GT GreenbergTraurig

Advisory | International Arbitration & Litigation/ Data, Privacy & Cybersecurity

May 2021

Data Protection Obligations in International Arbitration

Introduction

In today's digital society, accelerated by the COVID-19 pandemic, data protection laws have become increasingly common, complex and wide-ranging. Given the high speed at which these laws are being introduced and evolve, arbitral participants' knowledge about their data protection obligations, and the serious penalties they risk for failure to comply[1], is seldom exhaustive and up-to-date.

Several of the major arbitral rules and guidance have been updated in the last two years and now include a general requirement for tribunals and parties to consult and address data protection issues early on during an arbitration[2].

Parties to an international arbitration, their lawyers, the tribunal members and the arbitral institution (the "**Participants**")[3] have numerous data protection obligations, which may compete and overlap,

[1] For example, under the GDPR (Articles 83 and 84), parties that fail to comply with the rules may be subject to civil liability, with fines potentially as high as 4% of the breaching entity's global gross revenue or 20 million Euro, whichever the higher. Parties may also be subject to criminal liability (see for example, section 170 of the United Kingdom Data Protection Act 2018).
[2] See for example, the 2019 'Note to Parties and Arbitral Tribunals on the Conduct of Arbitration under the ICC Rules of Arbitration' (par. 80 to 91), the 2020 LCIA Arbitration Rules (Article 30) and the 2020 IBA Rules on the Taking of Evidence in International Arbitration (Article 2(e)).
[3] This GT Advisory focuses on these Participants only. However, other actors in international arbitration, such as experts or vendors, may also have specific data protection obligations.

creating a complex compliance framework, especially in disputes that typically involve a significant amount of personal data, such as large-scale construction, technology and digital information disputes.

In March 2020, the International Bar Association (**IBA**) and the International Council for Commercial Arbitration (**ICCA**) issued a draft guidance – the Draft ICCA-IBA Roadmap to Data Protection in International Arbitration (the "**Draft Roadmap**") – for consultation. While a finalised version of the Draft Roadmap will not be officially released until September 2021, the current version already provides fairly detailed and helpful guidance for Participants.

Under the Draft Roadmap Participants would need to consider at the outset of an arbitration (i) all the potential flows of, and other activities involving the processing of, personal data, (ii) the data protection rules applicable to such flows and activities, (iii) the person(s) responsible for compliance with those rules and (iv) how to comply with those rules in an efficient and cost-effective manner, with minimum disruption to the arbitral process.

This GT Advisory sets out the key data protection obligations of Participants, with illustrative references to the Draft Roadmap and to the General Data Protection Regulation, Regulation (EU) 2016/679 (**GDPR**), which introduced many of the principles other modern data protection laws have adopted.

The following discusses the applicability of data protection laws to international arbitration, describes who is responsible for compliance with the data protection laws, and identifies key rules and principles likely to apply to Participants.

Which data protection law(s) apply?

The GDPR is often referred to as the benchmark for modern data protection. In its wake, numerous jurisdictions around the globe have adopted new rules which bear similarities with the GDPR (and also differences, taking into account their own specificities), including the United Kingdom[4], DIFC Dubai, Brazil, California, Singapore and Virginia[5].

It is critical that Participants identify at the outset of an arbitration all data protection laws which may apply to the arbitration. This exercise involves the Participants looking holistically at the likely activities and flows involving personal data and identifying the territorial and material scope of all potentially applicable data protection laws.

For instance, the GDPR applies when (i) personal data[6] (ii) is processed[7] within the GDPR's jurisdictional scope, meaning either:

[4] The United Kingdom retained the GDPR after Brexit, in the form of the UK GDPR, which applies alongside an amended version of the Data Protection Act 2018.
[5] Annex 9 of the Draft Roadmap sets out a helpful non-exhaustive list of national and regional data protection laws in important arbitration jurisdictions.
[6] Article 4(1) of the GDPR defines 'personal data' as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".
[7] Article 4(2) of the GDPR defines 'processing' as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

a. in the context of the activities of an establishment of a controller[8] or a processor[9] in the European Union (**EU**)[10]; or

b. in relation to the offering of goods or services to individuals in the EU[11].

GDPR's scope in international arbitration is extensive:

a. Personal data includes any data that identifies or may identify an individual such as names, home address, email address, video and audio recordings, location data and any other identifier or combination of identifiers.

b. Processing includes all activities involving the collection, use, dissemination, deletion, reception, organisation and storage of personal data.

Therefore, GDPR covers a wide range of activities performed by Participants in arbitration, including those related to the preparation and sharing of arbitration documentation (including pleadings, witness statements, express reports, submissions and awards), as well as those which involve contemporaneous evidence (for example, emails, letters, logs, reports, notes, photos, video recordings and audio recordings).

Who is responsible for compliance with the applicable data protection rules?

Data protection rules generally allocate principal responsibility for compliance to the person(s) who determine(s) the processing and means of processing of the personal data[12] in a given activity, often referred to as data 'controller' or 'joint controllers' if the determination is done jointly by two or more persons.

In the context of arbitration, the Participants are likely to be considered controllers for their processing[13] and will therefore be responsible for compliance with the data protection rules, either individually or jointly, as applicable.

They should allocate responsibility for compliance through a data protection protocol[14]:

a. They may be required to do so under the applicable data protection laws, for instance if they are joint controllers in a given activity[15].

b. In addition, they may have overlapping obligations arising from different activities in which different Participants process the same personal data independently[16]. Allocating such obligations amongst the Participants will avoid duplication of work and inefficiencies in the arbitration.

