DATA PROTECTION, CYBERSECURITY AND INTERNATIONAL ARBITRATION: CAN THEY RECONCILE?

*Ananya Bajpai & Shambhavi Kala**

Abstract

*For the past few years, international arbitration has been on an upward surge. It has grown exponentially, becoming a preferred forum of dispute settlement. Simultaneously, data protection and cybersecurity have been at the fore of discussion globally, with the enactment of the General Data Protection Regulation ["**GDPR**"] in the European Union ["**EU**"], the right to privacy being declared a fundamental right in India, and jurisdictions like India modelling their law on the GDPR. The time has come for the intersection of both these fields to be considered seriously. The International Council for Commercial Arbitration ["**ICCA**"] and the International Bar Association ["**IBA**"] have formed a task force to investigate the question of data protection in international arbitration, and a Cybersecurity Protocol has been released by the ICCA in conjunction with the New York City Bar Association ["**NYC Bar**"] and International Institute for Conflict Prevention and Resolution ["**CPR**"]. These positive developments show the way forward for arbitration and data protection. In this paper, the authors analyse these developments, assess the status of data protection and information security in arbitration, and provide some suggestions about the way forward.*

I. Introduction

The right to privacy was first advocated by Samuel Warren and Louis Brandeis in their article on "The Right to Privacy" published in 1890.[1] They argued that privacy was a "right to be let alone" as instantaneous photographs and newspaper enterprises began invading the sacred precincts of private and domestic life.[2] In 1948, the Universal Declaration of Human Rights ["**UDHR**"] declared the right to privacy as a fundamental right.[3]

Meanwhile, the EU sought to develop its privacy law in the form of Data Protection Directive 95/46/EC ["**Directive**"] in 1995.[4] The Directive sought to protect the processing of personal data of individuals, but required that the EU Members come up with their own national laws pursuant to the Directive.[5] Thereafter, the European Commission sought to unify data protection law across the EU through the GDPR. The GDPR aims to harmonize 27 national regulations on data

---

* Editors-in-Chief for Volume 8 of the Indian Journal of Arbitration Law (IJAL). The authors are in the final year of B.A. LL.B. (Hons.) at National Law University, Jodhpur (India).

1 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

2 *Id.* at 195.

3 G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948), art. 12.

4 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [*hereinafter* "EU Directive"]; Consolidated Version of the Treaty on the Functioning of the European Union, art. 288, Oct. 26, 2012, 2012 O.J. (C 326) [*hereinafter* "TFEU"].

5 EU Directive, *supra* note 4, art. 4(1).

protection into one, improve data transfer rules for EU citizens outside the EU, improve user control over data and guarantee a stronger protection of personal data.[6]

In India, data protection was not given similar importance until very recently. The government amended the Information Technology Act, 2000 which provided citizens a right to be compensated for improper disclosure of information.[7] Subsequently, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 imposed additional requirements on business and commercial entities for collection and disclosure of sensitive personal data.[8] In 2016, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act was passed, which required the telecom and the financial services sectors to keep their customers' personal information confidential.[9] In 2017, the Supreme Court of India delivered the landmark judgment, *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*, which held that the right of privacy is a fundamental right emanating from Article 21 of the Indian Constitution.[10] The court pronounced that the protection of informational privacy from both the State and private actors was necessary and for the common good, and was catalytic in providing for a robust regime of data protection in India.[11] Thereafter, the government of India constituted a Committee of Experts under the Chairmanship of Justice B.N. Srikrishna to prepare a report on the draft Data Protection Bill, 2018, which submitted a draft of the Personal Data Protection Bill in July, 2018 ["**2018 Bill**"].[12] The Ministry of Information and Technology solicited comments and suggestion on the 2018 Bill from various stakeholders, and based on the suggestions, the Union Cabinet cleared the Personal Data Protection Bill, 2019 [the "**Bill**"].[13] The Bill is currently awaiting a report from the Joint Parliamentary Committee after which it shall be debated and discussed in the parliament.[14]

International arbitration often has actors and players that handle personal data from varied jurisdictions. Owing to different national regimes, transfer of data across the borders through different layers and heavy penalisation for non-compliance with data protection laws, it becomes imperative that international arbitration arms itself with a robust and consistent framework for data protection. This paper seeks to highlight how multiplicity in data protection regimes and the lack of arbitration specific data protection laws can create complications and confusion in

---

6 European Commission Press Release IP/12/46, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Business (Jan. 25, 2012).

7 The Information Technology Act, 2000 (as amended by the Informational Technology Amendment Act, 2008), No. 21 of 2000, §§ 43A. 72A. (India).

8 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R. 313(E) (India).

9 Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18 of 2016, § 29. (India).

10 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 188 (India) [*hereinafter* "Puttaswamy."].

11 *Id.* ¶ 190; WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA 4 (2018).

12 COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS [*hereinafter* "Srikrishna Committee Report"]; Personal Data Protection Bill, 2018 (India).

13 Personal Data Protection Bill, No. 373 of 2019 (India) [*hereinafter* "PDP Bill"].

14 Arindrajit Basu & Justin Sherman, *Key Global Takeaways From India's Revised Personal Data Protection Bill*, LAWFARE (Jan. 23, 2020), *available at* https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill.

international arbitration. For this purpose, the authors have focussed on how (two recent legislations,) the 2019 Indian Bill on Personal Data Protection and the GDPR, affect international arbitration.

This paper is divided into six parts. **Part II** explains the EU's GDPR, its basic principles, concepts and requirements in the context of international arbitration. Thereafter, **Part III** analyses the Roadmap provided by the ICCA-IBA Joint Task force which guides various participants in international arbitration regarding data protection. It shall also analyse privacy rules of arbitral institutions and delve into the protocol on cybersecurity in International Arbitration published by the ICCA, the NYC Bar and the CPR with the support of the Permanent Court of Arbitration ["**PCA**"] and analyse privacy rules of arbitral institutions as well. In **Part IV**, the authors shall discuss the Indian Data Protection Bill, 2019 and the consequences for international arbitration, if any. **Part V** then contemplates fundamental questions regarding the multiplicity of data protection regimes and its impact on international arbitration. Finally, the authors provide their conclusions in **Part VI**.

