Kluwer Arbitration Blog

The Tanzanian Personal Data Protection Act (PDPA) and its applicability in Arbitration Proceedings

Mark Malekela (Alistair Group, Tanzania) and Katarina Jurisic (Technical University of Munich) · Wednesday, May 7th, 2025

Data protection laws and regulations are generally mandatory and apply anytime personal data is processed, including the methods, locations and times that personal information may be processed. However, such laws and regulations do not expressly or explicitly address data protection in arbitration proceedings.

On 27 November 2022, the National Assembly of Tanzania passed the Personal Data Protection Act (**PDPA**), which came into force on 1 May 2023. The PDPA regulates the processing of personal data in the United Republic of Tanzania and aligns with broader global trends in data protection, particularly the European Union's General Data Protection Regulation (**EU GDPR**). The PDPA is supplemented by the Personal Data Protection Regulations.

The PDPA establishes the Personal Data Protection Commission (**Commission**) as the supervisory authority responsible for enforcement and compliance. A key provision of the PDPA is the requirement for entities to register as data controllers or processors with the Commission under Section (**Sec.**) 15. With the final registration deadline expiring on 30 April 2025, businesses, including arbitration institutions and practitioners, must assess whether their activities fall within the PDPA's scope and, if so, proceed with registration. Given the broad definition of **"***data processing***"** under the PDPA, arbitration proceedings may inadvertently be subject to compliance requirements, potentially altering established procedural standards.

Despite its significance, the application of the PDPA in arbitration remains uncertain. Tanzanian arbitral institutions, such as the Tanzania Institute of Arbitrators (**TIArb**) and the Tanzania International Arbitration Centre (**TIAC**), currently lack explicit data protection focused rules or practice guidance, failing to address whether the existing legal framework adequately accommodates the evolving regulatory landscape. In light of this, this blog post aims to address two urgent questions – first, whether arbitrators and arbitral institutions qualify as data controllers or processors under the PDPA, and second, examining the potential data protection issues and obligations that may arise in arbitration proceedings and solutions that may be adopted to address them.

1. **Data Protection in International Arbitration in Tanzania**

As per Sec. 3 PDPA, the Act applies whenever “personal data” about a “data subject” is “processed” during activities falling within the jurisdictional scope of the PDPA. Henceforth, the PDPA applies to all data controllers and processors operating within Tanzania, and, in certain circumstances, to those outside the country that process personal data of individuals or entities in Tanzania. Territorially, the PDPA applies to both Tanzania Mainland and Zanzibar. In Zanzibar, the PDPA only applies to issues designated as ‘Union Matters’ under Art. 4(3) of the Constitution as provided for in Sec. 2 PDPA.

However, complexity may arise from the PDPA’s provisions on cross-border data transfers pursuant to Sec. 31 et seqq. PDPA. Given the inherently international nature of arbitration, personal data is often exchanged across multiple jurisdictions. Sec. 31 and 32 PDPA impose restrictions on such transfers, requiring either the existence of adequate safeguards or express consent from data subjects. These restrictions may conflict with arbitration rules that prioritize procedural efficiency, potentially leading to delays in the proceedings and compliance risks. Compared to the EU-GDPR, the PDPA does not adopt an adequacy decision for third countries’ data protection levels. Instead, it requires data controllers to assess whether a third country’s legal framework ensures adequate protection. Nevertheless, the Minister for Communication, in consultation with the PDPC, can issue regulations specifying the circumstances where cross-border transfers are not permitted.

The application of the PDPA in international arbitration imposes significant obligations on arbitrators and arbitral institutions. Arbitrators and arbitral institutions as data controllers share the same set of data protection obligations under the PDPA. The obligations of data controllers and processors under the PDPA are critically assessed in light of international best practices, particularly the ICCA-IBA Task Force Report on Data Protection in International Arbitration (**ICCA Report**) and Kluwer’s recent White Paper on Confidentiality and Data Protection in International Arbitration.

Arbitrators and Arbitral Institutions as Data Controllers

A key issue arising from the PDPA’s enforcement is whether arbitrators and arbitral institutions qualify as data controllers or data processors. Under Sec. 3 PDPA, a data controller is any individual or legal entity or public body which determines the purpose and means of processing personal data, while a data processor processes personal data on behalf of the controller and under the data controller’s instruction.

Considering that arbitral institutions handle sensitive personal and commercial data through exchange of correspondences between arbitral participants, receive and store all documentation contained in the files of an arbitration case, arbitral institutions as public bodies or legal entities are to be considered as “data controllers/data processors”, regarding different data processing activities that arise throughout the course of the resolution of a dispute through arbitration.

On the other hand, arbitrators are neutral third persons who guide the arbitral proceedings in order to resolve the dispute and are therefore necessarily those responsible to determine the means of processing personal data in arbitration proceedings. This corresponds to the definition of a data controller as provided in Sec. 3 PDPA. It remains to be seen how the PDPC will apply the registration requirement for data controllers to arbitrators in arbitration proceedings.