[8] Article 4(7) of the GDPR defines 'controller' 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*".
[9] Article 4(8) of the GDPR defines 'processor' as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".
[10] GDPR, Article 3(1).
[11] GDPR, Article 3(2)(a).
[12] See for example, Article 4(7) of the GDPR.
[13] Draft Roadmap, page 9.
[14] Annex 4 of the Draft Roadmap provides a helpful example of data protection protocol.
[15] See for example, Article 26 of the GDPR.
[16] For example, when a party collates contemporaneous documents containing personal data to provide to its lawyers, and the lawyers later use some of the personal data in pleadings or submissions.

Participants can delegate the performance of a processing activity to a third party 'processor' under their control (for example a translator, a transcriber or a reprographics vendor), in which case they are generally required to enter into data processing agreements with the processors to ensure compliance with the applicable data protection rules[17].

What are the Participants' obligations?

Assuming they are data controllers (which is generally the case for Participants), the below rules are likely to apply to Participants in international arbitration.

Data transfer between jurisdictions may be restricted.

Under the GDPR, Participants can only transfer personal data to a third country outside of the EU if[18]:

a. The EU Commission issued an 'adequacy decision' deeming the third country to provide adequate data protection[19].

b. In the absence of a decision, an "*appropriate safeguard*" (such as "*standard data protection clauses*") which complies with Article 46 of the GDPR combined with a determination by the Participant that privacy rights will be respected in the importing country[20].

c. In the absence of such a safeguard, there must be grounds for a derogation under Article 49 of the GDPR[21]. The derogation which arises when "*the transfer is necessary for the establishment, exercise or defence of legal claims*"[22] may apply in the context of some international arbitration[23].

Data processing is prohibited unless a lawful ground for processing applies.

The grounds on which general personal data may be processed are set out in Article 6.1 of the GDPR. The ground generally most suited to processing personal data in international arbitration is when "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party*"[24]. However:

a. A Participant cannot rely on this ground if such interests are overridden by the interests or fundamental rights and freedoms of the data subject, for example if the processing raises significant risks to the subject's profession or personal life[25].

b. In addition, the Participant, to rely on this ground, must undertake a legitimate interests assessment and record it[26].

[17] See for example, Article 28(3) of the GDPR.
[18] GDPR, Article 44.
[19] GDPR, Article 45(1).
[20] GDPR, Article 46.
[21] GDPR, Article 49(1).
[22] GDPR, Article 49.(1)(e).
[23] Draft Roadmap, page 12. Note, however, that the European Data Protection Board has cautioned companies that this derogation may only be used if the transfer of personal information is, indeed, "*necessary*" It has also advised that prior to a transfer a company (or Participant) must conduct a "*careful assessment of whether anonymized data would be sufficient in the particular case*" or, alternatively consider "*pseudonymized data*" Data that is not relevant to a particular matter should not be transferred. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 at 12 adopted on 25 May 2018.
[24] Draft Roadmap, page 18.
[25] Draft Roadmap, page 18.
[26] Annex 5 of the Draft Roadmap provides helpful guidance for such assessment.

The grounds on which special categories of personal data (including personal data revealing racial or ethnic origin, political opinions, religion, biometrics or health[27]) may be processed are set out at Article 9.2 of the GDPR. The ground generally most suited to processing special category data is when "*processing is necessary for the establishment, exercise or defence of legal claims*"[28].

The Participants must follow the applicable data processing principles.

Participants must follow all applicable data protection principles when processing personal data. Modern data protection laws, including the GDPR[29], generally require personal data to be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject;

b. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed;

d. accurate and, where necessary, kept up-to-date;

e. kept in a form that permits identification of data subjects for no longer than necessary given the purposes for which the personal data is processed; and

f. processed in a manner that ensures appropriate security of the personal data.

The Participants must record and demonstrate compliance.

Controllers must generally be able to demonstrate compliance with the applicable data protection law(s)[30] and keep a written record of the approach and measures they have adopted to comply[31].

Participants should consider undertaking a data mapping exercise at the outset of the arbitration and identify the processing activities and personal data flows that are likely to occur, the data protection limitations that may apply to each processing and flow, the persons likely to be responsible for compliance with such limitations and the measures that will be adopted for compliance with such limitations.

Conclusion

This GT Advisory identifies some of the key data protection obligations Participants must generally consider in international arbitration. They should, however, always undertake a fact-specific detailed review of all the potentially applicable data protection rules and consider their effect when preparing for, during and after the arbitration[32].

[27] GDPR, Article 9(1).
[28] Draft Roadmap, page 18.
[29] GDPR, Article 5(1).
[30] See for example, Articles 5(2) and 24(1) of the GDPR.
[31] See for example, Article 30(1) of the GDPR.
[32] Annex 3 of the Draft Roadmap provides a helpful starting point for such analysis. It provides a non-exhaustive checklist of data protection considerations which may impact Participants under the GDPR.

The rules and relevant regulatory bodies may provide some helpful guidance on how data protection obligations should be implemented in practice[33]. However, none looks in depth into how Participants should implement data protection rules in international arbitration.

The Draft Roadmap, in the circumstances, is a much-welcomed initiative and, when finalised, will provide Participants with a much-needed framework to guide their data compliance through the life cycle of international arbitration.

Author

This GT Advisory was prepared by:

- Leith Ben Ammar | +44 (0) 203.349.8778 | benammarl@gtlaw.com

[33] See for example, the GDPR's recitals, the Article 29 Working Party's guidelines and the European Data Protection Board's guidelines.