University of New South Wales Law Research Series

IS INTERNATIONAL ARBITRATION PRUDENT WHEN DEALING WITH PERSONAL DATA CHALLENGES?

LEON TRAKMAN, ROBERT WALTERS AND BRUNO ZELLER

Forthcoming (2019) *Transnational Dispute Management*
[2019] *UNSWLRS* 95

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Is International Arbitration Prudent when Dealing with Personal Data Challenges?

Leon Trakman, Robert Walters, Bruno Zeller[1]

Abstract

The trade in personal data is pervading many of the traditional areas of law, such as contract and intellectual property, and is likely to result in increasing disputes over this trade. International arbitration offers a way to resolve these disputes. This article examines the role of international arbitration in data protection law. It draws on the European Union's (EU) General Data Protection Regulation (GDPR) and resort to international commercial arbitration (ICA) to resolve personal data disputes across jurisdictions. It examines the EU laws alongside those of Australia and Singapore. The purpose is to demonstrate the fundamental value of ICA in resolving personal data disputes; how to apply ICA to such disputes as distinct from other international commercial disputes; and how to address divergences across regions and states in approaches to protecting personal data. The article highlights the challenges and possible effectiveness of ICA, which will largely depend on the consent of data subjects to use their personal data in addressing disputes over the alleged abuse of that data.

Introduction

Personal data is increasingly a tradable commodity that has begun to dominate in a range of legal areas. These include competition law,[2] intellectual property law,[3] and transnational contract laws.[4] Legal disputes can arise in such areas of law, and disputing parties can contract to submit these disputes to arbitration. The current fragmented approach to the development and implementation of data protection varies greatly from jurisdiction to jurisdiction. The benefit of relying on ICA to resolve disputes over personal data is that arbitrators, by and large, can be expected to be appointed by disputing parties based on their expertise in data protection law. In contrast, domestic courts of general jurisdiction ordinarily lack such expertise. Unlike domestic courts, ICA arbitrators are also not constrained by domestic rules of evidence and procedure that confine domestic courts, enabling them to adopt more flexible and sustainable procedures that can expedite data disputes.

[1]* Leon Trakman B. Com, LLB (Cape Town); LLM, SJD (Harvard). Professor of Law and Former Dean, Faculty of Law, University of New South Wales, Sydney

**Robert Walters LLB (Victoria), MPPM (Monash), PhD Law (Victoria), Lecturer Victoria Law School, Victoria University, Melbourne, Australia. Adjunct Professor, European Faculty of Law, The New University, Slovenia, Europe

*** Bruno Zeller B. Com, B. Ed, Master of International Trade Law (Deakin), PhD (The University of Melbourne). Professor of Transnational Commercial Law, University of Western Australia, Adjunct Professor Murdoch University. Perth, Adjunct Professor Sir Zelman Cowan Centre, Victoria University, Melbourne

[2] See Robert Walters, Leon Trakman, Bruno Zeller, 'Personal Data Law and Competition Law – where is it heading?' (2018) 39(12) *European Competition Law Review* 505.

[3] See Leon Trakman, Robert Walters and Bruno Zeller, 'Is Privacy and Personal Data set to become the new Intellectual Property?' (2019) *International Review of Intellectual Property and Competition Law*.

[4] See Bruno Zeller, Leon Trakman, Robert Walters, Sinta Dewi Rosadi 'The Right to be Forgotten – the EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)' (2019) 1 *European Human Rights Law Review* 23.

However, international commercial arbitrators are not immune to the application of domestic law. Parties to data disputes that contract to have their disputes resolved through ICA ordinarily make a choice of a domestic law that binds the arbitrators they appoint. The ancillary result is that ICA arbitrators, however much they adopt transnational methods of dispute resolution, must nevertheless rely on specific data protection laws that ordinarily diverge from the law applicable in other jurisdictions. A central concern of this article, therefore, is to better comprehend the competing applicable laws governing the protection of personal data that regulate the collection and processing of personal data. In issue, too, is how different regional jurisdictions, such as the EU, and states such as Singapore and Australia, define personal data, how they determine the limits of a data subject's consent to use personal data, and how they provide for the resolution of disputes between data subjects and downstream data with whom those subjects lack contractual relationships.

As a result, this article examines what the authors consider to be the most important elements of data protection law in resolving disputes through ICA. These elements include: the definition of personal data, the legal boundaries of consent in the use of that data, and the importance of both the definition of and consent to use personal data in resolving ICA disputes.

Section I highlights the historical significance of international commercial arbitrators who decide disputes between data subjects and data users in our 21st century e-merchant law. Section II examines the control that is exercised over personal data in the EU, compared to the limited regulation of such data in Australia and Singapore. Section III examines the varied approach taken by these three jurisdictions in defining personal data, and the likely impact of such variation upon resort to ICA in resolving data disputes. Section IV evaluates the significance of coupling the definition of personal data with the consent to use that data. Section V highlights differences in approach to these issues taken by the EU, Australia and Singapore towards the concept of consent and how these differences are likely to impact upon the resolution of disputes through ICA. Section VI highlights the materiality of personal data in the transfer of information in a global economy that increasingly trades in personal data, along with the need for ICA to regulate such transfers in a borderless data economy that resists legal regulation. Section VII proposes how ICA can manage how personal data is collected, processed, used and stored by third parties.

Section I: Potential Issues in International Arbitration

Data protection is increasingly being recognized as a hot topic not only in cyber security, but also, international arbitration. Trans-regional arbitration has a lengthy history that traces back to medieval times.[5] There, the disputes between merchants engaged in trans-regional trade were allegedly resolved by merchant judges expeditiously and cost-effectively. The further adage was that such merchant judges delivered justice *ex aequo et bono,* according to that which was "just and fair" to itinerant merchants and not according to the "laws" of local potentates seeking to regulate merchants from other regions.[6]

The medieval Law Merchant has direct parallels to the e-Merchant Law of the 21st Century. International commercial arbitrators, like medieval merchant judges, are increasingly expected

[5] See Leon E. Trakman, *The Law Merchant: The Evolution of Commercial Law* (Fred B. Rothman, 1983) Chapters 1–2.
[6] See Leon E. Trakman, 'Ex Aequo et Bono: Demystifying an Ancient Concept' (2008) 8(2) *Chicago Journal of International Law* 1.

to resolve disputes arising in global e-markets between merchant corporations that collect and mine personal data at the expense of both data subjects and the public good.[7] A 21st Century mission of international commercial arbitrators includes delivering expeditious and fair justice. That mission applies not only between transnational merchants who trade in personal data, but also between merchants and the consumers in whose personal data they trade.[8]

However, in the contemporary world, the nature and operation of international arbitration law is far from harmonized, or uniformly adopted by nation states.[9] Nor is it uniformly applied to transnational commerce, not least of all to the use of personal data and its impact upon data subjects. On the one hand, there is a framework for the regulation of international commercial arbitration (ICA), comprising both the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention (NC)) 1958 and the UNCITRAL Model Law on International Commercial Arbitration 1985 and revised 2006. However, the recognition and enforcement of international and foreign arbitration awards is neither uniformly conceived, nor consistently applied.[10] Nonetheless, it is important to recognize that, while modern ICA is consensual between the disputing parties, it is ordinarily subject to law (and not usually determined *ex aequo et bono* operating outside the law).[11] As a result, how arbitrators decide on whether and to what extent data users abuse or misuse personal data depends on the applicable law. Given that that law varies across jurisdictions, arbitrators that are bound by the choice of law of the parties are likely to diverge in deciding disputes on the use of that data in specific cases.

