The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DATA PROTECTION IN CROSS-BORDER ARBITRATION: THE DPDP ACT 2023 MEETS INTERNATIONAL PRACTICE

~ Pari Shreya Maligonda

ABSTRACT

The Digital Personal Data Protection Act, 2023 (hereinafter referred to as 'DPDP Act') is considered the most significant piece of legislation in India with regard to data governance. The Act provides for a right-based regime for processing of digital personal data, which is heavily based on GDPR provisions, albeit with India's own regulatory spin [1]. In its attempt to assert India's position as a key international commercial arbitration center, there arises the issue of interaction of data protection law with arbitral practice, which has received inadequate scholarly attention to date. Cross-border arbitration almost inevitably results in exchange of personal data between multiple jurisdictions, which includes witness statements, documents, parties correspondence, records of e-discovery, and case management databases maintained by arbitral institutions [2]. All this information is exchanged between parties, lawyers, arbitrators, arbitral institutions themselves, and technology providers, often lacking appropriate data governance measures altogether. This paper focuses on application of the DPDP Act, 2023 to these transactions, as well as potential conflicts between Indian regulation and provisions of GDPR, Singapore PDPA, and Hong Kong PDPO, and

compliance challenges faced by parties of international arbitration proceedings. Moreover, this paper identifies gaps in the Act and suggests a framework for ensuring compliance in arbitral practice under Indian law.

I. Introduction

The arbitration system has its distinct place within the framework of dispute resolution: it is an individual and voluntary dispute resolution method which derives its legitimacy from the right of the disputing parties to opt out of the national judicial system and have their disputes settled through an agreed-upon arbitrator or a panel of arbitrators [3]. Often, confidentiality is mentioned amongst the fundamental qualities of the arbitration process, appealing to commercial entities that seek a private and confidential solution to their disputes, with the confidence that sensitive business data will not be made available to the public and rival businesses [4]. However, the aspects that attract commercial entities to arbitration the ability of arbitration to operate internationally, adapt to institutional frameworks, utilize digital communication platforms, and gather documents from other jurisdictions are also the aspects that lead to the creation of enormous amounts of personal data that are transferred across borders, sometimes lacking adequate governance plans under current privacy legislation.

The adoption of the Digital Personal Data Protection Act, 2023 (hereinafter "the DPDP Act" or "the Act"), receiving the Presidential assent on 11 August 2023, significantly changes this picture for any arbitral procedure involving Indian parties, Indian personal data, or data concerning Indian data principals [5]. The Act provides rights for data principals, duties for data fiduciaries and data processors, mechanisms for lawful processing of personal data based on consent, and rules for transfer of personal data outside India. However, although the Act makes no express reference to arbitral procedures, its applicability to all entities processing digital personal data of individuals in India, or otherwise in relation to services or products offered to Indian individuals, necessarily brings arbitration institutions, parties, representatives, and arbitrators into scope where Indian personal data is concerned.

The paper continues with another six sections. The second section deals with the ecology of personal data used in arbitral proceedings, covering types of personal data, processors of

personal data, and transnational data flows typical in international commercial arbitrations involving India. Section three presents an analysis of the major features of the DPDP Act. Section four analyzes the DPDP Act through a comparative lens by considering the GDPR [6], Singapore PDPA [7] and Hong Kong PDPO [8]. Section five addresses the issues arising from the interaction between arbitral proceedings and personal data protection laws. Section six provides policy recommendations.

II. Personal Data in International Commercial Arbitration: The Ecosystem

A. The Nature and Amount of Personal Data

International commercial arbitration, at its very heart, is a process that involves substantial documentation. The exchange of documents, the submission of pleadings, the drafting and filing of witness statements, and the conduct of hearings all involve a large amount of personal data being produced, processed, and transmitted across national borders [9]. Personal data related to witnesses, experts, and sometimes even party employees in terms of their identities, contact information, professional associations, financial information, correspondence, and life histories frequently appear in the evidentiary record. Personal data is obviously central to the issues when the dispute itself revolves around employment, joint venture, consumer, or intellectual property matters; however, even in cases that only concern commercial disputes between sophisticated corporations, personal data can be found in the form of personally identifiable email communications, signature authorizations on bills, and communications revealing personal opinions or decisions.