II. The General Data Protection Regulation

In 2018, the GDPR took effect, replacing the Directive which came into force in 1995 in the EU. The GDPR seeks to strengthen the protection of the individual's right to personal data protection and considers it a fundamental right.[15] The GDPR establishes the following basic principles:[16]

(i) That personal data shall be processed in a fair, lawful and transparent manner (lawfulness, fairness and transparency);
(ii) That personal data shall be collected for specific, explicit and legitimate purpose and cannot be further processed in a manner that is not compatible with such purposes (purpose limitation);
(iii) That personal data shall be adequate, relevant and limited to the purposes necessary for which they are processed (data minimisation);
(iv) That personal data shall be accurate and up-to-date (accuracy);
(v) That personal data shall not be stored for longer than is necessary for the purposes for which the personal data is processed (storage limitation);
(vi) That personal data shall be processed in a manner that ensures appropriate security of the personal data, which includes protection against unauthorized or unlawful processing (integrity and confidentiality); and
(vii) Responsibility of the controller to demonstrate compliance with the above six principles (accountability).

---

15 Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation), pmbl. (1), 2016 O.J. (L 119) [*hereinafter* "GDPR"].

16 *Id.* art. 5.

The GDPR places various obligations upon the data controller. It defines a 'controller' as any person, authority, agency or body which determines the means and purposes of the processing[17] of personal data[18] and a 'processor' as a person or any other authority, agency or body which processes data on behalf of the controller.[19] Additionally, a controller or processor is considered to be established in the EU if it exercises effective and real activities through stable arrangements in the EU.[20]

As per Opinion 1/2010 on the concepts of "controller" and "processor", solicitors and barristers could be considered as controllers.[21] Drawing the same analogy, the ICCA-IBA Roadmap to Data Protection in International Arbitration ["**Roadmap**"] states that parties, their legal counsels, arbitrators and arbitral institutions may be considered controllers (also referred to as "Arbitral Participants").[22]

Arbitral Participants would therefore be required to fulfil certain key requirements. The GDPR requires the consent of the 'data subject' to the processing of his/her personal data[23] and assuming that Arbitral Participants are controllers, they will have the primary responsibility to demonstrate that the data subject consented to the processing.[24] They will also have the obligation to inform the data subject about the processing of his/her personal data,[25] keep record of processing activities,[26] handle requests for exercising the data subject's rights[27] and implement appropriate measures to ensure security of the personal data that is processed.[28] Moreover, Arbitral Participants will have to notify the supervisory authority within 72 hours in case of a data breach.[29]

International arbitration is document intensive. Even before the matter is taken up by the arbitral tribunal, parties have to collect documents (which falls under the definition of 'processing') and inevitably contain personal data. Parties also communicate with solicitors, legal counsels, experts, opposing party, arbitrators etc. and transfer certain personal data to them. Parties shall have to

---

17 Processing has been defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." *See* GDPR, *supra* note 15, art. 4(2).

18 *Id.* art. 4(7); The GDPR defines personal data in a very broad manner. Personal data would mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." *See id.* art. 4(1).

19 *Id.* art. 4(8).

20 *Id.* recital 22.

21 *Opinion of the Working Party on the Protection of Individuals with regard to the processing of personal data on the "concepts of "controller" and "processor""* 2010 WP 169 28.

22 THE ICCA-IBA JOINT TASK FORCE ON DATA PROT. IN IN INT'L ARB., THE ICCA-IBA ROADMAP TO DATA PROTECTION IN INTERNATIONAL ARBITRATION 9 (2020) [*hereinafter* "ICCA-IBA ROADMAP"].

23 GDPR, *supra* note 15, art. 6(1).

24 *Id.* art. 7(1).

25 *Id.* art. 12, 13 and 14.

26 *Id.* art. 30.

27 *Id.* art. 15-22.

28 *Id.* art. 32.

29 *Id.* art. 33(1).

ensure compliance at each stage. Once such data is transferred, the relevant Arbitral Participant shall have to ensure that the personal data is still compliant with the GDPR as well.

A peculiar feature of the GDPR is the provision with respect to transfer of data outside the EU. It requires an 'adequacy decision' to be made by the European Commission regarding a third country's level of protection.[30] In case a third country's data protection is considered 'adequate', such a transfer will be treated like transmission of data within the EU and the data exporter need not provide additional safeguards.[31] So far, the European Commission has recognized countries such as U.S.A (limited to Privacy Shield framework),[32] Canada, Japan, Switzerland, New Zealand, Uruguay, Isle of Man, Jersey, Andorra, Faroe Islands, Guernsey, Israel and Argentina as providing adequate protection.[33] India also plans to approach the EU for an 'adequacy' status once it passes its Personal Data Protection Bill, 2019.[34]

Alternatively, in the absence of an 'adequacy decision', a data exporter may still transfer data by employing appropriate safeguards and if there are enforceable rights and effective legal remedies available to the data subject. Such safeguards include binding corporate rules, standard data protection clauses, and approved code of conduct or certification mechanisms with binding and enforceable commitments of the controller or the processor in the third country.[35]

Finally, in the absence of an 'adequacy decision' and safeguards, the GDPR allows for derogation, *inter alia*, if such transfer is necessary for the establishment, exercise or defence of a legal claim.[36]

As per the Roadmap, the legal claims derogation will be applicable to international arbitration.[37] However, the transferor of such data will still have to ensure that the level of protection guaranteed under the GDPR is not undermined.[38] For instance, the transferor will have to ensure that transfer of personal data is adequate, relevant and limited to what is necessary with the purpose of processing such data.[39] Arbitral Participants are advised to identify and document at the outset of the proceedings the data that will be needed to be processed and the lawful basis that the Participants may rely on.[40] While the GDPR does consider consent as a valid ground for data

---

30 GDPR, *id.* art. 45.

31 *What Rules Apply if my Organisation Transfers Data outside the EU?*, EUR. COMM'N, *available at* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en.

32 The EU-US Privacy Shield Framework came up in 2016 to replace the US-EU Safe Harbor Framework. It creates a mechanism to comply with data protection requirements when transferring personal data from the EU to the United States of America. *See EU-U.S. Privacy Shield Framework Principles*, U.S. DEP'T OF COMM. (2016), *available at* https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.

33 *Adequacy Decisions*, EUR. COMM'N, *available at* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

34 Megha Mandavia, *India to Approach the EU Seeking 'Adequacy' Status with the GDPR*, ECON. TIMES (July 30, 2019), *available at* https://tech.economictimes.indiatimes.com/news/internet/india-to-approach-the-eu-seeking-adequacy-status-with-the-general-data-protection-regulation/70440103.