II. Control of Personal Data

In order to understand and appreciate the involvement of arbitration in disputes over the use of personal data, it is necessary for disputing parties to address the disparate laws and regulatory frameworks in which that data is used.[12] These differences relate, in particular, to how the applicable law protects personal data and the privacy of data subjects. In issue is how the use of personal data is legally regulated in the specific jurisdiction. A further challenge arises over the applicable law due to different legal regulations of personal data, such as adopted by the EU and states outside the EU. For arbitrators to decide disputes over the use of personal data, the disputing parties need to appraise them of divergences in the regulation of personal data.

A. The European Union

The GDPR has afforded the citizens of the EU actionable rights that go some way to protecting their personal data and privacy over the Internet. However, Kathleen Paisley maintains, the GDPR includes various areas in which EU member states are expressly allowed to derogate from its terms.[13] These include the right of states to exempt "judicial proceedings" and "the

[7] See Leon E. Trakman, 'From the Medieval Law Merchant to E-Merchant Law', 53(3) *University of Toronto Law Journal* 265.
[8] Leon E. Trakman, 'The Twenty-First Century Law Merchant' (2011) 48(4) *American Business Law Journal* 775.
[9] See Jean-Francois Poudret and Sebastien Besson, *Comparative Law of International Arbitration* (Sweet & Maxwell, 2nd ed, 2007).
[10] See Leon Trakman, 'Aligning State Sovereignty with Transnational Public Policy' (2018) 93(2) *Tulane Law Review* 207.
[11] See Trakman, above note 8.
[12] See Robert Walters, Leon Trakman, Bruno Zeller, *Data Protection Law Asia Pacific (Australia, India, Indonesia, Japan, Malaysia, Singapore and Thailand) and European Union* (Springer, 2019).
[13] See Kathleen Paisley, 'It's All About the Data: The Impact of the EU General Data Protection Regulation on

enforcement of civil law claims" from the application of some of the more strenuous rights and obligations imposed by the GDPR, provided that other safeguards are put in place.[14] Paisley notes that Ireland has applied this exemption broadly to exempt certain types of personal data from the GDPR that are typically under scrutiny in an arbitration dispute over the use of that data. At the same time, other provisions of the GDPR remain applicable in Ireland. Paisley further argues that the GDPR protects the autonomy of state courts, acting in their judicial capacities, to regulate the use of personal data.[15] She finds support for such judicial independence in Recital 20 of the GDPR.[16]

The GDPR's multilayered regulatory approach to dispute resolution poses challenges to the GDPR itself. Specifically, Article 55 of the GDPR provides that supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacities. However, that Article makes no reference to arbitration. The result is that the general exemption from the supervisory authority, such as within the EU-state of the data importer, does not expressly provide for the resolution of disputes over the use of data through ICA.[17]

The GDPR also allows state exemptions from its protection of personal data. EU member states can place limits on the right of data subjects to have transparent notice of data use (potentially including data privacy notices),[18] access to data,[19] rectification and erasure of data,[20] the right to restrict further processing of data,[21] data portability,[22] and to object to automated decision making.[23] An important though yet unresolved issue relates to the extent to which EU member states can exempt many of these specific rights granted to data subjects by the GDPR. According to Article 23, the restriction placed on such rights of data subjects depends upon whether the exemption respects the "essence" of fundamental rights and freedoms. That requires that the exemption must be necessary and proportionate "in a democratic society to

International Arbitration' (2018) 41(4) *Fordham International Law Journal* 841.

[14] *EU General Data Protection Regulation: Regulation (EU) 2016/679* [2016] OJ L 119/1 ('GDPR').

[15] See Paisley, above n 13.

[16] Ibid. Recital 20 states that while this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

[17] Ibid. The exemption of the courts of EU member states from oversight by the supervisory authority nevertheless does not mean that the GDPR does not apply to EU courts. Rather, it means that that the GDPR regulations are enforced in those member states by the judicial authorities themselves, rather than the supervisory authorities. The argument therefore is that the recognition and enforcement of an arbitration between disputing parties in different member states is still possible with the assistance of EU courts in that recognition and enforcement process. In addition, given that parties to data protection disputes may adopt an EU jurisdiction or law through a choice of jurisdiction and law clause, the applicable law will apply to both EU and non-EU citizens. This is especially pertinent when the applicable law provides for, or recognizes the contractual choice of the disputing parties, to resolve their disputes through ICA.

[18] See GDPR arts 12–14.

[19] Ibid art 15.

[20] Ibid arts 16–17.

[21] Ibid art 18.

[22] Ibid art 20.

[23] Ibid arts 21–22.

safeguard", among other things, "the protection of judicial independence and judicial proceedings" and "the enforcement of civil law claims".[24]

As a result, the Article 23 exemption does not mean that member states can exclude the right to data protection under the GDPR.[25] Recital 52 further provides that, in special categories of personal data, processing should be allowed where necessary to establish, exercise, or defend legal claims, whether in-court proceedings, or administrative or out-of-court proceedings, and when similar language is included in another recital of data transfers.[26] Importantly, out-of-court proceedings are not defined by the GDPR. Furthermore, the GDPR does not provide any further guidance on data processing that is "necessary" to establish, exercise or defend a legal claim. However, such out-of-court proceedings are most likely to include arbitration over the processing of data that is "necessary" to establish, exercise or defend legal claims.[27] Paisley notes that the legal claims exemption in the GDPR itself applies only to allow the processing of special categories of data.[28] The GDPR also limits the application of that exception, notably to the right of data subjects to erasure of personal data and to restrict processing,[29] and to object to further processing[30] as a basis for allowing data transfer to third countries.[31] Paisley believes that ICA has a decision-making function, which is of a judicial character.[32] However, the judicialization of arbitration proceedings is controversial: it may undermine the allegedly less formalized, speedier and less costly proceedings, as compared to court proceedings.