The advent of virtual and hybrid hearings, which have been facilitated by the outbreak of the COVID-19 pandemic and will continue as a regular practice in international arbitral proceedings, has created additional layers of difficulty for data protection [10]. Virtual hearings that take place on applications like Zoom, Microsoft Teams, or Opus2 require the processing of audio-visual data and metadata. An exercise that involves e-disclosures through technological assisted review applications would imply uploading of large amounts of

documents to the cloud, which are often based outside the jurisdiction of arbitration. Institutional case management systems, like NetCase from ICC, the electronic filing system at SIAC, or Casework Connect from LCIA, ensure that personal data is processed abroad by arbitral institutions other than the ones where parties, counsel, and arbitrators come from [11].

B. The Parties Processing the Personal Data

There are several parties that handle the personal data in a general international arbitration case with an Indian nexus. The parties themselves collect and disclose their personal data in relation to their employees, customers, suppliers, and other parties dealing with them. The counsels on both sides would collect their clients data, witness data, and data related to the other side while working on their submissions and obtaining evidence. The arbitral tribunal which would be made up of either one or three arbitrators from different countries is another party that handles the disclosed data. The arbitral institution is responsible for administering the case and will have copies of important communications in the proceedings [12].

However, the definitional architecture of the DPDP Act, which recognizes data fiduciaries as those who decide upon the purpose and means of processing personal data, and data processors, who merely perform the data processing at the behest of the former, fails to mirror the arbitral reality where multiple actors are present [13]. The arbitral organization might function as a data fiduciary while dealing with its administrative record, but will function as a data processor when it comes to handling the evidence submitted by the disputants. A law firm can work as a data fiduciary in deciding upon which witness material needs to be collected but would become a data processor in running the technology-assisted review tool offered by a technology provider company.

C. Cross-Border Data Flows in Arbitration

The unique characteristic of international arbitration from the perspective of data protection lies in its cross-border nature of data flows [14]. It is common practice for lawyers in London and New York to counsel clients in India and to access their personal data in connection with such instructions. The arbitrators in Switzerland or Singapore would receive evidence in respect of Indians. Case management systems in institutions would process case-related data

in servers located in Ireland, Singapore, or even in the US, according to load balancing settings. Vendors of e-discovery services would process Indians' personal data from centers in the Philippines or the UK.

Transfers of personal data of Indian data principals to countries or territories outside India under the DPDP Act are regulated by section 16 of the Act, which grants powers to the Central Government to impose restrictions or conditions on such transfers through notifications. As at the time of writing this paper, no notification has been made by the Central Government identifying any countries or territories as having restricted transfer provisions, thereby leaving both parties to arbitration and their advisors in a position of structural uncertainty regarding the legality of data transfers that are crucial for the process of international arbitration. Furthermore, the absence of a mechanism for allowing data transfers under the DPDP Act is an additional element of uncertainty [15].

III. DPDP Act 2023: Key Provisions Relating to Arbitration Practice

A. Scope & Territorial Jurisdiction

Section 3 of the DPDP Act sets out its territorial jurisdiction in terms that mirror, but do not match, Article 3 of the GDPR [16]. It covers processing of digital personal data occurring in India as well as any such processing outside India which is in connection with any activity relating to the offering of goods or services to data principals within the territory of India.This extra-territorial provision, which corresponds with the GDPR targeting criterion, has wide-ranging repercussions on international arbitration bodies, foreign law firms, and foreign arbitrators who handle personal data of Indian data principals in relation to arbitrations in which Indian parties are involved. An arbitral body based in London that frequently handles arbitrations between Indian parties, or a foreign law firm in New York advising Indian clients in international arbitrations, may very likely fall under the purview of this extra-territorial application of the Act.

