Exclusively Online | **4 September 2020**

The Impact of the “General Data Protection Regulation (GDPR)” on International Arbitration Proceedings

Aspects of personal data protection are becoming increasingly more important not only in commercial transactions but also arbitration proceedings. The fact that international arbitrations are essentially private in nature doesn’t exempt participants in these proceedings from mandatory data protection laws. In order to be compliant, the authors suggest to address data protection issues in the early stages of the proceedings either in a case management conference or the first procedural order.

Personal Data Protection in International Arbitration Proceedings

More often than not, arbitration clauses in complex international agreements are the last item on the negotiating parties’ agenda. Arbitration clauses don’t always get the special attention they deserve and are sometimes referred to as “midnight clauses”. This fate seems to be shared to some degree for data protection requirements in international arbitration proceedings.

The Increase of Data Protection Laws

It has become increasingly challenging for data owners to retain control over their own personal information in this digital era. That is why data protection laws have been expanding across the globe. As of now, 107 countries have put in place legislation to secure the protection of data and privacy in their respective countries (https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx), including Hong Kong with the enactment of the Personal Data (Privacy) Ordinance (“PDPO”) which came into force in 1996. The most recent major data legislation is the California’s “Consumer Privacy Act” which came into effect on 1 January 2020.

The year 2018 saw the most drastic change to data protection laws in decades with the coming into effect of the European “General Data Protection Regulation”, impacting the development of data protection regulations worldwide. The GDPR and the Hong Kong’s PDPO share some conceptual similarities. However, the GDPR imposes more onerous requirements, e.g. the GDPR adopts a stricter accountability and governance principle, whereas the PDPO merely recommends certain privacy management measures as good practices for achieving accountability.

The General Data Protection Regulation and Its Extra-territorial Scope

The pivotal principle under the GDPR is that the processing of personal data is generally prohibited, unless there occurs a justification for the processing. **Even when the GDPR recognizes a reason for the data processing, such data may only be processed if they are genuinely required to achieve a specific purpose.**

Under the rules of the GDPR, not only do organizations have to ensure that personal data are collected legitimately under the strict conditions, but those who have control over and process the data are bound to observe the rights of data owners or data subjects by preventing the data from being exposed and exploited.

The scope of GDPR extends outside of the EU, even when the data processing doesn’t take place within the EU, provided any of the arbitrators, arbitral institutions, parties, witnesses and expert witnesses are domiciled in the EU. The GDPR is also applicable if the proceedings take place outside the EU but involve the processing of personal data from any parties domiciled in the EU.

For many years, the Hong Kong International Arbitration Center (“HKIAC”) has gained the reputation of one of the world’s leading arbitral institutions. Therefore, it is no surprise that the main nationalities of the parties and arbitrators involved in the HKIAC proceedings consistently consist of EU citizens (https://www.hkiac.org/about-us/statistics). Hence, the relevance and impact of the GDPR Hong Kong’s arbitration scene cannot be underestimated.

The GDPR and Its Implications for International Arbitration Proceedings

In the course of arbitration proceedings, a considerable amount of personal data will be processed, largely for the clarification of the underlying facts or the rescission or annulment of arbitral awards.

The expansive definitions of what amounts to personal data and the processing of the data under the GDPR essentially connote that any arbitral activities involving the processing of data that identifies or could identify an individual in the evidence presented in the form of emails, contracts, notebooks, witness statements, expert reports, and even the arbitral award, are likely to be bound by the regulations. Simply put, the GDPR apply to any party, counsel, arbitrator and the tribunal in an arbitration proceeding involving documents relating to personal data of an EU citizen, especially during the disclosure and exchange of documents, witness statements, expert reports, the preparation and issuance of the arbitral award and etc.

Compliance with the GDPR

The obligations of the GDPR apply to all persons in custody of the data who are either “controllers” or “processors” of the data. “Controller” is anyone or any organisation that determines the purposes and means of processing personal data; whereas “processor” is any entity that processes personal data on behalf of the data controller. The corollary to this is that any arbitrator, counsel or tribunal in custody of the personal data of the parties would at some point during the proceedings, be regarded as data controllers and/or processors.

The data controller is obliged to take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implementing appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the applicable rules.