35 GDPR, *supra* note 15, art. 46(2).

36 *Id.* art. 49(1)(e).

37 ICCA-IBA ROADMAP, *supra* note 22, at 12.

38 GDPR, *supra* note 15, art. 44.

39 *Guidelines 2/2018 on Derogation of Article 49 under Regulation 2016/679*, EUR. DATA PROT. BD., 12 (May 25, 2018), *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

40 ICCA-IBA ROADMAP, *supra* note 22, at 18.

processing, Participants may look for other lawful grounds as consent can be refused or withdrawn at any time.[41] Other issues with consent as a lawful basis have been identified by the Roadmap and discussed below.

A concern that still remains is regarding the application of the GDPR. The GDPR has expanded the territorial scope of EU's data protection regime. The GDPR applies to the processing of personal data[42] by a controller or a processor established *in the EU*[43] or where the processing activities are relating to the offering of goods or services to *individuals in the EU*.[44] Further, the NAFTA Tribunal, constituted by the PCA with an EU arbitrator, in *Tennant Energy* v. *Canada* has held that arbitration under the NAFTA, a treaty to which the EU is not a party, does not come within the material scope of the GDPR,[45] despite the Roadmap considering otherwise due to the extra-territorial reach of the GDPR.[46] Interestingly, the Tribunal did not consider that it was constituted by the PCA, an international organisation,[47] and would thus, be subjected to the transfer rules as per the GDPR.[48]

Such contrary holdings shall surely add to the uncertainty regarding the application of the GDPR; Arbitral Participants would be advised to err on the side of caution and incorporate the protection required under the regime as data infringement would cost a fine between €10 to €20 million or 2 to 4% of worldwide annual revenue.[49]

A more detailed discussion on the data protection concerns that arise in arbitration has been conducted by the ICCA and IBA based on the GDPR. This has been analysed in the following section.

III. Guiding International Arbitration through Data Protection Regimes and Cybersecurity Issues

The ICCA and the IBA formed a joint task force to investigate the application of data protection principles in international arbitration.[50] A draft was released for public consultation in February, 2020. The Roadmap uses the GDPR as the basis for its inferences, since it is amongst the most "comprehensive and onerous" regulations in place in the world.[51] Using the principles of the

---

41 *Id.* at 17.

42 The GDPR defines personal data as "any information relating to an identified or identifiable natural subject", *see* GDPR, *supra* note 15, art. 4(1).

43 *Id.* art. 3(1).

44 *Id.* art. 3(2)(a). It also applies to monitoring of behaviour of data subjects in the European Union, *see id.* art. 3(2)(b).

45 *See* Tennant Energy, LLC (U.S.A.) v. Gov't of Can., PCA Case No. 2018-54, Tribunal's Communication to the Parties (Perm. Ct. Arb., 2019). Article 2(a) elaborates upon the material scope of the GDPR ("This Regulation does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law"). Interestingly, the tribunal did not consider that it was constituted by the Permanent Court of Arbitration, an international organisation (art. 4(26)), and would thus, be subjected to the transfer rules as per the GDPR (art. 42).

46 *See id.* art. 3; ICCA-IBA Roadmap, *supra* note 22, at 7-8.

47 GDPR, *supra* note 15, art. 4(26).

48 *Id.* art. 42.

49 *Id.* art. 83(2)(a).

50 *ICCA-IBA Joint Task Force on Data Protection in International Arbitration Proceedings*, INT'L COUNCIL FOR COMM. ARB., *available at* https://www.arbitration-icca.org/projects/ICCA-IBA_TaskForce.html.

51 *Id.* at 3.

GDPR, the Roadmap addresses data protection concerns which may arise in arbitration and devises 'practice tips' to assist professionals navigate such concerns.

On the specific point of cybersecurity, the ICCA has, in conjunction with the NYC Bar Association and the International Institute for Conflict Prevention and Resolution and with the support of the PCA, released the Protocol on Cybersecurity in International Arbitration ["**the Protocol**"].[52] This Protocol sets out principles of cybersecurity and is intended to act as a guide for information security risks and measures which can be implemented in arbitration. It does not contain a one-size-fits-all approach and allows parties to individualise the measures as per their requirements.[53]

This section analyses the Roadmap and the Protocol's directions for participants of international arbitration.

A. The ICCA-IBA Roadmap on Data Protection in International Arbitration

One of the primary concerns associated with data protection in arbitration is whether any type of arbitration is excluded from the application of data protection regulations. The answer to this question will generally vary from jurisdiction to jurisdiction. For example, in the EU, the GDPR excludes the processing of personal data when it is done outside the scope of EU law,[54] which may be the case in an arbitration where parties have chosen non-EU law to govern their dispute. However, as has been pointed out in the Roadmap, due to the extra-territorial reach of the GDPR,[55] if any of the Arbitral Participants are subject to the GDPR, they will have to process data in accordance with it.[56]

A distinction may also be drawn with respect to the type of arbitration. For example, in case of an investor-State arbitration, an international organisation may be at the helm, for example the International Centre for Settlement of Investment Disputes ["**ICSID**"] or the PCA. The question then arises – are such organisations excluded from the application of data protection law? The Roadmap states that in such cases, there may be special privileges or immunities in the treaties that constitute these international organisations, as a result of which arbitrators and counsel may be excluded from the scope of data protection laws.[57] For example, the Convention for the Pacific Settlement of International Disputes, 1899, provides members of the PCA with diplomatic immunities and privileges.[58] This is echoed in the Convention for the Pacific Settlement of International Disputes, 1907.[59] However, whether these privileges and immunities would protect arbitrators from data protection regulations is an unsettled question.

---

52 ICCA-NYC BAR-CPR CYBERSECURITY PROTOCOL FOR INTERNATIONAL ARBITRATION, ICCA-NYC BAR-CPR WORKING GROUP ON CYBERSECURITY IN ARBITRATION (2020), *available at* https://www.arbitration-icca.org/media/14/76788479244143/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf [*hereinafter* "ICCA-NYC BAR-CPR PROTOCOL"].

53 *Id.* at 7, 16.

54 *See* GDPR, *supra* note 15, art. 2(a).

55 *See id.* art. 3.