The Act also excludes from its coverage the processing of personal data by individuals for personal or domestic purposes, and processing of data which is publicly available [17]. The

former exclusion finds no applicability to the participants in arbitral proceedings, since their processing of personal data in connection with the proceedings clearly falls neither under personal or domestic purposes, nor does it generally involve the use of public data. The latter exclusion is more relevant to the situation, but cannot be availed of by private persons conducting commercial arbitration proceedings.

B. Consent and Lawful Purposes

Under the DPDP Act, the consent-first principle applies when it comes to legal processing of personal data. Data fiduciaries are supposed to take free, specific, informed, unconditional and unambiguous consent of the data principal prior to processing personal data of such a data principal [18]. Besides consent, section 7 of the DPDP Act establishes a set of purposes which are referred to as legitimate uses, for which consent is not necessary. Section 7(e) enables processing of personal data for compliance with any law for the time being in force in India or any judgment or order passed by any Indian court or tribunal. Section 7(f) allows processing for performing 'any function of the State [19].

Of these bases, section 7(e) will be of most relevance to arbitral proceedings. While it may be debated whether compliance with the procedures established by the Arbitration and Conciliation Act, 1996 constitutes compliance with any law for the time being in force in India, it is my understanding that it does because the Arbitration and Conciliation Act is a central enactment and therefore compliance with such procedural orders amounts to compliance with law [20]. On the other hand, institutional arbitration rules (e.g., SIAC Rules or ICC Rules), which would similarly allow parties to produce documents in support of an arbitration, are contractual in nature and will not constitute the required basis under section 7(e) as they are not legislative in nature [21]. Practically speaking, this means that one cannot rely solely upon section 7(e) to process personal data pursuant to the procedural orders issued by institutional arbitral bodies without demonstrating a link between the said procedure and either the Arbitration and Conciliation Act or some other Indian statute. Finally, the DPDP Act makes no provision equivalent to the legitimate interests basis under Article 6(1)(f) of the GDPR [22].

C. Rights of Data Principals

Data principals are granted rights to access information regarding processing, the right to correction or erasure of personal data, the right to lodge grievances, and the right to nominate someone else as a representative to exercise rights should the principal die or become incapacitated by virtue of Chapter III of the DPDP Act Sections 11, 12, 13, and 14 respectively [23]. More especially, the right to erasure can cause difficulties in the field of arbitration because of the significance of the record created in arbitration. This includes witness statements, documents, and procedural orders that hold legal significance way beyond the completion of the proceeding. Awards can be made in several jurisdictions, and further proceedings, such as application for setting aside the award or recognition, will require that the original record be referred to. Thus, if the data principal makes use of the right to erase during arbitration, this may disrupt the proceedings and the subsequent enforcement of the award.

The DPDP Act fails to incorporate an explicit derogation from the erasure right for archival, research, and judicial purposes, as does Article 17(3)(b) and Article 17(3)(d) of the GDPR [24]. This omission represents one of the largest structural shortcomings in the DPDP Act when viewed through the prism of legal process. It can be said that the scope of the erasure right is implicitly limited because the information must be accurate and cannot be erased if doing so breaches another law. But the lack of a clear statutory exception makes it difficult to predict whether an anti-dissipation order issued under the rules of the Arbitration and Conciliation Act will trump an order seeking the erasure of data. The DPBI will have to solve this problem, as will the courts eventually.

D. Duties of Data Fiduciaries

Chapter II of the DPDP Act subjects data fiduciaries to several duties pertinent to arbitration as follows: the obligation to provide notice prior to or at the time of processing (Section 5) , the obligation to secure the accuracy of personal data (Section 8(3)), the obligation to undertake measures to guarantee data security (Section 8(5)), the obligation to report personal data breaches to the DPBI (Section 8(6)), and the obligation to delete personal data once there is no need for its retention as per the law and purpose of collection thereof (Sections 8(7) and 8(8)) [25].