The GDPR also sets out principles germane to the processing of personal data as follows:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
b. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (so-called “secondary processing”);
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed (“data minimization”);
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 (which limits data retention);
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

The arbitrator’s role in resolving the disputes is often complex and would usually involve a massive load of data processing. The upshot of this is that a myriad of data protection obligations under the GDPR would be triggered, such as:

- providing relevant information to the concerned data subjects regarding the processing of the data;
- providing a copy of the personal data undergoing processing;
- rectifying/erasing the inaccurate personal data;
- maintaining records of processing activities;
- carrying out data protection impact assessment when necessary and etc.

In situations where arbitrators are part of the same tribunal and having joint control, the arbitrators may be regarded as joint controllers under the GDPR. The GDPR obligates the joint controllers to enter into a transparent arrangement allocating the compliance obligations in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information and thereafter to inform the data subject of the essence of the agreement. Additionally, data subjects have an independent right of action against each joint controller irrespective of the terms of the agreement.

Further, data controllers are responsible for, and must be able to demonstrate compliance with these principles. Thus, to demonstrate that the GDPR requirements are being complied, the arbitrators and arbitral institutions are encouraged to have a written mutual agreement modulating the issues on how data protection within the arbitration tribunal shall be protected. Arbitral tribunals should oversee aspects such as:

- the categories of personal data concerned;
- the purposes of the processing of the data;
- legal justifications of the data processing;
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the territory of the processing;
- the main responsibilities of the arbitrators as data controllers or data processors.

Practical Implications of the GDPR for Arbitral Institutions

Any organization who flouts the GDPR regulations, whether through its data controllers or data processors, could face a penalty of up to 4% of its annual global turnover or EUR 20 million, whichever is the higher.

In view of these obligations, various arbitration institutions (e.g. ICC: https://iccwbo.org/content/uploads/sites/3/2017/03/icc-note-to-parties-and-arbitral-tribunals-on-the-conduct-of-arbitration.pdf, DIS: http://www.disarb.org/en/76/content/privacy-policy-id73, VIAC: https://www.viac.eu/en/privacy-statement) domiciled in the EU have promulgated various data declarations. Some European institutions such as the Arbitration Institute of the Stockholm Chamber of Commerce even provided a secure digital platform for communication and file sharing on account of the GDPR. In contrast, arbitration institutions outside of the EU but having connections and dealings with EU parties seem to lag behind in this respect.

The arbitral tribunal plays an important role in spearheading that the proceedings are GDPR compliant in all respects. Therefore, the tribunal should be taking a bird’s eye view and determine the likely flow of data during the proceedings, on what legal basis the flow of data will take place and to whom the GDPR will apply.

Administrational efforts can be minimized if aspects of data protection are addressed in the initial stages of the proceedings, i.e. pre-trial conference or procedural orders. As a standing practice, initial procedural orders should always address issues of data protection to ensure compliance with the GDPR and other data protection laws throughout the entire proceedings.

The starting point for international arbitration proceedings is that there must be a GDPR justification for collecting/processing personal data. What tribunals could do is procure consent declarations from the EU parties. The consent must be given voluntarily, which may not always be practical as the said consent can be withdrawn anytime. As such, the better approach would be to pursue the *“legitimate interests”* ground under Art. 6(1)(f) GDPR.

Tribunals also have to be aware that the GDPR obliges them to advise parties in relation to the purposes for which their data are being used under Articles 13 and 14 GDPR. This provides also the parties whose data are processed with certain rights under the GDPR, i.e. right of access, right to rectification, right to restriction of processing, right to erasure etc.

Conclusion

The GDPR regulations are undeniably critical and pertinent to international arbitration proceedings. This is bolstered by the International Council for Commercial Arbitration and International Bar Association’s creation of a “Joint Task Force on Data Protection in International Arbitration Proceedings” that is currently working on a guide for data protection in the realm of international arbitration. In March 2020 it has published its first draft titled “ICCA-IBA Joint Task Force’s Roadmap to Data Protection in International Arbitration” for public comment.

In arbitration proceedings where enormous amounts of data are being processed frequently, it is incumbent for the parties to exercise caution and be vigilant of the GDPR requirements **in order to avoid jeopardizing the arbitral proceedings. Considering also the statutory presumption that if the data have not been processed in**

accordance with the GDPR, the data processor must prove that he/she has adhered to the GDPR requirements. To minimize the risk of infringing the GDPR, the parties in arbitration proceedings should draft a data policy agreement to put on record how the data protection law shall be complied with. This includes records of processing activities, a data protection impact assessment, in case of data transfer the transfer will be subject to appropriate safeguards and appropriate standards for the security of data processing.

Andreas Respondek

Respondek & Fan Pte Ltd

Tasha Lim