Sec. 5 PDPA provides for an extensive set of safeguarding obligations, e.g. regarding a lawful, fair and transparent processing of data with a clearly defined purpose. Data controllers must further safeguard compliance with the principle of data minimization, meaning that arbitrators and institutions may only collect and process personal data strictly necessary for the arbitration. Additionally, data must be kept accurate and updated, with rectification or erasure carried out without delay.

These principles align with the recommendations of the ICCA Report, which emphasizes that arbitration practitioners must incorporate and consider data protection safeguards into their case management procedures. The ICCA Report notes that arbitrators and institutions must proactively assess whether they qualify as controllers or processors and implement compliance measures accordingly. In practice, this requires arbitral institutions to establish clear policies on data privacy, especially regarding cross-border transfers of personal data.

Security Obligations and Appointment of a Data Protection Officer

A particularly complex obligation under the PDPA is the appointment of a data protection officer (DPO) by the data controller and/or data processor under Sec. 27(3) PDPA who shall ensure that the control and security measures are in place to protect the personal data collected or being processed and are being complied with. However, it is uncertain whether, for temporary settings where data is collected and processed, such as in arbitration proceedings, a DPO must be appointed. The wording of Sec. 2(3) PDPA (inclusion of “shall”) indicates such appointment to be mandatory. In any case, the role of a DPO is to be distinguished from the data controller and data processor as confirmed in Sec. 3 PDPA, therefore excluding the presiding arbitrator to act as data controller and DPO simultaneously.

Martin Zahariev’s previously published analysis rightly indicated that requiring the appointment of a DPO for each arbitration would impose an excessive administrative burden and could create conflicts of interest. The ICCA Report similarly highlights the need for flexible compliance measures tailored to the unique structure of arbitration, advocating for pragmatic solutions such as contractual safeguards between arbitrators and institutions rather than mandatory DPO appointments.

Moreover, the PDPA mandates that all data controllers and processors implement appropriate security measures to prevent unauthorized access, loss, or destruction of personal data. Sec. 31 and 32 PDPA impose restrictions on transborder data transfers, requiring that data must not be sent to jurisdictions with inadequate protection unless explicit safeguards are in place. This is particularly relevant for international arbitration, where case-related data often moves across multiple jurisdictions. On the other hand, arbitrators may consider incorporating standard contractual clauses that allow for data transfers, considering the need for review, minimization, culling, and redaction before transferring personal data to participants located outside Tanzania.

Without clear data protection guidelines for arbitration, compliance with these restrictions may hinder the efficiency of proceedings and create unnecessary regulatory burdens.

Data Subject Rights and Potential Procedural Disruptions

Moreover, the impact of data subject rights on the confidentiality of arbitration is of critical importance. Sec. 38 PDPA allows data subjects to request rectification, blocking, or erasure of their personal data, while Sec. 37(3) PDPA empowers the PDPC to order the deletion of personal data if a data controller or processor is satisfactorily found in violation of the PDPA. These provisions may raise concerns in arbitration where confidentiality is a fundamental principle. For instance, it is uncertain if, in case a party or witness invokes their right to erase personal data, such exercise of rights could interfere with the arbitrator's ability to rely on evidence. The ICCA-Report warns that overly broad data subject rights risk undermining arbitration's core procedural integrity, especially if parties use data protection laws as a strategic tool to obstruct proceedings.

Furthermore, consent requirements under Sec. 30 PDPA could present another challenge for the efficiency of arbitral proceedings. The PDPA requires written consent for the processing of sensitive personal data and yet offers limited exemptions. This narrow scope may increase the risk of tactical abuses where parties may revoke consent mid-proceeding to disrupt the arbitration. This calls for a balanced approach, allowing arbitration agreements to include standard contractual clauses on explicit consent in protection of personal data while recognizing legitimate exceptions for data processing in legal proceedings.

2. **Outlook into the Future**

While the PDPA introduces necessary data protection safeguards, its application in arbitration requires careful balancing as data protection laws apply to individuals and entities involved in arbitration proceedings, which may fall under different data protection laws or none, resulting in different rules and obligations for different participants.

Without clarification by the PDPC, it is unclear who will qualify to be appointed as a DPO if neither the arbitrators nor the arbitral institutions qualify. Further, with the possibility to appoint a DPO, additional costs arise, which raises the question of who – the parties, the PDPC or the arbitral institutions – will bear the costs for appointment of a DPO. Closely related is the issue of whether the disputing parties could protest the appointment of the DPO, *e.g.*, due to reasonable doubts about the officer's impartiality.

This article therefore, advocates for the arbitral institutions to include corresponding provisions with clear instructions on how to safeguard personal data in arbitral proceedings under the institutional rules (whether under the TIAC or TIArb Arbitration Rules). In this context, the ICCA-Report provides helpful guidance in this regard.

Without guidelines on data protection in arbitration, it is not predictable with certainty how the PDPA will impact the day-to-day handling of arbitration in Tanzania by both the arbitrators and the arbitral institutions. However, given that the PDPA has already come into operation and in light of the increasing use of technology and the existence of personal data in digital form in international arbitrations seated in Tanzania, we are looking forward to following how the arbitral institutions in Tanzania will address data protection challenges.

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, May 7th, 2025 at 8:55 am and is filed under Arbitral Tribunal, Data Protection, Tanzania, Uncategorized
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.