Yet another challenge to protecting personal data through "out-of-court" proceedings is that the GDPR envisages that specific bodies within the judicial system of the member states supervise data processing. The GDPR specifically provides that such supervision should ensure compliance with its rules and enhanced awareness among members of the judiciary of their obligations under those rules, including handling complaints about such data processing operations.[33] However, this challenge ought not to be overstated, given that civil law

[24] Ibid art 23.
[25] Ibid.
[26] Ibid recital 52. Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
[27] See GDPR art 23.
[28] See Paisley, above n 16, 859.
[29] Ibid arts 17–18.
[30] Ibid art 21.
[31] See Paisley, above n 16. Article 23 allows a member state to apply an exemption to a much broader category of rights directed at protecting judicial independence and enforcing civil claims. The other rights covered by Article 23 (especially the rights to data transparency, access to data, and rectification) are difficult to apply to ICA and potentially inconsistent with its decision-making function.
[32] See Paisley, above n 16, 859.
[33] See GDPR art 23.

jurisdictions in the EU regard arbitration as inhering in the civil justice system, as distinct from common law jurisdictions that regard arbitration as operating outside the civil justice system.[34]

However, the most significant limitation of the GDPR is that is only applies within EU jurisdictions, subject to exemptions reserved for EU member states. It is not available to states outside the EU unless they adopt a GDPR-like regime or disputing parties are subject to EU regulations.

i. Administering Data Protection under the GDPR

The functional benefits of the GDPR, notably its regulatory framework, are well worth being adopted by non-member states. For example, such a regulatory framework could require data collectors to appoint officers to supervise the collection and use of personal data. That framework could also provide arbitrators with a means of identifying deficiencies in that supervisory framework.

The GDPR has adopted a multi-layered regulatory regime, including by appointing data controllers and regulators within organisations that collect and process data. It requires such an organisation to appoint a data controller, data processor, sub-processor and/or data protection officer. These officers are responsible for collecting, storing, using and disseminating personal data. Data controllers have the further responsibility to implement technical systems and processors, to protect the organization from the illegal collection, use and processing[35] of personal data.[36] The GDPR also recognizes that, given the globalization of data collection and processing, data controllers may be located outside the EU and its member states. To help facilitate this process, Article 27 provides that representatives of controllers be established, even though they are not located in the EU or in any member state. However, this does not apply to the processing of special categories of personal data as referred to in Article 9(1)[37] or in processing personal data relating to criminal offences.[38]

The GDPR also provides that a controller may appoint a processor to ensure compliance with data processing requirements under the GDPR.[39] Article 28(2)(4) specifies that a processor must not appoint a sub-processor without the prior written consent of the controller.[40] Article

---

[34] This proposition does not apply to the the UK. While it is a member of the EU, it is a common law jurisdiction that does not treat arbitration as a component of the civil justice system.

[35] See GDPR art 24.

[36] Ibid art 5. Additionally, Article 25 reinforces such responsibility by requiring data controllers to take particular measures to ensure that personal data is limited to the required recipient. The controller is also accountable for organizational data protection policies and procedures, including by undertaking a data protection impact assessment to determine the level of risk to the rights and freedoms of a person to whom the data applies. Article 26 states that two or more controllers within the organization can determine their respective responsibilities in promoting compliance with the GDPR, including in protecting the rights by data subjects. Article 13 requires that data controllers provide specified information in collecting personal data from data subjects. Article 14 requires data controllers to provide such information where personal data has not been obtained from the data subject.

[37] Ibid art 9 restricts certain data that can reveal race, ethnic origin, political or religious belief. It also applies to membership of a trade union and revealing biometric data or sex and sexual orientation of a person.

[38] Ibid art 10.

[39] Ibid art 28(1)(3).

[40] There is a binding obligation on the controller when appointing a processor, which must be done in writing. Importantly, a processor can only act on written instructions of the controller. Nonetheless, a processor may appoint a sub-processor but only on the approval of the controller. Upon agreement of the controller of a sub-processor(s), those sub-processors must be appointed on the same terms as are set out in the contract between the

28(3)(h) requires that, in the event that a processor believes that the controller's instructions conflict with the requirements of the GDPR or other EU or Member State laws, the processor immediately inform the controller. Regarding specific responsibilities, the processor must keep records of its processing activities performed on behalf of the controller. These records include the details of the processor, the categories of processing activities performed, information regarding cross-border data transfers,[41] and a general description of the security measures implemented.[42]

Significantly too, Data Protection Officers (DPOs)[43] must be appointed by all public authorities. This requirement is separate from that imposed on controllers and processor in the private sector. Similar to their data processor counterparts in the private sector, data protection officers are responsible for informing and advising the controller or processor of their obligations under the GDPR.[44] This is a critical function in providing support to the data controller and processor. Importantly, too, the GDPR's expansive protection of personal data is evidenced by the person who is appointed as data processor. That processor must be a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller, and who determines the means by which to process that data.[45] This personage, function and responsibility of the data controller is a salutary indication to states outside the EU of the scope of data protection envisaged by the GDPR. This is because it not only has extensive reach within the EU. Third countries have adapted and applied the GDPR in developing and applying their respective data protection and privacy laws.

A court determining whether the data controller and processor has caused damage to a data subject is analogous to an arbitrator deciding whether to protect personal data and privacy rights. While the GDPR focuses on the structural and functional grounds for courts to protect personal privacy, these grounds have potentially comparable application to ICA.

---

controller and the processor. This approach ensures there is consistency and continuity in the application of the GDPR between the controller, processor and sub-processor(s).

[41] See GDPR art 30(2).

[42] Ibid, arts 28(1), 28(3)(e), 28(4), 32. Where non-compliance has been detected, the processor will be liable personally for any damage or loss (Article 82). This forces the actual processor to ensure they have taken all the appropriate steps to ensure compliance with the GDPR. It also places a form of co-responsibility on both the controller and processor. The processor has further responsibility to implement appropriate security measures to protect personal data against accidental or unlawful destruction or loss, alteration, and unauthorized disclosure. Some of the measures to be taken include data encryption, reviews, testing and the back-up of data. Importantly, the controller's liability for non-compliance with the GDPR is high, as it allows a data subject to claim directly against that processor. This responsibility, not limited to recording data, is likely to become important in any dispute over the trade and use of personal data.

[43] Ibid art 37.

[44] Ibid art 39. The role provides advice on data impact assessment to ensure the national supervisory authority is appropriately informed. The role is a critical contact point whereby the supervisory authority can contact this known individual within an organization. The structure within an organization allows for a robust and systematic approach to the implementation of the GDPR. The structure also reinforces the notion that the organization must be able to regulate themselves, with minimal oversight from the regulator, but, be accountable to a regulator. This is reinforced by Article 38, whereby the controller has responsibility for ensuring the officer is appropriately involved and supported. The officer is subject to the same level of confidentiality as the controller and processor, when processing data.

[45] Ibid art 4(8).

ii. Remedies under the GDPR

Remedies for the breach of personal data under the GDPR are primarily procedural. The data subject is entitled to reasonable notice of the breach of personal data, to be informed about that breach, the risks arising from it, and the measures taken to avoid them. Identifying the nature and scope of those remedies is best understood according to how the GDPR expresses them.