56 ICCA-IBA ROADMAP, *supra* note 22, at 7-8.

57 *Id.* at 37.

58 Convention for the Pacific Settlement of International Disputes art. 24, July 29, 1899, 1 A.J.I.L. 103 (1907).

59 Convention for the Pacific Settlement of International Disputes art. 46, Oct. 18, 1907, 2 A.J.I.L. Supp. 43 (1908).

The Roadmap is applicable to 'Arbitral Participants', which includes the parties, their counsel, the arbitrators, and arbitral institutions. However, the information in the Roadmap may also be pertinent to other entities involved in an arbitration, such as tribunal secretaries, experts, and other service providers.[60] Therefore, the inferences drawn in the Roadmap have to be assessed with regards to the impact they will have on Arbitral Participants and associated entities.

While the Roadmap specifies certain entities which may be involved in the arbitration and therefore affected by data protection obligations, there may be other entities who have access to data in an arbitration. These include third party funders, who may be financially supporting the claim of an impecunious claimant. Could third party funders be classified under 'service providers'?[61] While this is an unanswered question in the Roadmap, it does state that when arbitration-related information containing personal data[62] is shared with a third party, this constitutes processing,[63] which requires compliance with data protection law. Therefore, in an arbitral proceeding, where each entity involved collects some personal data from the other (claimant from the respondent, tribunal from the parties, experts from the parties, and so on), data protection obligations would be incumbent upon them. Arbitral Participants ought to be cognizant of these obligations from the outset and develop a framework to comply with them.

Another pertinent point highlighted by the Roadmap is that of third country data transfers. The GDPR stipulates conditions for third country transfers, which have been discussed above. These restrictions become particularly relevant when considered in light of jurisdictions which have data localisation regimes in place. For example, the Reserve Bank of India released norms in April 2018 which require system providers operating payment systems to ensure that all payments data are stored in a system only in India ["**RBI Notification**"].[64] The RBI has also clarified that data may be shared with overseas regulators, if so required, depending upon the nature and origin of transaction with due approval of the RBI.[65] Similarly, Vietnamese law stipulates that domestic and foreign service providers on telecommunication networks and on the Internet, and cyberspace service providers carrying out activities of collecting, using, analysing and processing personal data, data about users' relationships and data generated by them, must store such data in Vietnam for a specified period.[66]

Let us consider a situation where an Indian payments operator (such as Paytm) is involved in a dispute with a foreign party, with the International Court of Arbitration at the International

---

60 ICCA-IBA Roadmap, *supra* note 22, at 2.

61 The Roadmap provides "e-discovery experts, information technology professionals, court reporters, translation services, etc." as examples of service providers.

62 GDPR, *supra* note 15, art. 4(1).

63 *Id.* art. 4(2). It is relevant to note that processing includes collection and storage. Therefore, in a situation where the third party funder collects identifiable information relating to a natural person, they would have to comply with data protection obligations.

64 RESERVE BANK OF INDIA, Storage of Payment System Data, RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018 (Apr. 6, 2018.). However, it ought to be noted that this restriction applies only to domestic operations. For cross border payment transactions, the data may also be stored abroad. *See Frequently Asked Questions, Storage of Payment System Data*, RESERVE BANK OF INDIA, *available at* https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130 [*hereinafter* "FAQ"].

65 *See* FAQ, *id.* item 7.

66 Law on Cybersecurity, No: 24/2018/QH14, art. 26(3) (2018) (Viet.).

Chamber of Commerce ["**ICC**"] administering the dispute. It is conceivable that Paytm would have transfer some amount of personal data (for example, with relation to its employees) abroad for the adjudication of the dispute. Whether the ICC would be considered an 'overseas regulator' for the purposes of the RBI Notification is unclear. Further, obtaining approval of the RBI would be a time-consuming roadblock in the arbitration. The Roadmap takes note of the possibility of such restrictions and advises that Arbitral Participants identify these at the outset and devise steps to transfer data in compliance with them.[67] However, in the absence of an exception pertaining to legal proceedings, it is unclear how data transfers can take place in compliance with data localisation norms. Clearer regulations would pave the way for smoother arbitral proceedings, and in this regard, it may be beneficial for jurisdictions to consider a straightforward legal derogations exception for data transfers in their data protection regulations.

The Roadmap also acknowledges certain data protection principles, which it considers universal[68] - consisting of fair and lawful processing, proportionality, minimisation, purpose limitation, data subject rights, accuracy, data security, and transparency. It analyses the issues that could arise with respect to the application of these principles in the context of an arbitration. For example, the GDPR considers 'consent' to be a lawful basis of processing.[69] Consent under the GDPR must be freely given, specific, informed, and an unambiguous indication of the data subject's agreement to the processing of their personal data. Also, this consent can be withdrawn at any point.[70] While this seems straightforward, the Roadmap does not consider consent to be an appropriate basis for processing[71] – it raises a variety of issues.[72]

Consider a situation where a data subject gives consent for his data to be processed by a company. A dispute later arises and is taken to arbitration, where the data subject's data is processed. In this situation, the consent given earlier is not 'specific' as it is not given for the purposes of the arbitration, and it is also not 'informed', as the data subject could not have known about the arbitral proceeding. Consent is needed specifically for the *particular* transfer or category of transfers in question. Informed consent requires that the subject is adequately informed of the circumstances of the processing in advance.[73] In an arbitration, it may be difficult to predict how personal data may need to be processed, and obtaining specific consent for each transfer or each processing would be an overwhelmingly difficult task. The fact that consent may be withdrawn at any point further complicates matters. In a situation where an employee of a company has given crucial testimony, their withdrawal of consent for the processing of their personal data (which would be included in their testimony), could collapse a party's case.

---

67 ICCA-IBA ROADMAP, *supra* note 22, at 14.

68 *See,* GDPR, *supra* note 15, art. 12-22; Lei No. 13,709 de Aug.14 de Agosto de 2018, DIÁRIO OFICIAL DA UNIÃO [D.O.U] de 15.8.2018, art. 6 (Braz.) *in* ICCA-IBA ROADMAP, *supra* note 22, at 14.

69 GDPR, *supra* note 15, art. 6(1)(a).

70 *Id.* recital 32.

71 ICCA-IBA ROADMAP, *supra* note 22, at 17.

72 *Id.*

73 *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, 2093/05/EN WP 114, at 12 (Nov. 25, 2005), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf.