The storage limitation requirement of Sections 8(7) and 8(8) is relevant to arbitral institutions and legal practices, which often keep files on cases for ten to twenty years after concluding the matter, in the hope of future enforcement, post-award litigation, or professional liability lawsuits [26]. Unless there is a legitimate reason for doing so, such practice will violate the DPDP Act storage limitations unless the data fiduciary can point to a legitimate need for continuing retention. The Act does not indicate the period within which data should be retained and leaves it open to the discretion of the data fiduciary, depending on guidelines by the DPBI, which are yet to be issued.

IV. Comparative Analysis: DPDP Act, GDPR, Singapore PDPA, and Hong Kong PDPO

A. The GDPR Framework

The GDPR, which became enforceable on 25 May 2018, serves as the benchmark standard against which all data protection regulations are compared thereafter, the DPDP Act included [27]. In cases involving cross-border arbitration proceedings involving parties, arbitrators, or institutional administration hailing from Europe, GDPR will often coexist with the DPDP Act, leading to conflict areas needing attention. One of the GDPR legal basis frameworks in Article 6 is far more detailed than the DPDP Act's framework of consent plus legitimate uses. Specifically, Article 6(1)(f) – the legitimate interests basis - offers a substantial amount of latitude to process personal data in the course of a legal proceeding such as arbitration where there is a balance between the legitimate interests of the data controller, such as enforcing contractual rights, and the fundamental rights of the data subjects [28]. No such basis of legitimate interests has been provided in the DPDP Act, an unusual omission in contrast to the GDPR approach.

Regarding data transfers, the GDPR is more developed in its provisions as compared to the DPDP Act. Article V of the GDPR has provisioned the adequacy decision by the European Commission, standard contractual clause, binding corporate rules, code of conduct, and certification systems as legitimate means of transferring data [29]. There are also detailed guidelines by the European Data Protection Board on the interface of these means with extra-territoriality of the GDPR [30]. Under the DPDP Act's negative approach, which

disallows transfers to any country that has been notified by the Central Government, there is neither clarity nor flexibility as provided under the GDPR; this can discourage foreign entities from choosing India as the forum for arbitration until a positive transfer mechanism is developed.

B. The Singapore PDPA

Singapore is the key partner to India in arbitration matters with the Singapore International Arbitration Centre (SIAC) being able to claim that it handles the highest volume of India related matters compared to all other international arbitral institutions [31]. Consequently, the Personal Data Protection Act 2012 (Singapore PDPA), as amended by the Personal Data Protection (Amendment) Act 2020, acquires practical importance in cases of disputes resolved through SIAC [32]. The Singapore PDPA concerns organisations collecting, using, and disclosing the personal data of individuals in Singapore. According to this law, personal data can be used for the sole purposes of collection and for which consent was provided.

Most critically, the Singapore PDPA includes an explicit exemption for legal proceedings within its Second Schedule, allowing the collection, use, and disclosure of personal data without the need for consent where such is required for the purposes of legal proceedings, compliance with law, or investigation [33]. This specific exception is much clearer for arbitral parties than the vague compliance with law basis of section 7(e) of the DPDP Act. In addition, the Personal Data Protection Commission of Singapore (PDPC) has provided guidance on the PDPA's applicability to legal proceedings, including procedures for document production and treatment of witnesses during arbitration [34]. Such sectoral guidance has not been issued by any Indian regulatory authority in relation to the DPDP Act.

Regarding transfers across borders, the Singapore PDPA mandates (as per section 26) that an organization which is engaged in transferring personal data outside of Singapore ensures that there is a comparable standard of protection available from the party receiving the personal data in the same way as guaranteed under the PDPA [35]. The PDPC has also provided guidelines for assessing the effect of a transfer as well as the drafting of standard model contract clauses for purposes of data protection. This represents a more mature approach towards cross-border transfers than the current one offered by the DPDP Act.

