Kluwer Arbitration Blog

How Do You Deal With Data Protection And Cybersecurity Issues In a Procedural Order?

Gerald Leong (Herbert Smith Freehills) · Wednesday, February 19th, 2020

It would be difficult not to have encountered at least one arbitration event in the past year where data protection or cybersecurity was discussed. As these discussions become more frequent, one may wonder: what are the practical implications of data privacy and cybersecurity on the actual conduct of international arbitrations?

This was what the Singapore Branch of the Chartered Institute of Arbitrators (CIArb) sought to imagine in a unique competition organised a few months back. Armed with a detailed hypothetical fact scenario, competitors were asked to draft a Procedural Order (PO) providing directions on data protection and cybersecurity measures to be implemented in the conduct of the arbitration.

The Fact Problem

The problem was set against the backdrop of a rather unique set of 'facts'. Party A was a US-incorporated company financially backed by an imaginary EU member state, State C. Party A entered into a contract with Party B, a Singapore-incorporated software company. Pursuant to the contract, Party A funded Party B to develop an application, to be deployed on wearable devices, which collected health data from citizens of State C. To that end, Party B set up a branch in State C and its servers for the project were sited there. The personal data of citizens of other EU states were supposed to be excluded. The agreement was governed by Singapore law and provided for UNCITRAL arbitration seated in Singapore.

The dispute arose when Party A claimed that Party B's servers were hacked by a state-linked actor. Party A sought discovery of documents against Party B while Party B contended that granting discovery would amount to a breach of EU's General Data Protection Regulation (GDPR). The Tribunal was requested to decide in a PO, among other things, whether: (1) discovery would be a breach of the GDPR and (2) cybersecurity measures for the arbitration should be ordered.

Does the GDPR apply to an arbitration seated outside the EU?

The first question likely to be asked in a PO is which data protection laws apply. When, as in the CIArb competition, both the *lex arbitri* and substantive governing law were not the law of an EU

member state, the question as to whether the GDPR nevertheless applies is not straightforward.

One possible approach is to consider if the GDPR is mandatory law. However, the issue of whether, and what, mandatory laws apply in international arbitration is itself fraught with some difficulty. In the CIArb competition, the parties expressly stated in their dispute resolution clause that discovery was subject to any applicable mandatory law.

Even if one takes the view that the GDPR is mandatory law, the next question is whether the activities in the arbitration fall within the scope of the GDPR. The GDPR applies to all matters that fall within its (a) material scope and (b) territorial scope. The former is concerned with the type of activities. According to Article 2(1) of the GDPR, its material scope extends to all "processing of personal data wholly or partly by automated means". This is a wide definition and it is conceivable that the parties and the tribunal in an arbitration would end up processing personal data; not least during document production and review. This is reinforced by one of the recitals in the GDPR which states that it was intended to apply to "out of court procedures". That being said, at least one tribunal has thought otherwise. In June 2019, a tribunal in the NAFTA arbitration of ***Tennant Energy v Canada*** decided that the arbitration did not fall within the material scope of the GDPR.

The territorial scope relates to the actors in the arbitration. In that regard, the GDPR applies to any data controller or processor established in the EU, as well as to one outside the EU if he/she offers goods or services to data subjects in the EU. The following actors in an arbitration could potentially fall within the territorial scope of the GDPR:

- Parties to the arbitration – any party that does business in the EU and collect data there, even if they are based outside the EU
- Arbitrators – as discussed in this previous blog post, arbitrators residing in any EU member state appear to fall within the territorial scope of the GDPR
- All the stakeholders to an arbitration if administered by an institution based in the EU.

What are the implications if the GDPR is found to apply?

If the GDPR is found to apply to the arbitration, there are at least two implications. First, data processing is prohibited unless one of the grounds in Article 6(1) of the GDPR is found to apply. Arguably, the most relevant is Article 6(1)(f): processing that is necessary for the legitimate interests of the data controller.

Second, there are restrictions on the transfer of personal data outside of the EU. There must either be grounds for derogation under Article 49 of the GDPR, or there must be appropriate safeguards which comply with Article 46.

Therefore, to comply with the GDPR, a tribunal would likely have to set out in the PO whether data transfer is allowed and if so, whether any safeguards are to be implemented. This is by no means easy as there are very few resources targeted at helping international dispute resolution ensure compliance with the GDPR. One of the few resources currently available is the **Working Document 1/2009 on pre-trial discovery for cross border civil litigation**. While it pre-dates the GDPR, this EU document discusses some of the principles relevant to balancing discovery with data protection obligations. Further, and more updated, guidance should soon be available as the ICCA-IBA Joint Task Force on Data Protection in International Arbitration is expected to issue a

Draft Roadmap on data protection in international arbitration imminently.

Cybersecurity

Cybersecurity in international arbitration is a real concern given the growing frequency of cyberattacks. The consequences of a cyberattack on an arbitration could be severe given that sensitive commercial and personal data may be involved in an arbitration.

Presently, cybersecurity standards in international arbitration are primarily being driven by soft law, the most prominent of which is the **Protocol on Cybersecurity in International Arbitration** prepared jointly by ICCA, the NYC Bar Association and CPR. Launched in late 2019, the Protocol provides the principles and process for establishing cybersecurity measures in an international arbitration, as well as sample measures.

Practical measures

Besides deciding whether data protection and cybersecurity measures *should* be in place, it is possible for the PO to also set out suggested best practices which parties can take to ensure compliance. A well-regarded resource is the Sedona Conference's **International Principles on Discovery, Disclosure & Data Protection in Civil Litigation** which comes with an accompanying draft protocol that addresses data privacy issues, among others. Kathleen Paisely, working group member for the Protocol on Cybersecurity in International Arbitration, has helpfully proposed an adaptation of this protocol for international arbitration. Among other things, the protocol identifies and sets out principles regarding:

- The data controllers and processors
- Categories of data that are to be processed
- Legal basis for processing data
- How data transfers are to be regulated
- Data minimisation measures
- Cybersecurity

Conclusion

As the need for data protection and cybersecurity in international arbitration becomes more accepted, attention will shift to the practical measures that can be taken to achieve these objectives. There is as yet no widely-accepted method of implementing these measures. It is hoped that as the practice of a tribunal addressing data protection and cybersecurity measures becomes more common, more guidance and consensus will be built.

To make sure you do not miss out on regular updates from the Kluwer Arbitration Blog, please subscribe here. To submit a proposal for a blog post, please consult our Editorial Guidelines.

This entry was posted on Wednesday, February 19th, 2020 at 11:30 am and is filed under Cybersecurity, Cybersecurity Protocol, Data Protection
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.