Therefore, even if an arbitration agreement between parties contains a 'consent for data processing and transfer' clause, this would likely not cover all the possible instances of processing and transfer that may arise in the course of an arbitration.[74] What then, would be the lawful basis of processing? The Personal Data Protection Act, 2012, of Singapore provides a list of circumstances where personal data can be processed without consent.[75] One of these is that the collection is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data.[76] Hong Kong law contains a similar provision.[77] The term 'proceedings' would squarely cover arbitral proceedings.[78] Thus, if personal data is being processed for the purposes of an arbitration in Singapore or Hong Kong, specific consent would not be required. In Singapore, processing without consent may also be permitted if the collection is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services.[79] This would cover cases where a law firm or legal counsel collects personal data of individuals (who may not be directly associated with the case) without their specific consent. However, not all jurisdictions have rules pertaining to derogation from the rule of consent in case of legal claims. For example, the GDPR only contains derogations for transfers of personal data to third countries or international organisations, not for the general purpose of processing.[80] Parties would therefore have to be cognisant of the legal bases for processing in the jurisdiction where they are processing data and where consent is the primary basis, efforts will have to be made to obtain such consent (as specifically as possible) from the very outset of the proceedings.

Data minimisation is an important principle of data protection, which requires that personal data be adequate, relevant, and limited to what is necessary for the purpose for which it is processed.[81] This principle is based on the objective of necessity and relevance – i.e. that the personal data collected should be limited to what is *necessary* for the specified purpose. Further, the personal data should be *relevant* to the processing.[82] The Roadmap highlights several issues that could arise in arbitration as a result: preparing for a proceeding often involves collecting information about all possible individuals related to the transaction. In such a situation, law firms or counsel could end

---

74 ICCA-IBA ROADMAP, *supra* note 22, at 17.

75 *See* Personal Data Protection Act, No. 26 of 2012, sch. 2 (Sing.) [*hereinafter* "Singapore PDPA"].

76 *Id.* ¶ 1(e).

77 Personal Data (Privacy) Ordinance, (1995) Cap. 486, § 60B (H.K.): "Personal data is exempt from the provisions of data protection principle 3 if the use of the data is— (a) required or authorized by or under any enactment, by any rule of law or by an order of a court in Hong Kong; (b) required in connection with any legal proceedings in Hong Kong; or (c) required for establishing, exercising or defending legal rights in Hong Kong" [*hereinafter* "HK PDPO"].

78 *See* Singapore PDPA, § 1 (Sing.): "proceedings" means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of —(a) a breach of an agreement; (b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or (c) a wrong or a breach of a duty for which a remedy is claimed under any law."

79 *Id.* sch. 2.

80 *See* GDPR, *supra* note 15, art. 49.

81 *See id.* art. 5; HK PDPO, sch. 1, item 1(1).

82 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, EUR. DATA PROT. BD, 19 (Nov. 13, 2019), *available at* https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

up collecting information about hundreds of employees.[83] Another issue that arises is the number of people who will have access to that data – this may include third party funding organisations, expert witnesses, institutional arbitration case managers, etc. For the purposes of protecting personal data, arbitral institutions and law firms should adopt a policy of pseudonymising or anonymising personal data from the outset.[84]

The GDPR provides, under Article 15, that the data subject has the right to obtain information from the controller *inter alia* as to whether their personal data is being processed, the purposes of the processing, and the recipients to whom the personal data will be disclosed.[85] In an arbitration, personal data of employees, contractors, suppliers, etc. may be used for the purposes of a claim. However, it may not be strategically prudent for a data controller (say, one of the parties in the arbitration) to reveal how that personal data is being used in the arbitration. This could compromise both the confidentiality of the arbitration as well as the arbitral strategy of the parties, in addition to being damaging for business relations.[86] For this purpose, a balance needs to be achieved between the need for transparency and confidentiality. Confidentiality has now become an oft-cited reason to prefer arbitration over litigation. The Roadmap, once again, suggests addressing data subject rights at the outset of the proceedings and putting in place a protocol for the same.[87]

B. The Protocol on Cybersecurity

Party autonomy is prioritised in the approach of the Protocol, as parties would be best apprised of their specific requirements and would have the greatest interest in ensuring information security.[88] The tribunal would have the power to decide information security measures, but should defer to the parties' agreement,[89] except in some specific instances, such as when third parties or the interest of the tribunal is concerned.[90] The tribunal is also entitled to resolve disputes and can impose costs or sanctions in this regard.[91] However, the Protocol advises the negotiation of a specific dispute settlement mechanism to cover post-arbitration disputes to address a situation where the tribunal may have become *functus officio*.[92]

Pertinently, the Protocol raises the issue of arbitral institutions and their capabilities for handling information security. The Protocol recommends collaboration between the arbitral participants and the institution to ensure that the measures adopted by them are consistent with the rules, practices and capabilities of the institution.[93] India has displayed a commitment towards strengthening institutional arbitration with the Arbitration and Conciliation (Amendment) Act, 2019, and the New Delhi International Arbitration Centre Bill, 2019. Information security in

---

83 ICCA-IBA ROADMAP, *supra* note 22, at 21.
84 *Id.*
85 GDPR, *supra* note 15, art. 15.
86 Avinash Pooroye & Ronan Feehily, *Confidentiality and Transparency in International Commercial Arbitration: Finding the Right Balance*, 22 HARV. NEGOT. L. REV. 275, 278 (2017).
87 ICCA-IBA ROADMAP, *supra* note 22, at 26.
88 ICCA-NYC BAR-CPR PROTOCOL, *supra* note 52, principle 9.
89 *Id.*
90 *Id.* principle 11.
91 *Id.* principle 13.
92 *Id.*
93 *Id.* principle 4(c).

arbitration ought to be a priority for the government to avoid the challenges that arise as a result of the lack of a strong data protection law.

The Protocol further advises that information security measures be decided on the basis of the risk profile of the dispute, assessing existing security practices, and the infrastructure and capabilities of the parties.[94] Schedule B of the Protocol discusses risk factors in great detail, comprising of *inter alia* the nature of the information (personal data, sensitive data, health data, trade secrets, payment information, etc.), the identity of the parties, the concerned industry, and the value of the dispute.[95] Analysing these risk factors could significantly assist the parties formulate effective information security measures for their disputes, which mitigate risk. Sample information security measures are provided in Schedule C of the Protocol.

