

Kluwer Arbitration Blog

Data Protection in India and Arbitration: Key Questions Ahead

Tarun Krishnakumar · Tuesday, April 16th, 2019

For a country with a significant corpus of the world's personal data, India's data protection framework is **notoriously deficient**. Improperly scoped, imprecisely drafted, and with no real enforcement culture, the extant framework¹⁾ often tends to create more problems than it solves.

With a view towards overhauling this framework, the Government of India, in July 2017, **constituted** a Committee of Experts ('**CoE**') under the Chairmanship of Justice (Retd.) BN Srikrishna to recommend a new data protection framework for India. After a year of deliberations, the CoE released the **Personal Data Protection Bill** ('**Draft Bill**'), along with a detailed report, in July 2018. After further consultations, the Draft Bill was to be introduced in Parliament for enactment. However, ongoing General Elections have put these plans **on hold**.

Partially modeled **along the lines** of the GDPR, the Draft Bill proposes an omnibus framework which includes detailed obligations relating to the manner of processing personal data²⁾, grounds on which such data may be processed³⁾, data principal⁴⁾ rights, accountability measures, and the constitution of a Data Protection Authority. While this progress is welcome, there are concerns that several provisions of the Draft Bill are unclear, excessively burdensome, or impractical in their current form.

Alongside other gaps, there is no clarity on the applicability of the proposed framework to alternative dispute resolution mechanisms such as arbitration. While data protection frameworks typically exempt judicial proceedings from compliance, it is critical to examine if these exemptions equally apply to arbitration. This is as a significant amount of personal data is likely to be **processed** in the course of a typical commercial dispute. If arbitration is not exempt, compliance concerns arise not only for *parties* processing personal data (as part of pleadings, evidence, or arguments) but also for the *tribunal* in collecting and storing it. Despite the significant overhead that data protection compliance could bring to arbitration, no discussions have begun on this interplay.

Arbitration in context of the Draft Bill

A key issue in the Indian context is whether the proposed framework applies to arbitral proceedings at all. The Draft Bill, in Chapter IX, contains a suite of processing activities which are exempted from compliance with all or parts of the proposed framework. In this regard, the question

is whether the exemption granted to ‘*Processing for the purpose of legal proceedings*’ would extend to cover arbitration-related processing. The relevant provision (Clause 44(1)) provides that:

“Where disclosure of personal data is necessary for **enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding** such processing shall be exempted from the following provisions of this Act— (a) Chapter II, except section 4; (b) Chapter III; (c) Chapter IV; (d) Chapter V; (e) Chapter VI; and (f) Chapter VII, except section 31.”

The import of this provision depends on whether arbitration would be considered as being a proceeding to ‘enforce [a] legal right or claim’, ‘defend any charge’, or ‘oppose any claim’. While arbitration is, no doubt, a mechanism to resolve disputes between parties by adjudicating upon their rights, its core nature is controversial.

Specifically, it is unclear if arbitration may be described as being for the purpose of *enforcing* a legal right or claim. While courts ultimately *enforce* arbitral awards, it would be wrong to suggest that *all responsibilities* for enforcing legal rights lie solely with the judiciary. In many cases, arbitral tribunals are empowered to determine disputes and the legal rights implicated by them.

In contrast, it is relatively easier to conclude that arbitration is a type of proceeding where parties ‘seek any relief’ or ‘oppose any claim’ – terms which are sufficiently broad to include stages of almost any dispute resolution mechanism. While a detailed examination of the nature of arbitration is beyond the scope of this post, it would seem *prima facie* that arbitration would be covered under Clause 44(1) of the Draft Bill.

What are ‘Legal Proceedings’?

Further the Supreme Court has interpreted ‘legal proceedings’, the term used in the section heading to Clause 44, to include arbitral proceedings. Albeit in a different context, the generality of the Court’s observation provides useful guidance. In *General Officer Commanding v. CBI*⁵, the Court observed that:

The phrase ‘legal proceeding’...is not synonymous with the ‘judicial proceedings’. Every judicial proceeding is a legal proceeding but not vice-versa, for the reason that there may be a ‘legal proceeding’ which may not be judicial at all, e.g. statutory remedies like assessment under Income Tax Act, Sales Tax Act, arbitration proceedings etc. So, the ambit of expression ‘legal proceedings’ is much wider than ‘judicial proceedings’.

Even if this were not conclusive, it may be noted that Clause 44(2) of the Draft Bill exempts processing related to *judicial* functions. By necessary implication, this indicates that Clause 44(1) was intended to cover *non-judicial* and *quasi-judicial* legal proceedings such as arbitration.