C. Hong Kong PDPO

The third example of a jurisdiction in which data privacy may impact an arbitration proceeding having an Indian nexus is Hong Kong. As a leading arbitration forum for Asian and China-related disputes, Hong Kong also offers another layer of data protection laws that could be relevant. The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO), promulgated in 1995 and substantially amended in 2021, covers data users engaged in the process of collecting, retaining, processing, or using personal data in Hong Kong [36]. Similar to the DPDP Act, the PDPO does not grant any exemptions for proceedings of a legal nature, but only provides for such in connection with Data Protection Principle 3 of the Ordinance, which restricts the purposes of the processing of personal data to the purposes for which it was initially collected [37].

IV. Comparative Analysis

Comparing the four regimes, one can observe an interesting convergence regarding key fundamentals of data privacy protection such as consent/prescribed legal basis, purpose limitation, data security requirements, cross-border transfer restrictions, and the set of data subjects rights, while significant divergences exist in implementation details, which are vital to arbitrators [38]. As far as fundamental provisions are concerned, the DPDP Act shares similarities with the GDPR, due to a focus on data subjects' rights and introduction of a data fiduciary/data processor distinction, but differs from the GDPR in terms of three crucial elements: less generous grounds of legitimate uses (no legitimate interests basis), no derogations for legal proceedings (in contrast to Article 17(3)(e) of the GDPR), and less advanced regulation of cross-border data transfers (compared to GDPR Chapter V) [39]. The exception for legal proceedings in the Singapore PDPA and the legitimate interests basis in the GDPR cover the shortcomings of the DPDP Act in that regard. A data fiduciary adhering to the GDPR may fail to comply with the DPDP Act where legitimate interest constitutes the only available processing ground under the latter legislation.

V. Compliance Difficulties in the Nexus Between Data Protection and Arbitration Proceedings

A. Legal Bases for Processing Personal Data

The first and foremost compliance difficulty faced by the arbitrating parties under the DPDP Act arises in relation to establishing legal bases for processing personal data at each step of the arbitral process [40]. The pre-arbitration stage, where the parties collect information,

make out witnesses, conduct due diligence, and prepare their cases, is the most complicated legally speaking. Processing of personal data of possible witnesses, adversaries, and third parties takes place without their consent at this stage, and this processing cannot be described as processing for the purpose of compliance with any law, since the arbitration proceedings have not yet been initiated [41].

A certain clarity is achieved once the arbitral proceedings have been formally instituted. After this stage, it becomes easier to resort to section 7(e) of the DPDP Act for the basis of processing; this is because there exists a statutory authority to conduct such proceedings, and following the directions issued by the arbitral tribunal implies compliance with an obligation imposed by Indian law. For arbitration proceedings where the procedural law originates from foreign jurisdiction and where the seat of arbitration is abroad, the basis of compliance with Indian law will be rather difficult to justify, and consent and contractual terms could prove helpful instead.

B. The Confidentiality Transparency Dilemma

In terms of the obligations of data fiduciaries to be transparent, there is a fundamental conflict between data protection laws and the concept of arbitral confidentiality. Section 5 of the DPDP Act places an obligation on data fiduciaries to notify the data principal of data processing and its purpose(s) before or at the moment of processing the data [42]. However, due to the confidentiality requirements of the arbitral process, as contained in the rules of arbitral institutions, arbitral agreement provisions, and arbitral decisions, there would be restrictions on notifying potential witnesses, former employees, or data principals whose data is being processed without being a party to the arbitral process that their data is being processed.

