity or (b) not in compliance with this Agreement with regard to such activity, the other Contracting Party shall in good faith provide any cooperation, including any information, as reasonably requested, required and available, to clarify and resolve such issue. If the two Contracting Parties are both Arbitration Parties and cannot agree, the Arbitral Tribunal shall review the alleged non-compliance. The Arbitration Parties shall fully cooperate in the context of such review. The Arbitral Tribunal's reasonable and reasoned opinion shall be binding for both Contracting Parties under this Agreement, subject to its powers in the Arbitration and subject to the dispute being brought before a competent state authority.

### 5.5 Documentation

Annex A provides the records of processing pursuant to article 30 GDPR for the Arbitral Tribunal and other Contracting Parties. Further, each Contracting Party is responsible for its own ability to demonstrate compliance

with article 5(1) GDPR pursuant to article 5(2) GDPR (or equivalent provisions under applicable Data Protection Laws), and shall, on its own, undertake a data protection impact assessment where required under the GDPR or applicable Data Protection Laws.

## 6. Various Provisions

This Agreement shall remain in force as long as any of the Contracting Parties is processing Matter Data or engaged in any of the processing activities defined in Annex A.

Each Contracting Party shall be responsible for compliance with this Agreement by its employees, contractors, subcontractors, agents and other third parties it relies upon for its processing of personal data for the Purpose.

Any changes to this Agreement shall be valid only if agreed in writing. Should any terms of this Agreement be void or ineffective or lose their effectiveness due to later circumstances, this shall not affect the validity or effectiveness of the remaining provisions.

This Agreement shall be governed by [■] substantive law (excluding any conflict of laws provisions). The ordinary courts at the seat of the Arbitral Tribunal shall have the exclusive jurisdiction to adjudicate any disputes under or in connection with this Agreement.

[Signatures of the Contracting Parties]

# Annex A

## Description of the Processing Activities Covered*

| Activity/ Purpose | Controller(s) | Categories of Data | Categories of Recipients |
|---|---|---|---|
| Arbitral File, including submissions by each Arbitration Party for inclusion into the File (including any Redfern procedure) | Arbitral Tribunal, Arbitration Parties[, Arbitration Counsel] | Business correspondence, contracts and other factual information and pleadings contained in party submissions, documentary evidence, witness statements, expert reports, pleading notes and other records; hearing transcripts; procedural orders; awards; correspondence with the Arbitral Institution | Contracting Parties, service providers, witnesses, experts, other individuals appearing in the Arbitration, Arbitral Institution |
| Hearings | Arbitral Tribunal, Arbitration Parties[, Arbitration Counsel] | Same as for the Arbitral File. | Contracting Parties, service providers, witnesses, experts, other individuals appearing in the Arbitration, |

| Activity/ Purpose | Controller(s) | Categories of Data | Categories of Recipients |
|---|---|---|---|
| | | | Arbitral Institution |
| Administration of the Proceeding | Arbitral Tribunal, [Arbitration Parties[, Arbitration Counsel]] | Information about submissions, evidence, parties, witnesses, experts, service providers, costs, locations and other aspects of the Arbitration | Contracting Parties, service providers, witnesses, experts, other individuals appearing in the Arbitration, Arbitral Institution |
| Arbitral Award | Arbitral Tribunal, [Arbitration Parties[, Arbitration Counsel]] | Information about the case | Arbitration Parties, Arbitration Counsel, Arbitral Institution |

The above processing activities are limited to the Arbitration, and do not include the Arbitration Parties' preparation of submissions or their internal processing of their own submissions.

The Contracting Parties agree that in addition to the GDPR, **[**the Swiss Data Protection Act**]** and [■] are considered a Data Protection Laws applicable to "Arbitral File" and "Hearings2 processing activity for the purpose of this Agreement. This shall not prejudice whether a particular Contracting Party is subject to the GDPR or any other Data Protection Laws.

The data subjects affected may include the Arbitration Parties' employees officers, directors or consultants, the employees, officers, directors

or consultants of their customers, business partners and other companies relevant to the Arbitration, and any individual appearing in the Arbitration.

None of the parties has appointed a data protection officer or representative pursuant to article 27 GDPR.

The data security measures are described Section 0 of the Agreement.

Personal data may be transferred to any location worldwide, if necessary for the purposes of the Arbitration (cf. article 49(1)(e) GDPR). The duration is governed by Section 0 of the Agreement.

