DISPUTE RESOLUTION JOURNAL®

AMERICAN ARBITRATION ASSOCIATION®
INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION®
AAA Mediation.org®

JULY 2020 | VOLUME 74 | NUMBER 4

The Impact of GDPR on International Arbitration—A Practical Guideline

Clara-Ann Gordon*

Introduction

Since May 25, 2018, the European Union's ("EU") General Data Protection Regulation ("GDPR") applies.

The GDPR applies to "personal data." This term includes any information relating to an identified or identifiable natural person (e.g., an individual's name, address, and any online identifier such as an e-mail address). The GDPR also has a broad scope of application, reaching entities in the EU as well as entities outside the EU processing data of EU-based individuals. For example, a witness based in the EU may in some circumstances import GDPR obligations into an arbitration, even if the arbitration is otherwise completely independent of the EU. Moreover, this wide scope of application is paired with potentially high penalties of up to €20 million or 4% of an entity's total worldwide annual turnover of the preceding financial year (whichever is higher) for certain infringements of the GDPR.

The GDPR has significantly altered the landscape of data protection. The international arbitration community must be aware of the terms of the GDPR and how it impacts the arbitral process and the parties involved: i.e., arbitrators, procedural parties, witnesses, counsels from law firms, experts, other third parties (collectively "Involved Parties").

I. Does The GDPR apply to International Arbitration Proceedings?

As soon as data with personal content of EU-based individuals is electronically processed (e.g., in emails or in documents that are stored electronically), the application of the GDPR must be assumed. There is no exception

*Clara-Ann Gordon is lawyer specialized in data protection and IT, an equity partner with the Swiss law firm Niederer Kraft Frey and a CEDR certified mediator. Moreover, she is the president of ITDR-Institute for Data Protection and IT Dispute Resolution.

for arbitration proceedings in the GDPR. It must be noted though that data of legal entities (for instance, an organization's address or telephone number) are not protected by the GDPR. However, the personal data of those individuals acting for that legal entity are protected by the GDPR. Once an individual based in the EU is involved, the arbitral tribunal should assume that the GDPR is applicable. Moreover, the scope of the GDPR does not depend on the location of the arbitration proceedings, but rather on whether the Involved Parties are based in the EU. An arbitrator from a non-EU state (a so-called third country) is not necessarily subject to the GDPR, unless she/he specifically targets residents based in the EU. Especially in international arbitration proceedings, there may therefore be constellations where not all Involved Parties are subject to the GDPR.

II. Can the Applicability of the GDPR be Avoided?

It is theoretically possible to choose a seat of arbitration outside the EU and for all Involved Parties to be from outside the EU. However, if only one of the Involved Parties in the arbitral proceedings is based in the EU and personal data from such an individual are processed, then the GDPR is applicable again.

III. What does this mean for the Involved Parties?

The Involved Parties who are based in the EU will be subject to the provisions of the GDPR. An Involved Party not based in the EU will in doubt not be subject to the GDPR.

This leads to the next question as to what happens if not all Involved Parties in arbitral proceedings are based in the EU. If within the arbitration proceedings not all Involved Parties are subject to the GDPR, then certain measures might need to be taken. For instance, processing of personal data may require a separate justification (e.g., consent) and, with regard to data transfers to a party in a third country like the U.S., if no exceptions apply (see Article 49(1) of the GDPR), the conclusion of EU Standard Contractual Clauses ("SCC") should be considered. This must all be agreed among the Involved Parties.

IV. What are the Duties of the Involved Parties?

The arbitrator subject to the GDPR will, for example, most likely be qualified as a "controller" according to Article 4(7) of the GDPR, since she/he processes the personal data on her/his own authority and not based on instructions given. Hence the arbitrators will be subject to the provisions applying to controllers and of course all other provisions of the GDPR.

For arbitrators, as the persons responsible, the rules set out in Article 5 of the GDPR apply. Importantly, data processing must be transparent and can only be carried out for the purpose for which the data were collected. The processing of personal data shall also be limited to what is necessary (so-called "data minimization"). Finally, the data must be kept up to date, must not be stored for too long, and must be securely processed.

Arbitrators are subject to broad information duties under the GDPR. It is therefore recommended at the beginning of the procedure to issue a data protection notice to the Involved Parties on the use of their data and to explain the principles of data protection law. Arbitrators can either individually issue such data protection notices or parties can mutually agree on a data protection notice for their respective arbitral procedure.

With regard to the other stakeholders (counsel, experts, witnesses), it needs to be assessed on an individual basis what their roles are under the GDPR (e.g., controller or processor) and what obligations and duties might apply to them as a result.

Whether or not the stakeholders are considered to be "joint controllers" in the meaning of Article 26 also needs to be assessed in each individual case.

V. Joint Controllership and its Pitfalls

The question of whether arbitrators are considered to be joint controllers with shared responsibility must be determined on a case-by-case basis. As far as can be seen, there are currently no final and concretely implementable statements or decisions from the data protection authorities and courts. Case law and guidelines are yet to be issued. However, the contentious nature of arbitration proceedings, the legally stipulated independence of the arbitrator, and the arbitrator's procedural sovereignty—in our current

view—fundamentally argue against considering the arbitral tribunal or even all of the Involved Parties to the proceedings as "jointly responsible parties" for the personal data introduced into and processed in the arbitration proceedings.

VI. What is the Legal Basis for Processing?

Article 6(1) of the GDPR lists six different processing grounds, with the key bases being:

- processing with the consent of the data subject,
- processing for the performance of a contract with the data subject or in order to comply with a legal obligation, and
- processing for the performance of a task carried out in the public interest or in the legitimate interest of a third party.