The above mentioned conflict is not only pertinent to the Indian scenario; similar conflicts can emerge under the GDPR and the Singapore PDPA too. The GDPR's Article 14(5)(d), which allows for an exception from the requirement to provide transparency information if such information would make it impossible or seriously impede the fulfillment of the purpose of the processing activity, according to some observers, extends even to litigation and arbitration settings [43]. There is no corresponding provision under the DPDP Act, thus leaving parties in arbitration vulnerable unless the DPBI provides sectoral guidance acknowledging this legitimate conflict between transparency and confidentiality in private hearings [44].

C. Data Subjects Rights During and after Proceedings

The invocation of data subjects rights specifically, their right to access, under Section 11 of the DPDP Act, and their right to be forgotten, under Section 12—during various stages of arbitral proceedings poses significant procedural challenges which remain unresolved under Indian law [45]. The filing party will be faced with a difficult dilemma, if the witness, whose data is included in a witness statement filed during ongoing proceedings, invokes his/her right to erasure prior to the hearing, because this would either lead to the breach of directions given by the tribunal in its procedure, or even contempt of court in set-aside or enforcement proceedings; or else, the party risks regulatory penalties and civil actions under the DPDP Act.

However, in the GDPR, this conflict is addressed by Article 17(3)(e), which allows for exceptions to the right to erasure in cases where the processing of personal data is necessary for the establishment, exercise or defence of legal claims [46]. The application of this article can be seen even in the context of arbitration by data protection supervisory authorities in Europe. However, no such derogation clause exists within the DPDP Act. On the ground, data fiduciaries have the choice between obtaining explicit contractual waivers to the right to erasure from witnesses and other data principals whose data are processed by them (which has additional legal issues surrounding consent and fairness) or an implicit statutory derogation under the Arbitration and Conciliation Act.

D. Restrictions on Cross-Border Data Transfers and the Use of Cloud-based Arbitration Services

The aspect of the DPDP Act that creates the biggest problem operationally in connection with international arbitration is the possible prohibition against cross-border transfers of data pursuant to Section 16 [47]. International arbitrations involve the transfer of Indian personal data not only to foreign arbitrators, foreign counsel, foreign institution secretariats, but also foreign electronic discovery companies. If any of these organizations were based in any countries subsequently notified by the Central Government as restricted jurisdictions, such transfers of data would either need express consent from the data principals or would have to be modified operationally.

Another aspect related to this question, albeit one with technical considerations at play, is whether cloud-based dispute resolution service providers that maintain data storage in

multiple jurisdictions should be treated in any different way than those that store data on a single jurisdiction basis. Documents filed in the NetCase platform maintained by the ICC and the SIAC's e-filing platform could be stored on servers in Frankfurt, Dublin, Dallas, or Singapore, among other cities, based on the particular design of the system [48]. The use of cloud-based services could result in the transfer of personal data from India to another future notified country restricted under the DPDP Act without the knowledge of the users involved. This risk of incidental data transfer is not considered in the DPDP Act's data transfer provisions, nor is there a contract-based safe harbour solution in place like the GDPR's standard contractual clause.The Permanent Court of Arbitration's Cybersecurity Protocol for Arbitration Proceedings is an example to consider here [49].

E. Conflict of Laws

In instances where the DPDP Act overlaps with a foreign data protection law, which would be common practice when arbitrating cases involving India, the following conflict of laws issue becomes relevant [50]. The DPDP Act will always apply as the law of the country in which the Indian data principal resides; the foreign data protection law will always apply as the law of the country in which the foreign data fiduciary operates. If these two overlapping laws happen to place different obligations on the fiduciary—if, say, one says that specific records must be retained for a certain period of time, but the other says these same records should be deleted—then the data fiduciary has to make a choice about compliance with one of the regimes but not the other.

None of the Indian courts has yet adjudicated upon conflict of laws principles in relation to the DPDP Act. Applying by analogy principles that have been laid down with respect to the regulation of finance and competition, the more reasonable position would be for the data fiduciaries to adhere to the stricter regime of the two regimes where both could be complied with, while seeking guidance from the regulators in case there exists an insurmountable conflict between the two regimes . In the arbitration context, therefore, it would make good sense to ensure that the Indian compliance with the data protection provisions be structured on the GDPR regime, as the stricter and more developed regime, keeping in mind the practical position that GDPR compliance would ordinarily amount to compliance with the DPDP Act provisions, with the sole exception being the provision regarding legitimate interests.