The Protocol provides sample language for information security measures in Schedule D.[96] Importantly, however, the Protocol *does not* recommend including information security measures in their arbitration agreement, given that between the conclusion of the agreement and the initiation of the dispute, cyber risks, technology, and available measures may significantly differ.[97] Further, the measures should depend on the risk profile of the dispute.[98]

On the whole, the Protocol provides a holistic understanding of cybersecurity for arbitration. It covers possible risks and measures comprehensively. It may benefit arbitral institutions to develop information security polices which take a cue from this Protocol.

A perusal of the websites of two major arbitral institutions – the Singapore International Arbitration Centre ["**SIAC**"] and the Hong Kong International Arbitration Centre ["**HKIAC**"] – does not reveal a dedicated data protection policy. The Privacy Policy on SIAC's website is primarily concerned with users of the website, and there is no specific information on the information security measures taken by the institution during arbitrations.[99] Further, the Policy was last updated in 2014.[100] SIAC may benefit from updating this to reflect the sea-change in the global conversation on data protection, especially in light of the GDPR. Similarly, though the HKIAC has taken expedient measures to administer arbitrations during the outbreak of COVID-19, and these measures include expansive e-hearing facilities.[101] However, no information has been provided on the protection of data which is transmitted via virtual hearings, security measures for virtual hearing rooms, and security of software. Further, the authors could not locate a privacy policy on the HKIAC website. This is especially concerning considering that the HKIAC hears disputes pertaining to the Belt and Road Initiative, which would undoubtedly contain confidential information concerning different States. It is worth noting that during the consultation process on

---

94 *Id.* principle 6.
95 *See id.* sch. B.
96 *See id.* sch. D.
97 *Id.*
98 *Id.*
99 *See Privacy Policy*, SING. INT'L ARB. CTR., *available at* https://www.siac.org.sg/privacy.
100 *Id.*
101 *See Virtual Hearings*, H.K. INT'L ARB. CTR., *available at* https://www.hkiac.org/content/virtual-hearings.

the proposed amendments to the HKIAC Administered Arbitration Rules, 2013,[102] the Hong Kong Privacy Commissioner for Personal Data ["**PCPD**"] had highlighted the sensitive nature of documents in an arbitration and the need for steps to protect their security.[103] In relation to the proposed online repository as a means of service of documents,[104] the PCPD noted that encryption was necessary to ensure the security of data.[105] Further, the PCPD highlighted the conflict between the confidentiality of arbitration as provided under Article 45 of the HKIAC Rules and the right of the data subject to access data under the Hong Kong Personal Data (Privacy) Ordinance.[106] However, these concerns have not been addressed in the 2018 edition of the HKIAC Rules. n these times, it is urged that arbitral institutions formulate policies to tackle information security during virtual *and* physical hearings, as well as security of their websites.

Further, with the onset of COVID-19, many arbitral hearings had to go online unexpectedly. With one of the main video-call applications being embroiled in cybersecurity issues,[107] the arbitral community around the world needs to consider how information security must be addressed in remote arbitration. The GDPR, for instance, requires appropriate measures to be taken to ensure security – this includes ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.[108] Before beginning an arbitral proceeding, Arbitral Participants should ensure that the data being collected and processed for the purposes of the arbitration is stored in a safe location and the confidentiality of the arbitration is not compromised. This may involve carefully examining the security arrangements of any online data rooms and remote hearing applications which may be used during the arbitration and would require deployment of specialised resources (like information technology professionals). This will often mean that the infrastructure used by the Arbitral Participants to secure the arbitration ought to be state of the art. However, this poses serious questions of accessibility. Take for example India – the government wishes to make the country an 'arbitration hub' and further institutionalise arbitration.[109] The government is also the biggest litigant in India.[110] However, whether even the government has the resources to ensure security of data is questionable, and this is evidenced by lapses in the past.[111] The choice of arbitration as the preferred dispute resolution mechanism by other, smaller entities (such as Small and Medium Enterprises ["**SMEs**"]) will be hindered by the lack of appropriate cybersecurity

---

102 Now in force as Hong Kong International Arbitration Centre Administered Arbitration Rules, Nov. 1, 2018 [*hereinafter* "HK IAC Rules"].

103 PCPD's Submission in response to the Public Consultation on the Proposed Amendments to the 2013 HKIAC Administered Arbitration Rules, PRIVACY COMMN'R FOR PERS. DATA, ¶ 4, *available at* https://www.pcpd.org.hk/english/enforcement/response/files/Submissions_to_HKIAC_29092017.pdf [*hereinafter* "PCPD Submission"].

104 HK IAC Rules, *supra* note 102, art. 3(1)(e), 2018.

105 PCPD Submission, *supra* note 103, ¶ 5.

106 *See* HK PDPO, § 18.

107 Charlie Wood, *Zoom's security and privacy problems are snowballing*, BUS. INSIDER (Apr. 1, 2020), *available at* https://www.businessinsider.in/tech/enterprise/news/zooms-security-and-privacy-problems-are-snowballing/articleshow/74934074.cms.

108 GDPR, *supra* note 15, art. 32.

109 The Arbitration and Conciliation (Amendment) Act, 2019., No. 33 of 2019, statement of objects and reasons (India).

110 LAW COMMISSION OF INDIA, REPORT NO. 230, REFORMS IN THE JUDICIARY – SOME SUGGESTIONS, ¶ 1.25 (2009).

111 Gautam S. Mengle, *Major Aadhaar data leak plugged: French security researcher*, THE HINDU (Mar. 20, 2019), *available at* https://www.thehindu.com/sci-tech/technology/major-aadhaar-data-leak-plugged-french-security-researcher/article26584981.ece.

infrastructure. Such concerns merit consideration at an international level, keeping in mind the resources of developing nations.

IV. The Indian Personal Data Protection Bill, 2019

The 2019 Indian Bill is largely drawn from the EU's GDPR. Its application is based on the principle of territoriality and passive personality, nationality and extra-territorial jurisdiction based on the 'effects doctrine'.[112]

The Bill defines personal data to mean data relating to any characteristic, trait, attribute or any other feature of the identity of a natural person, directly or indirectly identifiable, and includes inferences drawn from such data as well. The Bill also refers to 'data principal' i.e., a natural person to whom the personal data relates to,[113] 'data fiduciary' who determines the purpose and means of processing of personal data which includes a company or an individual as well.[114] The Bill creates a relationship between a data principal and data fiduciary based on trust,[115] which is the hallmark of a fiduciary relationship.[116] Thus, lawyers and arbitrators may be considered as data fiduciaries for the purpose of arbitral proceedings.