Article 79 of the GDPR grants the data subject who has suffered "material or non-material damages" as a result of a violation of their data privacy the right to an effective judicial remedy against a controller or processor, and to receive compensation from them.[46] This right to an effective judicial remedy pertains to litigation, although the transfer of data for use in litigation to countries outside of the EU is restricted by Article 48. Paisley notes that a data subject may also not have a right to an effective judicial remedy before an arbitral tribunal unless the arbitrator is appointed by the designated data protection officer.[47] Should this be the case, then resolving data disputes in countries like Singapore and Australia become more complex because they do not have designated data protection officers with responsibilities under the GDPR. Moreover, Articles 37 to 39 of the GDPR provide that the designation, position and tasks of the dispute protection officer are covered under Article 38. Data subjects, in the view of Paisley, may contact that officer with concerns about the processing of their personal data.[48] However, she notes that the interests of the data subject are determinative when the data processor has breached a duty to protect personal data.[49] Importantly, a data controller is under a duty, without delay, to notify the supervising authority of a personal data breach under Article 33(1) of the GDPR. In providing such notification, the controller is required to:

> a. describe the nature of the personal data breach; b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c. describe the likely consequences of the personal data breach; d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[50]

A data processor, in turn, is under a duty to notify the controller without undue delay after becoming aware of a personal data breach.[51]

Article 34 provides for the communication of a personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. In such cases, "the controller shall communicate the personal data breach to the data subject without undue delay".[52] This communication "shall describe in clear and plain language the nature of the personal data breach."[53] However, such a communication shall not be required

---

[46] Ibid arts 4(7), 82(1).
[47] *Supra note 13* art 27.
[48] Ibid. Additionally, Article 4(2) provides that: "Processing means any operation or set of operations which is performed on personal data or set of personal data, whether or not by automated means, such as disclosure by transmission." In an arbitral proceeding, a data processor may be required to disclose information about the "operation(s)" performed on personal data. This requirement to disclosure is necessary to satisfy the legitimate interests of both the data controller and data subject
[49] *Supra* note 41.
[50] See GDPR art 33(3).
[51] Ibid art 33(2).
[52] Ibid art 34(1).
[53] Ibid art 34(2).

when: (a) "the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach"; (b) "the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects … is no longer likely to materialize"; and (c) "it would involve disproportionate effort". Article 34(4) provides that the controller "having considered the likelihood of the personal data breach resulting in a high risk" may require that the supervisory authority not inform the data subject.[54]

As is evident from Article 33, these requirements seek to ensure that the data subject is timeously informed about the risks of a personal data breach, subject to limited exceptions. It affirms that the GDPR recognizes these risks, without ensuring that all such risks will be detected and conveyed to the data subject. It also provides a legal foundation upon which a data subject can bring an ICA action against the person or entity allegedly responsible for that personal data breach. The obstacle is that personal data breaches are often concealed by encryption or other codes directed at preventing unauthorized access and, here, to impede regulatory action.

It is arguable that the GDPR's stipulation that the data subject be timeously informed about the risks of a personal data breach is a due process requirement. It is a similarly tenable requirement in an arbitration dispute. What is also sustainable is that international commercial arbitrators face similar difficulties in adopting GDPR requirements as do courts in jurisdictions outside the EU. In both cases, if the applicable law is not the GDPR, there is no justiciable basis for such non-EU judges or arbitrators to apply the GDPR.

B. Australia and Singapore

Unlike the EU, Australia and Singapore do not have the multilayered approach to the control of personal data. Neither of these countries provide that an organization is legally required to appoint controllers or processors.[55] This, in itself, enables data processors to dilute their duties to protect personal data because no specified individual within that organization has full responsibility for the management of personal data, such as through databases, systems, platforms and other data infrastructures.

Accordingly, it is reasonable to infer that the EU constitutes the primarily regulator of personal data. First, it is arguable that the EU's complex data protection framework is effective, clear, accountably and transparent in nature. Second, the EU's scope of potential application is not only regional, but also transnational. Third, its transnational potential is reflected in multiple EU member states engaging with multiple non-EU states. In demonstrating the value of the EU, the article will return to the data protection frameworks of Australia and Singapore in Sections IV and V below.

III. Defining Personal Data

Before asking whether courts or arbitrators can protect personal data, it is pertinent to first determine the applicable definition, or definitions, of personal data. What is the nature of an individual's personal data? Is it no more than such formalized factors as the date and place of birth of the data subject? Or should data protection have a substantive foundation that varies

[54] Ibid arts 34(4).
[55] See Australian Privacy Principle 11.

from one kind or class of persons to another, and for reasons that transcend such formalized factors?

At the outset, understanding the definition of personal data is, in our view, one of the most important attributes of international arbitration over the protection of personal data. Arguably, that definition is the necessary precursor to an informed, transparent and efficient arbitration process, because an arbitrator must know and appreciate from the inception of the case the precise nature and significance of the personal data being traded.

Generally, data protection over the internet includes formalized personal data, such as the name, date of birth, and residential address of the data subject.[56] However, the GDPR has responded to rapid technological developments by seeking to protect the personal data of "natural" persons processed by "automated means", including through online identifiers such as IP addresses and cookie identifiers that create profiles on individuals and identify them.[57] Despite the technological source of these identifiers, they are not new and are commonly found in passports and other personal identity documents issued by states. The EU has nevertheless extended the scope of "personal data" with the advent of new technologies in the 1970s, leading to easily accessible datasets that served as catalysts in establishing a data protection framework.[58] The GDPR however does not apply to non-automated processing of personal data that is not intended to be part of an online filing system. Article 9 provides an outline to clarify the nature and scope of personal data within this data protection framework.[59] Thus, the complexity and challenge in this area arises through the respective national data protection legal frameworks. This is because nations outside of the EU have approached this area of the law quite differently.

Notwithstanding the above, a slightly different approach has been taken by Australia and Singapore. That is, Australia and Singapore specifically state how personal data and information is to be defined. Australia defines general personal data and information to be a person's full name, alias or previous name, date of birth, sex, current or last known address, and driver's license.[60] Interestingly, personal data in Australian law also includes a person's current and last employer. A point of difference is that Australia does not have a national identification card, unlike Singapore.[61] Once a person has begun working or undertaking business, no matter at what age, that person requires a tax file number. However, a tax file

[56] See Walters, Trakman and Zeller, above n 2.
[57] Ibid.
[58] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (European Commission, 20 June 2007) <http://ec.europa.eu/justice/data-protection/article- 29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.
[59] See GDPR arts 2, 9 provide for the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited. However, there are exemptions to this and Article 9(2) states that sensitive data can be processed where consent has been obtained for employment and social security and social protection law. This also extends to areas that are in the public interest, such as health and national security. Capacity has been provided to member states that allows them to introduce additional conditions regarding the processing of genetic data, biometric data or data concerning health. The exemptions introduced by Article 9(2) are considered far reaching and extend to genetic data used in research.
[60] See Zeller et al, above n 4.
[61] Ibid.

number does not capture every person, because it only applies to those people who are registered to pay tax.[62]

Beyond personal data, Australia has specified sensitive information to include "racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation or practices, or criminal record; health information about an individual; genetic information" that also includes health information.[63] Furthermore, biometric information can be used for the purpose of automated biometric verification or biometric identification, which is treated as sensitive data.[64]

Singapore has generally grouped sensitive and personal data together in a similar manner to the EU. Apart from the full name of the person, Singapore for decades has consciously implemented mechanisms that can identify people easily, such as the National Registration Identity Card (NRIC).[65] Singapore is also the only jurisdiction to mention a person's passport and mobile phone number as identifiable personal information. Whatever other jurisdictions describe as sensitive data and information, Singapore has generalised such data to include facial images, voice recordings, fingerprints, iris images and DNA profiling.[66] The EU, rather than define sensitive data, has also adopted a broad approach that is similar to Singapore.[67]

Regardless of the perceived benefits of international commercial arbitrators deciding on the protection of personal data involving transnational entities, to date there is little material jurisprudence that provides guidance or direction in the data protection regimes of the EU, Australia or Singapore. Nor is there a supranational data protection regime upon which international commercial arbitrators can rely in defining or applying supranational personal data protection laws. What can be established is that, while the EU is perceived as having the most sophisticated laws and regulations governing the processing of personal data, the GDPR does not distinguish between personal data in general and sensitive personal data.