VI. Conclusion

The Digital Personal Data Protection Act 2023 is arguably the largest step taken by India to date in enacting legislation aimed at creating an internationally compliant data regime. Enactment of such legislation is desirable, and perhaps necessary, in light of the growing reliance upon personal data within today's internationalized economy. Yet, as shown in this paper, in its current form, the Act raises serious questions relating to the ability to navigate compliance issues in relation to cross-border arbitrations. The failure to provide derogations from the legislation in respect of legal proceedings, the development of an inadequate cross-border transfer regime, lack of provision for legitimate interests processing, and the failure to consider conflict of laws are just some of these issues.

The solution is found through legislative amendment, regulatory action including sectoral guidelines, positive transfer provisions, explicit derogation from legal proceedings in relation to legal proceedings, and self-regulatory adaptation by the arbitral community including tribunals, practitioners, and parties. It is important that the arbitral community understands the importance of incorporating data protection compliance as part of the arbitral regime. The Indian judicial and arbitral institutions will in due course develop the necessary jurisprudence to fill in the gaps in the Act. Until such time, the arbitral community needs to carefully address the interface between the DPDP Act and international arbitration practice. With proper implementation of the DPDP Act 2023, India can be not only compliant in terms of international standards but also a leader in the development of data norms in international arbitration practice.

CITATIONS

STATUTES AND LEGISLATIVE MATERIALS

1. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
2. Arbitration and Conciliation Act, No. 26 of 1996, India Code (1996).
3. Digital Personal Data Protection Act, No. 22 of 2023, § 3, India Code (2023).
4. Digital Personal Data Protection Act, No. 22 of 2023, § 7(e)-(f), India Code (2023).
5. Digital Personal Data Protection Act, No. 22 of 2023, §§ 11-14, India Code (2023).
6. Digital Personal Data Protection Act, No. 22 of 2023, §§ 8(3), 8(5)-(8), India Code (2023).
7. Digital Personal Data Protection Act, No. 22 of 2023, § 16, India Code (2023).

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
9. GDPR art. 3(2).
10. GDPR art. 6(1)(c), (f).
11. GDPR art. 17(3)(b), (d), (e).
12. GDPR arts. 44-49.
13. Personal Data Protection Act 2012 (Act No. 26 of 2012) (Sing.).
14. Personal Data Protection (Amendment) Act 2020 (Act No. 40 of 2020) (Sing.).
15. Personal Data (Privacy) Ordinance (Cap. 486) (H.K.).
16. Personal Data (Privacy) (Amendment) Ordinance 2021 (H.K.).

BOOKS AND TREATISES

17. Gary B. Born, *International Commercial Arbitration* 2779-2812 (3d ed. 2021).
18. Nigel Blackaby, Constantine Partasides, Alan Redfern & Martin Hunter, *Redfern and Hunter on International Arbitration* 391-445 (7th ed. 2023).
19. Christopher Kuner, *Transborder Data Flows and Data Privacy Law* 147-183 (2013).
20. Peter P. Swire & Kenesa Ahmad, *Foundations of Information Privacy and Data Protection* 201-230 (2012).
21. Julian D.M. Lew, Loukas A. Mistelis & Stefan M. Kroll, *Comparative International Commercial Arbitration* (2003).
22. Margaret L. Moses, *The Principles and Practice of International Commercial Arbitration* (4th ed. 2024).
23. Emmanuel Gaillard & John Savage eds., *Fouchard Gaillard Goldman on International Commercial Arbitration* (1999).
24. David St. John Sutton, Judith Gill & Matthew Gearing, *Russell on Arbitration* (25th ed. 2024).
25. Richard Garnett, *Substance and Procedure in Private International Law* (2012).