Further, the Bill applies to the processing[117] of personal data (i) if such data has been collected, disclosed, shared or otherwise processed within the territory of India (territoriality), (ii) by the State, an Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law (nationality), and includes processing of personal data by (iii) data fiduciaries or data processors not present within the territory of India, if the processing is – in connection with a business or a systematic activity of offering goods and services to data principles or with any activity which involves profiling of data principles within the territory of India (effects doctrine). Thus, Indian arbitrators, arbitral institutions and arbitral proceedings in India would clearly be required to comply with the data protection regime created under the Bill, depending upon whether they can be treated as data fiduciary or data processor.

First, every lawyer and arbitrator can only process data for a clear, specific and lawful purpose and restricted to only the specified purpose for which it was collected.[118] *Second*, they shall process personal data in a fair and reasonable manner that ensures privacy of the data principal[119] and for the purpose consented to by the data principal.[120] *Third*, personal data shall be collected only to the extent that is necessary for the purpose of processing.[121] *Fourth*, personal data shall be stored only

---

112 SRIKRISHNA COMMITTEE REPORT, *supra* note 12, at 19.

113 PDP Bill, § 3(14).

114 *Id.* § 3(13); The Bill further covers 'data processor' who processes personal data on behalf of the data fiduciary, *see* § 3(15).

115 Puttaswamy, (2019) 1 SCC 1, ¶ 224.

116 SRIKRISHNA COMMITTEE REPORT, *supra* note 12, at 8; *see also* Central Board of Secondary Education & Anr. v. Aditya Bandopadhyay & Ors., (2011) 8 SCC 645, ¶ 21 (India).

117 Processing has been defined as "an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction." *See* PDP Bill, § 3(31).

118 PDP Bill, § 4.

119 *Id.* § 5(a).

120 *Id.* § 5(b).

121 *Id.* § 7.

for as long as is necessary.[122] *Finally*, lawyers and arbitrators shall also have to issue a notice to the data principal about the collection of data prior to the collection.[123]

A key concern that has been raised with respect to the Bill is whether it will apply to arbitral proceedings at all due to the proposed Section 36(b) and (c) of the Bill.[124] As per Section 36(c) of the Bill, processing of personal data by any court or tribunal in India necessary for the exercise of any judicial function will not attract the application of the Bill. The Supreme Court of India in *Associated Cement Companies Ltd.* v. *P.N. Sharma & Ors.*, held that an authority is said to exercise judicial function when it is empowered by the State to determine the rights of two or more contending parties with regard to a matter in controversy conclusively.[125] However, the court went on to hold that while the Arbitration Act (1940) vested an arbitrator with some of the trappings of a court, yet it cannot be termed as a tribunal as the arbitrator derives its power by virtue of an agreement.[126] Thus, the exemption under this clause shall not be applicable to arbitral proceedings.

Nevertheless, the proposed Section 36(b) on exemption may be applicable to arbitral proceedings. As per the said provision, disclosure of personal data 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, shall be exempted from the application of the Bill. In *General Officer Commanding & Ors.* v. *CBI & Ors.*, the Supreme Court of India defined legal proceedings to mean proceedings regulated or prescribed by law in which a judicial decision may be given. In other words, it means proceedings in a court of justice by which a party pursues a remedy which a law provides but does not include administrative and departmental proceedings.[127] Further, the court had also noted arbitral proceedings to be legal proceedings.[128] Thus, most obligations under the Bill save those provided under Section 4 (i.e., no processing of personal data save for specific, clear and lawful purpose) and 24 (i.e., security safeguards) of the Bill shall not apply to arbitral proceedings.

In the following section, the authors attempt to provide guidance and analyse concerns that may be raised during an arbitral proceeding, in the backdrop of the EU's GDPR and the 2019 Indian Bill.

V. International Arbitration: A Potpourri of Data Protection Regimes

A typical international arbitration involves multiple actors from various jurisdictions across the world. As data protection regimes tend to follow their nationals (extra-territoriality), compliance with various national data protection laws can be complex and puzzling. For instance, a dispute between an EU and an Indian party before arbitrators appointed by an arbitral institution in Singapore would trigger the protections contained in all the three jurisdictions. As data would be

---

122 *Id.* § 9.

123 *Id.* § 5(a).

124 *See* Tarun Krishnakumar, *Data Protection in India and Arbitration: Key Questions Ahead*, KLUWER ARB. BLOG (Apr. 16, 2019), *available at* http://arbitrationblog.kluwerarbitration.com/2019/04/16/data-protection-in-india-and-arbitration-key-questions-ahead/.

125 Associated Cement Companies Ltd. v. P.N. Sharma, AIR 1965 SC 1595, ¶ 46 (India).

126 *Id.*

127 General Officer Commanding & Ors. v. CBI & Ors., AIR 2012 SC 1890, ¶ 12 (India).

128 *Id.*

transferred across jurisdictions with different kinds of protection, Arbitral Participants will necessarily have to demonstrate compliance at all stages of transfer.

In the collection of documents and preparing a case for oneself, the parties shall have to ensure that they comply with their own national data protection regimes. Additionally, if parties are involved in activities outside their national territory, then they shall have to ensure compliance with other domestic regimes as well. The ICCA-IBA Roadmap suggests identifying the applicable national laws for all the Arbitral Participants.[129] The EU party may be permitted to transfer personal data to the Indian party without the 'adequacy decision' and appropriate safeguards due to the legal claims' exception. Nonetheless, it will still have to ensure that the protection guaranteed to an EU data subject under the GDPR is upheld. Further, the EU party will have to cull for relevance, and provide for redaction or pseudonymisation of personal data as well as confidentiality.[130] Meanwhile, and assuming the application of the Bill, the Indian party shall have to ensure that such data is processed for specific, clear and lawful purpose. Further, the Indian party shall have to implement de-identification, encryption, protect the integrity of the data and prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.[131]

This may be particularly challenging in case of SMEs. SMEs face difficulties in international disputes as opposed to large corporations due to lack of resources and infrastructure.[132] The already complex and multi-layered process of complying with multiple data protection laws would act as a further impediment for SMEs to expand themselves internationally.