This failure to differentiate between personal and sensitive data is a limitation in a data protection regime, including in the use of arbitration to resolve disputes over the collection and processing of personal data. The social reality is that sensitive personal data is one of the most important factors in determining an individual's perception of privacy.[68] The gradation of sensitivity could also decide the security level that is needed to exercise fair and effective control over access to such data.[69] The collection and processing of sensitive data is also a significant concern for individuals whose data may be at risk of being publicized or otherwise disclosed to third parties.[70] Furthermore, sensitive data is often considered as the core of both privacy and data protection law, and requires a stricter legislative and other regulatory

[62] *Privacy Act 1988* (Cth); *Privacy (Tax File Number) Rule 2015* (Cth).
[63] *Privacy Act 1988* (Cth) s 6.
[64] Ibid.
[65] Walters, Trakman and Zeller, above n 2.
[66] See Zeller et al, above n 4.
[67] See GDPR art 9.
[68] Walters, Trakman and Zeller, above n 2.
[69] See Sabah Al-Fedaghi, 'How sensitive is your personal information?' (Proceedings of the 2007 ACM Symposium on Applied Computing, Seoul, 11–15 March 2007) 165–169.
[70] See Constantine Photopoulos, *Managing catastrophic loss of sensitive data: A guide for IT and security professionals* (Rockland, 2008) 3.

protection.[71] The failure of some jurisdictions to distinguish sensitive data from general data is a limitation that complicates dispute resolution, including through ICA.

Accordingly, all three jurisdictions examined in this article provide data subjects with a level of control over their personal data. However, the extent of that control is insufficiently explicated and relies on the parties and those responsible for resolving data disputes, such as arbitrators, to fill gaps in delineating the limits of such control over such personal data.

Another element in the data protection puzzle is whether regulators can provide data subjects with reasonable control over the use of their personal data, mediated by the consent permitted by the applicable law in contracts concluded between data subjects and those that collect and process that personal data. By appreciating how such consent is protected by law, arbitrators can make more informed and more legally supportable determinations of whether the collection and processing of data is supported by such consent.

IV. Consent to Use of Personal Data

Consent of the data subject to the collection, mining and processing of personal data is arguably a cornerstone of data protection and privacy law.[72] However, it becomes apparent that the nature of consent is not clear. That is, subject to the terms and conditions under which the data subject gives consent to the first user, when does that consent extend to the second, third, fourth or fifth user, expanding further to a downstream chain of users? And how do the parties to agreements over the use of personal data consent to arbitration as the means of resolving disputes between upstream and downstream users of that data?

This chain of consent gives rise to discrete issues in resolving disputes over the use of personal data. The testing issue, here, is whether the data subject retains the right to bring an ICA claim against downstream users to whom that subject has not given express consent, as distinct from the consent it has provided to the first user. The ancillary question is whether such consent can be implied, and if so, the nature and extent of that implication and the social and legal consequences arising from it.

The second consideration relates to the difficulty and cost of data subjects regulating data use through a complex sequence of downstream users; and the attendant difficulty of adjudicators and arbitrators to imply that consent to downstream users. Whether the data subject's regulation of personal data downstream is constrained by the absence of consent, or through that subjects' privacy or IP rights, it is functionally difficult for a data subject to invoke an ICA claim against a sequence of data users with whom that subject has no direct relationship, nor privity of contract. This difficulty is accentuated by the fact that data subjects are likely to have no knowledge of such downstream users other than by discovering the use of such personal data in the public domain.

Resolving these difficulties entails determining how to manage the use of data involving multiple data users, in any and all forms. Even if data subjects could manage the use of their personal data downstream, such as through algorithms directed at identifying users, the costs of such management are likely to be exorbitant. The practical result would defeat a central

[71] See Tuomas Ojanen, 'Privacy is more than just a seven-letter word: The Court of Justice of the European Union sets constitutional limits on mass surveillance' (2014) 10(3) *European Constitutional Law Review* 528.
[72] See Walters, Trakman and Zeller, above n 2.

means of resolving data disputes, even by resort to ICA, which is regarded as more expedient and cost effective than judicial processing. Complicating the arbitral process is the complexity in determining the very parties to a personal data dispute in the absence of express consent between them. This raises a discrete challenge for the international commercial arbitrator, in deciding whether they have a mandate to decide the personal data dispute in the absence or *unclear* expression of consent between the disputing parties. Even if such a mandate is established, arbitrators need to demonstrate the value of ICA in resolving disputes more expeditiously than through courts within the civil justice system.[73] These practical difficulties are complicated by the very nature of the data subject's consent for downstream processors and miners to use personal data. If the data subject and the targeted downstream user have not agreed to ICA by contract, an arbitration tribunal is likely to deny its jurisdiction to consider the data subject claim. Given that the right to bring an ICA claim ordinarily depends on the agreement of the parties to arbitrate, the data subject would lack a consensual basis upon which to bring such a claim. Arguably, without such agreement, the data subject would also be unable to invoke ICA, even if the data user had prima facie evidence that the data user had violated that subject's right to privacy, or less emphatically, had violated that subject's pervasive IP right in that data.

The alternative is to construe consent negatively, namely, to require that data users cannot collect or use that data without pre-existing consent to that use. The practical difficulty is data subjects being subject to duress or undue influence to secure their consent *ex post facto*. For example, it may be doubted whether employees should validly be held to have consented to their employer's handling of their personal data, given structural and economic dependence of employees that undermine their freedom to decline such consent to use. In that case, the ICA tribunal may well conclude that the employees' consent is invalid, or at least, ought to be construed restrictively, on grounds that the data subject did not freely consent to that data use.[74]

The converse response is to require data collectors, miners and processors to pay the data subject a user price in order to secure consent. That requirement is consistent with user contracts and licensing agreements. It is also economically and legally justifiable as payment for personal data that has economic value to the user. However, there are risks and potentially significant costs in paying data subjects for their personal information. Conversely, there is the pervasive risk of data subjects not understanding the nature and implications arising from giving consent to use of their data. These risks, in turn, impact on the capacity of arbitrators to decide a potentially growing number of disputes over data use in the face of the uncertain impact of these risks.

The next section will highlight how the different jurisdictions under study construe consent to access and use personal data. It will also examine how parties can consent to resolving disputes over the use of personal data through trans-border arbitration.