Consent, provided it meets the requirements of the GDPR, is an effective but uncertain basis for processing, as it can be revoked by the data subject at any time. In arbitration proceedings, the practical benefits of consent are also likely to be limited, since a data subject can only ever consent to the processing of his own data, but not to that of a third party. Therefore, a party cannot consent to the processing of the personal data of his witness, and obtaining consent from all third parties who may be affected is usually not practicable.

In relation to the Involved Parties, the data processing may often be necessary for the performance of the arbitration agreement (Article 6(1)(b)) but, in any event, it is in the legitimate interest of the arbitral tribunal (Article 6(1)(f)). In relations with witnesses and other third parties, data processing is likely to be carried out regularly in the exercise of a legitimate interest of the arbitral tribunal or of the parties to conduct the arbitral proceedings (Article 6(1)(f)), whereby a weighing of interests must be carried out in each individual case. Since an arbitral tribunal collects personal data for the purpose of administering justice, there is also a strong argument that the data processing is necessary for the performance of a task which is in the public interest and would thus be covered by Article 6(1)(e).

VII. What Impact does the GDPR have with regard to Evidence Taking?

The GDPR does not establish an explicit right to refuse to give evidence; the general regulations apply in this respect. If a witness references the data protection law in refusing to participate, then the appropriate courts must be consulted.

The GDPR does not expressly regulate this. Such issues are to be decided by the arbitral tribunal on a case-by-case basis on the submissions of the Involved Parties and under the applicable arbitration rules. As a rule, only those parts of documents that qualify as or contain personal data should be affected. The processing of the personal data of a witness or other third party is usually likely to be covered by the legitimate interest of the Involved Parties in the conduct of the arbitral proceedings, so that a wholesale refusal to disclose documents is unlikely to be possible. However, depending on the nature and extent of the personal data, it may be necessary—in consultation with the arbitral tribunal —to redact or otherwise anonymise personal data in line with the principle of data economy.

VIII. And what about the GDPR Data Security Obligations?

Each arbitrator must ensure that the IT systems and means of communication used by him/her (or his/her law firm) are subject to state-of-the-art security standards.

When using cloud services, it is particularly important to note that personal data is uploaded to the server of the respective provider. This is a case of commissioned data processing, so that the principles of GDPR Article 28 must be observed. In particular, it is necessary to conclude a data processing agreement ("DPA") with the provider. When choosing a cloud service outside the EU, the regulations for data transfers contained in Chapter V of the GDPR must also be observed. Alternatively, good encryption of the uploaded files and a password communication process should be considered. The concrete form and details of these measures should be discussed with the Involved Parties.

IX. Can a GDPR-Compliant Arbitration Procedure EVER be Guaranteed?

The arbitrator should inform the Involved Parties and also document (e.g., in a procedural order) that:

- arbitration proceedings are not excluded from the scope of application of the GDPR and that applicable data protection regulations must be observed;
- the Involved Parties are responsible for this and the arbitral tribunal assumes that the personal data introduced into the proceedings were collected in accordance with the applicable data protection regulations;
- the Involved Parties are in particular responsible for informing the data subjects about the processing of their personal data in accordance with the applicable data protection regulations; or
- the Arbitral Tribunal invites the Involved Parties to address any data protection issues relating to the arbitration proceedings at an early stage.

X. Practical Solutions

In light of the above, the arbitral tribunal should document all points relevant to data protection law in writing, either in a procedural order after hearing the Involved Parties, if possible, or in an agreement with the Involved Parties, if agreement can easily be reached. In addition to the above-mentioned points, the arbitral tribunal should, in particular, document the basis on which it considers itself exempt from certain obligations, such as obligations to provide information to third parties (for instance, under Article 13(4) and Article 14(5)(a), because the arbitral tribunal may assume that the third party already has the information); on the basis of confidentiality provisions; or because providing information to the persons concerned would jeopardize the conduct of the arbitral proceedings.

Finally, the International Chamber of Commerce, the American Arbitration Association-International Centre for Dispute Resolution, and other

ADR institutions have also issued useful guidelines. They suggest in particular that the arbitrator / arbitral tribunal does the following:

- Issue a procedural order on data processing;
- Issue an Arbitrator Privacy Policy;[1]
- Conclude a DPA among the arbitrators and the parties[2] with or without SCC for data transfer to countries outside the EEA (as the case may be) or join the EU-U.S. or Swiss-U.S. Privacy Shield Frameworks;[3]
- Keep an Article 30 GDPR Processing Activity Register; and
- With regard to the parties, they must ensure that they themselves—as well as their representatives, witnesses, experts, and so on—comply with the provisions of the GDPR.[4]

[1] *See, e.g.*, German Arbitration Institute, Arbitration Privacy Policy, http://www.disarb.org/en/76/content/privacy-policy-id73.

[2] *See* David Rosenthal, *Complying with the General Data Protection Regulation (GDPR) in International Arbitration—Practical Guidance,* 37 ASA Bulletin, No. 4, 822 (Dec. 2019) (including a sample data processing agreement for international arbitration).

[3] *See* International Centre for Dispute Resolution, About the Privacy Shield, https://www.icdr.org/privacyshield.

[4] *See* International Chamber of Commerce, Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration Under the ICC Rules of Arbitration, §§ 80-91, https://iccwbo.org/media-wall/news-speeches/icc-issues-updated -note-providing-guidance-parties/.