Implications of exempting arbitration under the Draft Bill

If arbitration is indeed exempt under Clause 44, most obligations under the proposed framework would not apply to its conduct. This would include the standards for processing in Chapter II, the requirement for legal grounds to process personal data in Chapter III, data principal rights in Chapter VI, and all but one of the transparency/accountability measures in Chapter VII. However, two significant caveats exist:

- The exemption under Clause 44(1) only applies where disclosure of data is *necessary* for “enforcing any legal right or claim, seeking any relief...”. Therefore, where personal data that is not strictly necessary for such purpose is disclosed in an arbitration, it will likely not be covered by this exemption.
- The following obligations continue to apply regardless of the exemption:
 - **Fair and Reasonable Processing:** Personal data must be processed in a fair and reasonable manner that respects the privacy of the data principal.
 - **Security Safeguards:** Data fiduciaries and processors⁶⁾ must implement (and periodically review) security safeguards including: (a) methods such as de-identification and encryption; (b) steps to protect the integrity of personal data; and (c) steps to prevent misuse, unauthorised access to, modification/destruction, disclosure of personal data. These safeguards must be risk-based considering the nature, scope and purpose of processing, and the likelihood and severity of harm that may result from such processing.
 - **Data Transfers:** Restrictions on [cross-border transfers of data](#) (contained in [Clauses 40 and 41](#)) would also continue to apply.

Concluding Remarks

Based on the above, it would appear *prima facie* that arbitration-related data processing would be exempt from most compliance under the Draft Bill. However, several niggling uncertainties remain. For instance, neither the preliminary [White Paper](#) nor the final [Report](#) of the CoE makes any reference to arbitration in discussions of Clause 44.

In fact, in commenting on Clause 44(1), the Report (p.136) notes that disclosure of personal data “*in pursuance of a legal claim*” would occur where data is required to be produced “*in connection with any legal proceeding*”. However, in apparent disconnect, the Draft Bill adopts a different, narrower standard: exempting disclosure where necessary for “*enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice*”. It is this unexplained narrowing of scope that raises questions concerning Clause 44(1) and its applicability to arbitration.

Further, the Report lists the ‘[Arbitration and Conciliation Act, 1996](#)’ as a legislation that would be impacted by the passage of the Draft Bill⁷⁾ However, no elaboration is provided on this point.

Lastly, like much of the Draft Bill, Clause 44(1) itself proves difficult reading. As extracted above, this exemption applies where “*disclosure of personal data is necessary*”. However, the second part of this provision exempts “*such processing*”. This inconsistency creates avoidable doubt if only disclosure (and not other types of processing) is covered by this exemption.

Despite these inconsistencies and lack of clarity, on balance, it is likely that arbitral proceedings will be covered under the present framing of Clause 44(1) and, therefore, be exempt from compliance with significant portions of India’s proposed data protection framework. However, whether such a broad exemption is in the interests of privacy, [cybersecurity](#), and transparency remains to be seen. While there is nothing to suggest that significant changes are likely to be made to the current text of the Draft Bill, a Government looking to establish India as a ‘[global arbitration hub](#)’ should take this opportunity to clarify and definitively settle this issue from the get-go.

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*.

Profile Navigator and Relationship Indicator

Includes 7,300+ profiles of arbitrators, expert witnesses, counsels & 13,500+ relationships to uncover potential conflicts of interest.

Learn how **Kluwer Arbitration** can support you.



Learn more about the newly-updated *Profile Navigator and Relationship Indicator*

 Wolters Kluwer

References

- as contained within the [Information Technology Act, 2000](#) and the [Information Technology ?1 \(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information\) Rules, 2011](#).
- ?2 'Personal data' is defined at Clause 3(29) of the [Draft Bill](#).
- ?3 'Processing' is defined at Clause 3(32) of the [Draft Bill](#).
- ?4 'Data principal' is defined at Clause 3(14) of the [Draft Bill](#).
- ?5 (2012) 6 SCC 228 (at Para 29).
- ?6 'Data fiduciary' and 'Data processor' are defined by Clauses 3(13) and 3(15) of the [Draft Bill](#).
- ?7 Annexure C, Point E(1) at Page 'i' of the [Report of the CoE](#).

This entry was posted on Tuesday, April 16th, 2019 at 8:00 am and is filed under [Cybersecurity](#), [Data Protection](#), [India](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.