V. Consent in the EU, Australia and Singapore

Consent to use personal data, by itself, is insufficient as a basis to control the use of that data by data collectors, miners and processors. The fact is that personal data is often captured, stored

[73] See Trakman, Walters and Zeller, above n 3.

[74] See, GDPR art 17 and recital 65, providing that an employee has a right to have personal data erased or cease to be processed where the employee objects to such processing or withdraws that consent, or where processing is no longer necessary for the purpose for which it was acquired and used.

and used by many other platforms beyond the consenting parties to the data use, such as by companies with which the data subject is unlikely ever to identify or interact.[75] Invoking the consent of data subjects to use personal information downstream is also impaired by the fact that, once the data is traded downstream (e.g. to the second, third, fourth or fifth point), the data subject would not know, nor be reasonably expected to know, anything about the use of his or her personal data. The stark reality is the difficulty faced by arbitrators in fathoming the boundaries of such consent along a lengthy and complex chain of users within a complex global network.

Data subjects could potentially address this obstacle in part through clear terms and conditions of consent to use granted to the first user, which also provide whether, when and how that user can extend the data subject's consent to subsequent users. This extension of consent can provide downstream users with greater legal protection in their use of personal data. Conversely, a data subject that limits such consent to the sale and use of personal data downstream provides that subject with a legally supported basis upon which to pursue ICA actions against one or more downstream users for the unauthorized use of that data. Such extended consent also provides an international commercial arbitrator with a more coherent basis upon which to determine whether the data subject did consent to downstream use, including contractual limits and conditions placed on that use.

The EU clarifies, while also complicating, the scope of consent to both upstream and downstream use of personal data. The concept of consent adopted by the GDPR encompasses: consent to use by contract, the performance of that contract, compliance with a legal obligation in such performance, protecting vital interests that are impacted by that performance, promoting the public interest, and protecting a legitimate interest pursued by the controller.[76] Article 7(4) of the GDPR affirms that the consent is not freely given if it is conditional.[77] Article 6 requires that processing personal data is lawful only if, and to the extent that, processing is necessary to satisfy one of four criteria.[78] The first criterion is that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.[79] The further EU requirement is that consent must constitute more than an informal conversation; it must be freely given, specific, informed and unambiguous, that is, persons consenting to the use of their personal data must be able to understand the purpose for which they are providing that consent.[80] This requirement of informed consent removes some ambiguity about the scope of consent by eliminating complexities over what constitutes an agreement. Recital 32 of the

[75] See Walters, Trakman and Zeller, above n 2.
[76] See GDPR art 6(1)(a).
[77] Ibid art 7(4). Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
[78] Ibid art 6.
[79] Ibid art 6(1)(a).
[80] Ibid art 4(11).

GDPR reinforces this point, by requiring that the consent of the data subject constitute a clear affirmative act, sufficient to demonstrate that the consent was freely given.[81]

The benefit of the GDPR requiring express consent is in ensuring that data subjects enjoy control over their personal data and that such control should not be foregone by an implication that is not the direct product of that subject's express consent. The benefit of such express consent is in providing an explicit regulatory framework which denies the right to use personal data to which the data subject has not expressly agreed. A further benefit is that, in the event of a dispute between data users and data subjects, the GDPR provides arbitrators with coherent guidance in determining rights to use personal data and in extending that use to downstream users. The GDPR also provides a legal framework in which adjudicators, including trans-border arbitrators, can resolve disputes over the consent to use personal data in an authoritative and sustainable manner.

A. Australia

The boundaries of consent to use personal data in Australia are conceived broadly.[82] The Australian Privacy Principles (APPs) require that personal information should be collected directly from the individual, unless that individual has consented to its collection from other sources, or if that collection is authorized by law. However, the APPs define consent as 'express consent or implied consent'.[83] The four key elements of such consent include: 1) the individual is adequately informed before giving consent; 2) the individual gives consent voluntarily; 3) the consent is current and specified, and 4) the individual has the capacity to understand and communicate that consent.[84]

The conception of consent to use personal data in Australia is distinct from the EU. Unlike the EU, which specifies what constitutes express consent, the scope of consent in Australian law is more likely to be inferred from the conduct of the individual and the APP entity.[85] It is not

[81] Ibid recital 32. The GDPR therefore requires the data controller to collect data only for a specified, explicit and legitimate purpose (otherwise known at the purpose limitation). The GDPR does not separately provide for the use limitation principle: it is folded into the purpose specification principle. The Organization for Economic Co-operation and Development Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, which were adopted in 1980—almost at the same time European Convention 108 was signed—have a similar approach to the purpose limitation principle, but are more specific on the exact time at which the purpose must be specified. Paragraph 9 states that the purposes for which personal data are collected should be specified not later than at the time of data collection. The Guidelines also incorporate the notion of incompatibility when they state that the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. Paragraph 10 explicitly mentions two exceptions to Article 9, determining that use of personal data for purposes other than those specified in accordance with Paragraph 9 may be admissible with the consent of the data subject or by the authority of law.

[82] *Privacy Act 1988* (Cth) s 6. However, it must be noted that the *Privacy Act* also deals with credit agencies, and there are specific provisions of consent related to their activities such as ss 21J and 21K.

[83] Australian Privacy Principles, consent is expressed in ss 6, 6.16, 6.17, 6.34, 6.35, 6.49, 6.52, 6.53, 6.54.

[84] Ibid.

[85] Office of Australian Information Commissioner, *Australian Privacy Principles Guidelines* (22 July 2019) Chapter B: Key concepts <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts>. An APP entity should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. It should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way. An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. Use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. An

implied if an individual's consent is ambiguous, or if there is reasonable doubt about the individual's intention. While the EU's GDPR envisages implied consent arising only from an individual's express consent, Australian law encompasses implied consent that is not contingent upon that express consent. The deficiency, here, is to determine when consent is implied where the data subject did not expressly agree to the use of personal data. As a result, ICA arbitrators who are subject to Australian law receive less explicit guidance in determining the scope of consent than under EU law.

B. Singapore

In Singapore, consent is required for the collection and disclosure of personal data.[86] Section 13 of Singapore's *Personal Data Protection Act 2012* (PDPA) prohibits organizations from collecting, using or disclosing an individual's personal data, unless that individual gives, or is deemed to have given, consent to collecting, using, or disclosing personal data. Deemed consent constitutes implied consent under Singapore's statutory law; this is distinguishable from Australian law in which consent is implied in fact, which arguably extends beyond the scope of statutory consent in Singapore law.[87] The requirement to obtain consent in Singapore does not apply when the collection, use or disclosure of an individual's personal data without consent is required, or is authorized under the PDPA, or any other written law.[88]

Section 15 of Singapore's PDPA addresses two situations in which an individual may be deemed to have consented. The first is when an individual voluntarily provides his/her personal data for a specified purpose. Under section 15(1), an individual is deemed to consent to the collection, use and disclosure of personal data for a purpose, if that individual voluntarily provides that data to the organization for that purpose and if it is reasonable that the individual would do so. The second situation in which consent is deemed is where an individual provides consent to the disclosure of his or her personal data by one organization ("A") to another ("B"). Under section 15(2), if an individual gives, or is deemed to have given, consent for disclosure of his or her personal data by A to B for a specified purpose, the individual is deemed to consent to the collection of that data by B for the identified purpose.[89] Nonetheless, organization A must notify the data subject of the purpose for which that personal data will be collected, used or disclosed.