Moreover, the arbitral institution will be considered as an organization (controller/data fiduciary) as well and will have to ensure compliance with the Singapore Personal Data Protection Act, 2012. The Roadmap recommends providing an express notice to the arbitrator that his personal data would be processed for the purposes of the arbitral proceedings and may be transferred to third countries.[133] In case of an arbitrator from Singapore, this would require compliance with the protection guaranteed under the Act unless exempted by the Commission.[134]

The Roadmap further suggests the consideration of basis and necessity for inclusion of personal data at the time of drafting the award and take steps to minimise the inclusion of personal data in the Award.[135] Nonetheless, the arbitral award may still contain personal data which shall have to be processed under the relevant data protection laws of the Arbitral Participants. This may also be difficult in investor-State arbitrations, where transparency is of greater importance. Should the data

---

129 ICCA-IBA ROADMAP, *supra* note 22, at 34.

130 Guidelines 2/2018 on Derogation of Article 49 under Regulation 2016/679, EUR. DATA PROT. BD., 10, 11 (May 25, 2018), *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

131 PDP Bill, § 24(1).

132 Petra Butler & Gary Born, Bilateral Arbitration Treaties: An Improved Means of International Dispute Resolution, UNCITRAL 9, *available at* https://www.uncitral.org/pdf/english/congress/Papers_for_Programme/104-BORN_and_BUTLER-BATs_An_Improved_Means_of_International_Dispute_Resolution.pdf.

133 ICCA-IBA ROADMAP, *supra* note 22, at 39.

134 Singapore PDPA, § 26(1).

135 ICCA-IBA ROADMAP, *supra* note 22, at 44.

subject remain identifiable, appropriate measures ought to be taken to process it in compliance with applicable laws.[136]

The Roadmap further recommends the use of a 'data protection protocol' – a document through which parties agree on how data protection will be applied in a particular context, which could allocate responsibilities for data protection compliance during the arbitration.[137]

Data protection in accordance with the applicable law ought to be the foremost consideration for Arbitral Participants, given the far-reaching consequences that breach of data protection laws have (such as massive fines under the GDPR and Indian Personal Data Protection Bill). Accordingly, the Roadmap advises that data protection be addressed in the first procedural conference so as to allow Arbitral Participants to discuss applicable laws and measures for compliance.[138]

VI. Conclusion: The Way Forward for Secure Arbitration

The transnational nature of arbitration and constant data flows make it a high-risk field in terms of data protection. Presently, the international and domestic data protection and cybersecurity framework for arbitration is woefully inadequate, and this could lead to bigger challenges in the future. Arbitral institutions across the world are expanding their scope, be it the SIAC releasing its Investment Arbitration Rules, the HKIAC hearing Belt and Road Initiative disputes, or Indian arbitral institutions hoping to strengthen their capabilities. As they expand their scope, the quantum of data and cases which they handle will also rise. For example, the SIAC handled 343 new cases as of 2016. In 2017, their active caseload was about 650 cases.[139] In light of this, institutions ought to make concerted efforts to ensure their data protection and information security practices are up to the mark. With virtual hearings becoming more popular, this will be of crucial importance for the future of arbitration.

The GDPR was a massive overhaul of the European data protection framework, with effects rippling across the globe due to its extra-territorial application. Jurisdictions like India are modelling their potential data protection regulations around the GDPR, and it is undeniable that the GDPR provides a high threshold for data protection. In light of this, the arbitration community ought to develop specific practices and guidelines which are tailor-made to the needs of this dispute settlement mechanism. Regard must be had to the recommendations and practice tips of the Roadmap developed by the ICCA and IBA.

An important concern is that of infrastructure and accessibility. Often, the protection of data and information security requires state of the art infrastructure, which might be an expensive investment for smaller businesses, institutions, and even the governments of some countries. The Commonwealth Secretariat Report has revealed that its Member States are willing to negotiate a

136 *Id.* at 43.
137 *Id.* at 41.
138 *Id.* at 40.
139 *Statistics*, SINGAPORE INTERNATIONAL ARBITRATION CENTRE, *available at* https://www.siac.org.sg/2014-11-03-13-33-43/facts-figures/statistics.

form of Bilateral Investment Treaty especially in light of the difficulties faced by SMEs.[140] It would be beneficial if the Commonwealth and the international community develop an arbitration treaty that specifically incorporates data protection and cybersecurity concerns. This shall improve the accessibility of arbitration as a dispute resolution mechanism and to provide some certainty with regards to standards of protection. Such a treaty also becomes important because of the nature of arbitration as a cross-border dispute resolution mechanism. Domestic data protection laws are not sufficient to cover all aspects in an *international* arbitration (such as transfer of data, access requests, etc.); further, the conflict between several national legislations adds to the uncertainty associated with data protection in arbitration, and while the Roadmap is highly informative, it is not binding.

Such a mechanism could provide for: *first*, a standard rule for aspects such as third country data transfers, standards of personal data processing, access controls, and other data protection and information security measures. *Second*, such a treaty could be useful for providing an international standard for security infrastructure to be used in arbitration. *Third*, drawing inspiration from the Paris Accord, such a treaty could make provisions for 'data protection/information security finance', whereby countries provide aid to one another to improve their data protection and security infrastructure. This would greatly improve the accessibility of arbitration across the world, and governments would have more confidence in taking their disputes to investor-State forums (or in domestic arbitrations with contractors) without the fear of data leaks. The treaty could be open to signature by international organisations (such as arbitral institutions, ICSID, and PCA) as well as nation States. Importantly, such a treaty must contain a provision on the prevailing system where provisions of the treaty conflict with national law.

Lastly, the IBA and UNCITRAL have been instrumental in providing uniformity in the sphere of international arbitration. In the absence of an international framework for data protection in arbitration, perhaps there is a role for them in this sphere to develop guidelines and principles to govern this extremely uncertain aspect of international arbitration. These could further be adopted by arbitral institutions. The promise of confidentiality would be in vain if risks of data breaches remain.

---

140 Prof. (Dr.) Petra Butler, Findings of the Commonwealth Study on International Arbitration, Centre for Advanced Research and Training in Arbitration Law (CARTAL Lecture Series, National Law University, Jodhpur) (Feb. 10, 2020) (transcript available with the authors).