The decision to use a legitimate interest as a legal basis for processing for all of the above processing activities has been made for the following reasons: *The Contracting Parties depend on the ability to use personal data in the Arbitration in order to permit the Arbitral Tribunal to conclude the issues in dispute, and redacting all personal data would not only be overly burdensome, it would also significantly limit the informational value of the evidence, such as information on the sender and recipients of documents and assessment as to who has made which statement. The processing of personal data will already be limited to what is necessary for the Purpose, it is subject to the safeguards of this Agreement even for those parties who are not subject to the GDPR, and the use of the personal data for the Purpose is strictly controlled by the Arbitral Tribunal and its procedural orders. The personal data is not made public; access to the personal data will be very limited. The personal data is mainly of business related nature, and it is unlikely that the processing for the Purpose will have any negative effects on the data subjects, and if it does have due to the findings made in the proceeding, then such findings will have been made in a strictly controlled, judicial process comparable as with a state court proceeding safeguarding the rights of such data subjects. Overall, the relevant Contracting Parties therefore believe that it is justified to have personal data submitted and processed as envisaged by the Processing Activities described in the above table, where this is not already justified on the other legal grounds listed in Section 0.*

* This shall also serve as the records of processing pursuant to article 30 GDPR.

# Annex B

## Confidentiality Declaration

---

by ***[Full Name]***

Living at ***[Home Address]***;

Currently working for ***[Employer]*** at ***[Address]***;

As ***[present title, occupation or job description]***.

---

I have been asked by ***[Name of Contracting Party]***, ***[Address]*** (the **Instructing Party**), to appear, or be involved, in the arbitration proceeding [■] Case No. [■] commenced by ***[Party 1]*** against ***[Party 2]*** through a request for arbitration submitted to the Secretariat of the ***[Arbitral Institution]*** on [■] (the **Arbitration**). As part of such involvement, I may be given or will otherwise obtain personal data of other individuals as well as other confidential information (the **Confidential Information**).

I hereby agree, for the benefit of the Instructing Party and the other parties to the Arbitration (including party counsel and arbitrators, all, the **Beneficiaries**), (a) to maintain in strict confidence any Confidential Information I receive, (b) to protect such Confidential Information with an adequate level of data security, (c) not to use such Confidential Information for any purpose other than the Arbitration, (d) to follow any instructions of the Instructing Party as to the processing of Confidential Information, and (e) to return or erase, without keeping a copy, any Confidential Information upon request or once my role in the Arbitration has ended, except that (x) I may retain a retain a copy of any written statement I have submitted in the Arbitration, and (y) I do not have to erase Confidential Information where this is not reasonably possible due to the nature of the systems legitimately used; in both cases, my obligations (a) – (d) shall continue to apply for as long as such Confidential Information is retained by me. This confidentiality declaration is governed by substantive Swiss law, and each Beneficiary may initiate legal actions against me at its own seat.

I take not and acknowledge that my own personal data, including whatever I submit to the Arbitration, may be processed by the Beneficiaries and other parties involved in the Arbitration for the purposes of the Arbitration, which may involve such personal data to become **[**public or**]** archived. I

confirm that, I was offered to be informed, and was informed to the extent I was interested, by the Instructing Party about these parties and how to contact them, their data protection officers and representatives, if any, the legal basis for such processing, including the legitimate interest, the categories of recipients and categories of my personal data at issue, including private and public sources used, the fact that the processing may take place worldwide and the safeguards in place, **[**the countries of processing**]**, the duration of the processing of my personal data, my data subject rights (including my right of access and correction), my right to withdraw any consent for processing I may have been asked to give, my right to lodge a complaint with a supervisory authority, whether I am required to provide personal data, ***[add any other required information]*** and the existence of any automated decision-making.

***[Date, Place] [Signature]***

---

**Submission of Manuscripts**
Manuscripts and related correspondence should be sent to the Editor. At the time the manuscript is submitted, written assurance must be given that the article has not been published, submitted, or accepted elsewhere. The author will be notified of acceptance, rejection or need for revision within eight to twelve weeks. Manuscripts may be drafted in German, French, Italian or English. They should be submitted by e-mail to the Editor **(mscherer@lalive.ch)** and may range from 3,000 to 8,000 words, together with a summary of the contents in English language (max. ½ page). The author should submit biographical data, including his or her current affiliation.

**Aims & Scope**
Switzerland is generally regarded as one of the World's leading place for arbitration proceedings. The membership of the Swiss Arbitration Association (ASA) is graced by many of the world's best-known arbitration practitioners. The Statistical Report of the International Chamber of Commerce (ICC) has repeatedly ranked Switzerland first for place of arbitration, origin of arbitrators and applicable law.

The ASA Bulletin is the official quarterly journal of this prestigious association. Since its inception in 1983 the Bulletin has carved a unique niche with its focus on arbitration case law and practice worldwide as well as its judicious selection of scholarly and practical writing in the field. Its regular contents include:

- Articles
- Leading cases of the Swiss Federal Supreme Court
- Leading cases of other Swiss Courts
- Selected landmark cases from foreign jurisdictions worldwide
- Arbitral awards and orders under various auspices including the ICC and the Swiss Chambers of Commerce ("Swiss Rules")
- Notices of publications and reviews

Each case and article is usually published in its original language with a comprehensive head note in English, French and German.

**Books and Journals for Review**
Books related to the topics discussed in the Bulletin may be sent for review to the Editor in Chief **(Matthias SCHERER, LALIVE, P.O.Box 6569, 1211 Geneva 6, Switzerland).**