The limitation in Singapore's PDPA is in providing data collectors and processors wide scope to invoke that statute to restrict the right of data subjects to control their personal data. An ancillary result is in failing to provide adjudicators, including arbitrators, with an adequate pathway for determining when consent to use personal data should not be implied. Moreover,

---

APP entity will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met: the opt out option was clearly and prominently presented it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out the individual was given information on the implications of not opting out the opt out option was freely available and not bundled with other purposes it was easy for the individual to exercise the option to opt out.

[86] Personal Data Protection Act 2012*,* sections 14 to 17. Section 14(1) of the PDPA states how an individual gives consent under the PDPA. In particular, an individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes.

[87] Australian Privacy Principles, consent is expressed in ss 6, 6.16, 6.17, 6.34, 6.35, 6.49, 6.52, 6.53, 6.54.

[88] PDPA s 14.

[89] Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts of the Personal Data Protection Act 2012* (27 July 2017) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-consent-obligation---ch-12-(270717).pdf>.

the PDPA arguably enables data collectors and processors to maintain that consent is implied based on their disclosure to the data subject of the specified purpose for which they will use that personal data. This open door to their collection, processing and use of personal data potentially complicates ICA in providing data collectors and users with a wide-ranging expanse in which to maintain that consent is implied by statute. At the same time, the PDPA provides arbitrators with a somewhat indeterminate legal framework in which to regulate the use of personal data.

C. Withdrawal of Consent

An important issue for an ICA arbitrator, too, is in determining when a data subject has withdrawn consent to the use of personal data. The concept of implied or deemed consent is significant because it adds another layer of complexity to the proposition that personal data is the subject of an intellectual property right, but without negating the value of that right.[90] Arguably, it is plausible that the right of individuals to both expressly and impliedly consent to the disclosure of their personal information presupposes that they have some form of intellectual property right in that data.[91] It is further arguable that the ability of data subjects to withdraw their consent to the use and processing of their personal data further strengthens their control through their ownership of that data.[92] This combination of consent to data use and intellectual property in that data are potentially important considerations in ICA, which empower an arbitrator to determine the application and use of consent by a data subject. In deciding whether and what level, if any, the data subject has withdrawn that consent, that arbitrator can influence whether the data subject had sold IP rights in that data.

The EU, Australia and Singapore all allow data subjects to withdraw their consent. Article 7(3) of the GDPR provides that data subjects shall have the right to withdraw their consent at any time. The withdrawal of consent under the GDPR does not affect the lawfulness of processing based on consent before its withdrawal. Similarly, in Australia, data subjects may withdraw their consent at any time, and that process of withdrawal should be readily accessible to those data subjects.[93] Once that subject withdrawn consent, an entity can no longer rely on past consent for any future use or disclosure of that subject's personal information.[94] Nevertheless, determining when a data subject has withdrawn consent is difficult to determine in practice, unless the entity has provided information to the data subject that such an option is available. Should the entity not provide such information, the data subject is unlikely to know or appreciate the opportunity to exercise the option.

However, there are implications supporting a data subject withdrawing consent, for instance, in not being able to access the service provided by the data processor. Section 16 of the Singapore PDPA provides that individuals may, at any time, withdraw any consent given or deemed to have been given in respect of the collection, use or disclosure of their personal data for any purpose by an organization.

These provisions for a data subject to withdraw consent to an entity using personal data can facilitate ICA, by providing a legal basis upon which arbitrators can determine the legal limits

[90] See Walters, Trakman and Zeller, above n 2.
[91] Ibid.
[92] Ibid.
[93] Office of Australian Information Commissioner, *Australian Privacy Principles Guidelines* (22 July 2019) https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/ ; *Privacy Act 1988* (Cth).
[94] Ibid.

of consent. The problem is when a data use contract prohibits the withdrawal of consent while the applicable law allows it. To hold that the applicable law prevails over the contract depends somewhat on whether that law provides a largely unqualified right to withdraw consent and the extent to which the data use contract explicitly denies such withdrawal. Such issues are necessarily addressed by adjudicators, including arbitrators, albeit subject to circumspection over their pervasiveness.

VI. Transnational Transfer of Personal Data

Of relevance to ICA is the fact that the transnational export of and trade in personal data is expanding on a monumental scale. This expansion is likely to lead to a mushrooming of disputes over the use of personal data. An obstacle in deciding such disputes is whether the laws governing trade in personal data ought to be regulated extra-territorially in light of laws that diverge across regions and states. The GDPR, notably, has as an extra-territorial reach. Article 49 provides for the transfer of personal data to a third country or an international organisation in the absence of an adequacy decision under Article 45(3), or appropriate safeguards under Article 46.[95] This poses challenges for the operation of ICA when that transfer requires the establishment, exercise, or defence to a legal claim and when there is no other way to reach an "adequate" decision.[96] Article 45 allows the European Commission to assess the adequacy of protection for the transfer of data extra-territorially. That enables the transfer of personal data to a third country to be undertaken, provided that third country has adopted the adequacy standard data protection clauses provided for by the European Commission.[97] To date the only countries to obtain recognition of that adequacy standard include: Andorra, Argentine, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States. Notable absentees are Australia and Singapore. Arguably, obtaining an adequacy assessment from the EU can go a long way to protect the transfer of personal data to a third country, unless model clauses are adopted, or binding corporate rules can manage this issue. The challenge for arbitrators is in evaluating these requirements and their applicability both under the GDPR and in accordance with the law of third party states. Accentuating that challenge is the absence of an interpretive history in applying the GDPR's adequacy requirements, inter alia, in light of the laws of those states.

Accordingly, the question arises whether the laws of Australia and Singapore provide a level of an adequacy standard that is comparable to the requirements of the EU. Section 26 of the Singapore PDPA requires that an organization shall not transfer any personal data to a country

[95] See GDPR art 49: In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; d) the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

[96] Ibid art 49(e).

[97] Ibid art 46.

or territory outside Singapore, except in accordance with requirements prescribed under that Act. The stated purpose is to ensure that such organizations provide a standard of protection to the personal data so transferred that is comparable to the protection under the PDPA Act.[98] Section 26 states further that the Personal Data Protection Commission may, on the application of any organization by notice in writing, exempt the organization from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organization. However, an exemption exists whereby the Commission may, through a notice in the Gazette, revoke, add to or vary any condition imposed under Section 26. This broad and flexible approach allows Singapore to either strengthen or dilute its approach to regulating the transfer of personal data extra-territorially.