JOURNAL ARTICLES

26. Rishad Chowdhury & Udbhav Tiwari, India's Personal Data Protection Framework: An Analysis of the DPDP Act 2023, 15 Indian J.L. & Tech. 45 (2023).
27. Nappinai N.S., Data Protection Law in India: Implications of the DPDP Act 2023, 58 J. Indian L. Inst. 203 (2023).
28. Simon Busuttil, Data Protection in Arbitration: Balancing Privacy, Confidentiality and Due Process, 34 Arb. Int'l 611 (2018).
29. Luca Beffa & Remy Patry, Data Protection in International Arbitration: Practical Guidance for Practitioners, 36 ASA Bull. 262 (2018).
30. Kabir Duggal & Natasha Mellersh, Protecting Personal Data in International Arbitration: A Compliance Framework, 12 Contemp. Asia Arb. J. 33 (2019).
31. Fiona Reith, GDPR and International Commercial Arbitration: Navigating the Interface, 33 Mealey's Int'l Arb. Rep. 1 (2018).
32. Samaa Haridi & Lee Rovinescu, Data Privacy Compliance in International Arbitration: Emerging Issues, 37 J. Int'l Arb. 85 (2020).
33. Valentina Ruhl, The Impact of the GDPR on International Arbitration Proceedings: Practical Guidance, 22 Eur. Bus. L. Rev. 563 (2020).
34. A. Vishwanath, The Digital Personal Data Protection Act 2023: Mapping the Contours of India's Data Governance Framework, 58 Econ. & Pol. Wkly. 22 (2023).
35. Bernardo Sepulveda-Amor, Data Protection in Arbitration: Perspectives from Arbitral Practice, in *Privacy and Data Protection in International Investment Law* 201 (Markus Krajewski & Rhea Hoffmann eds., 2022).
36. Catherine Rogers, Transparency and Confidentiality in International Arbitration, 54 Harv. Int'l L.J. 1 (2013).
37. Stavros Brekoulakis, International Arbitration and Public Policy, 27 Arb. Int'l 121 (2011).
38. Jan Paulsson, Arbitration in Three Dimensions, 60 L. & Contemp. Probs. 291 (1997).
39. Gabrielle Kaufmann-Kohler & Michele Potestà, Can the Mauritius Convention Serve as a Model for the Reform of Investor-State Arbitration?, 20 ICSID Rev. 74 (2015).
40. David J. McLean, Data Protection and Cross-Border Litigation, 16 Int'l J.L. & Info. Tech. 211 (2008).

INSTITUTIONAL RULES, GUIDELINES, AND REPORTS

41. Int'l Chamber of Commerce, *Note to Parties and Arbitral Tribunals on the Conduct of Arbitration Under the ICC Rules of Arbitration* (2021).
42. Int'l Bar Ass'n, *IBA Rules on the Taking of Evidence in International Arbitration* (2020).
43. Singapore Int'l Arb. Ctr., *Practice Note on the Conduct of Arbitral Proceedings* (2023).
44. London Court of International Arbitration, *Casework Connect: Data Processing Framework* (2022).
45. Hong Kong Int'l Arb. Ctr. & Singapore Int'l Arb. Ctr., *Guidance Note on Data Protection in Arbitration* (2021).
46. Permanent Court of Arbitration, *PCA Cybersecurity Protocol for Arbitration Proceedings* (2020).
47. Personal Data Protection Commission, Singapore, *Advisory Guidelines on the PDPA: Legal Proceedings* (2021).
48. European Data Protection Board, *Guidelines 05/2021 on the Interplay Between Article 3 and Chapter V of the GDPR* (2021).
49. Ministry of Electronics and Information Technology, Government of India, *Report of the Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna* (2018).
50. Law Commission of India, *Amendments to the Arbitration and Conciliation Act, 1996*, Report No. 246 (2014).