More importantly, section 27 of the PDPA provides for 'alternative dispute resolution'. It states that if the Commission is of the opinion that any complaint by an individual against an organization may more appropriately be resolved by mediation, the Commission may, with the consent of the complainant and the organization, refer the matter to mediation.[99] Most important though is the way in which Singapore has not, on the face of it, restricted the dispute resolution process to only mediation. Section 27(2) provides that, subject to subsection (1), the Commission may, with or without the consent of the complainant and the organization, direct a complainant or the organization or both, to attempt to resolve the complaint of the individual in the way directed by the Commission.[100] Significantly, this discretion allowing the Commission to direct the process of dispute resolution does not rule out the potential to resort to international ICA. Prospective resort to arbitration is accentuated further by the fact that mediation is a facilitative process in which the mediator assists the parties to reach agreement, which may not eventuate.[101] In contract, arbitration is a determinative process in which the arbitrator(s) reach a decision over the transmission of personal data which binds the parties. As a result, mediation that fails to facilitate a settlement agreement between the disputing parties often results in resort to arbitration in which the arbitrators decide the dispute over the communication and other use of that personal data.[102]

In Australia, APP 8.1 has determined that an overseas recipient is one that is not located in or on the Australian territory.[103] APP 8 does not apply to an organization that receives the personal information in a third country which is the same entity.[104] On the one hand, where an APP entity has offices located in both Australia and Singapore, and personal information is being sent from the Australian office to the Singapore Office, APP 8 will not apply because the recipient is the same entity. However, in a case in which the APP entity in Australia sends

[98] PDPA s 26.
[99] Ibid, s 27.
[100] Ibid; Personal Data Protection Commission Singapore above n 108. The PDPA generally recognises that a complainant and an organisation may resolve the issues in a complaint by negotiation, mediation or other modes of dispute settlement. Where the complainant and the organisation are able to resolve the issues in a complaint and reach an agreement on the matter including, for example, any actions to be taken by the organisation to address the complaint, the Commission will consider the agreement reached in determining whether to take any further enforcement action. In particular, the PDPA provides that the Commission may suspend, discontinue or refuse to conduct an investigation where the parties involved (that is, the complainant and the organisation) mutually agree to settle the matter (among other situations).
[101] See Bruno Zeller and Leon Trakman, 'Mediation and Arbitration: The Process of Enforcement', 24(2) (2019).*Uniform Law Review* 449
[102] Ibid.
[103] APP 8 and *Privacy Act 1988* (Cth) s 16C create a framework for the cross-border disclosure of personal information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (*Privacy Act 1988* (Cth) s 16C).
[104] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

personal information to a 'related body corporate' located outside of Australia,[105] and that related body corporate is a different entity to the APP entity in Australia, the former will be regarded as an 'overseas recipient' and APP 8 will apply. Importantly, APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient complies with the APP in relation to that information.

An arbitrator charged with the responsibility to resolve a dispute over the protection of personal data would need to determine the existence and nature of the relationship between the entities in the country of origin and in the third country, and the particular consequences arising from, but extending beyond, that relationship.

i. Discovery & Disclosure

It is widely understood that the nature of discovery differs, inter alia, between civil and common law countries. Discovery is the process by which each party to a litigation is bound to produce documents requested by the other. In general terms, civil law jurisdictions ordinarily limit disclosure to that which is proffered by each party as evidence in support of the party's case. In contrast, pre-trial discovery in common law countries, particularly the United Kingdom, are much broader in nature and scope.

ICA is not ordinarily subject to stringent discovery procedures that exist, particularly in common law jurisdictions. However, ICA arbitrators are bound by the choice of law and jurisdiction of the disputing parties which may impose more, or less, stringent discovery requirements. Due to the broad reach of the GDPR, even if a European entity involved in ICA proceedings is willing to provide discovery in such proceedings, it must still comply with the applicable privacy and data protection laws. It is therefore important that an ICA tribunal carefully manage the discovery process and carefully address privacy and data protection issues in recognition of the applicable law. In *Dante Yap Go v Bank Austria Creditanstalt AG,* the Singapore High Court held that:

> the discovery regime erects two principal barriers that must be satisfied before discovery is ordered. First, the documents must be relevant; and second, even if relevance is proven, discovery must be necessary either for disposing fairly of the cause or matter or for saving costs.[106]

As a result, in an arbitration where one party is from a common law jurisdiction and another from the civil law jurisdiction and where the tribunal is a mix of both common and civil law countries, there can be significant divergence in the way in which discovery and or disclosure is mandated by that tribunal. Again, the varied approaches taken across different countries that also differ from the EU pose further challenges to arbitration disputes over the use of personal data.

Nevertheless, even though laws and discovery procedures that vary across jurisdictions can complicate arbitration proceedings, arbitrators face comparable issues in deciding ICA disputes

---

[105] *Privacy Act 1988* (Cth) s 6. Section 6(8) provides 'for the purposes of this Act, the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the *Corporations Act 2001*'.
[106] [2007] SGHC 220, 69 [17].

well beyond personal data. Moreover, given that such arbitrators ordinarily address such issues, while courts do so less pervasively, it is arguable that arbitrators are better suited to make such decisions than domestic courts, all other factors being constant.[107]

VII. Possible Solution

Beginning with the EU,[108] to assist in facilitating personal data flows from one member state to another, a common set of rules have been promoted for adoption across such states, to ensure greater consistency in approach to the protection of personal data. This is done against the backdrop of the absence of global data protection and standardized contractual clauses.[109] Such a framework consistently enables adjudicators, including arbitrators, to determine when a data exporter has failed to use reasonable efforts to determine whether the data importer has protected personal data under shared data rules and standardized contract clauses; and enabling the data subject to proceed though litigation and/or arbitration against the data exporter for failing to do so.[110]

In addition to the above, the EU's Commission Decision 2004/915/EC provides guidance on the termination of a contract, variation from standardized clauses and in the description of the transfer of personal data. Such guidance can assist ICA arbitrators in determining whether to enforce the data contract in the event of a dispute, and when and how to do so. Firstly, the enforcement clause creates the possibility of data exporters carrying out audits on data importers' premises, or to request evidence of sufficient financial resources to fulfil its responsibilities. Secondly, the enforcement clause is governed by the law of the country in which the data exporter is established, except for laws and regulations on processing personal data by the data importer[111] which shall apply only if so selected by the data importer under that clause. Thirdly, and more importantly, the resolution of disputes with data subjects or the supervising authority provides that the parties consider participating in ICA to resolve any disputes.[112] However, decisions reached under EU law are not binding on member states and therefore the Commission Decision does not have to be applied. Nonetheless, the Decision does provide for a resolution of the above issues, without foreclosing the modification of contracts to clarify the applicable variables in data protection laws and personal data traded to and by third parties.

The Commission Decision also clarifies the scope of the data subject's consent to the export of personal data, including the requirements and documentation which the data importer is required to submit on the request of the exporter. Clause II(g) states that, upon the reasonable request of the data exporter, the importer will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular

[107] See Trakman and Montgomery, above n 38.
[108] *Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries* [2004] OJ L 385.
[109] Ibid, preamble 2–5.
[110] Ibid.
[111] Ibid cl II(h).
[112] Ibid cl V(b).

business hours.[113] The request will be subject to any necessary "consent" or approval from a regulatory or supervisory authority within the country of the data importer, which "consent" or approval the data importer will attempt to obtain in a timely fashion. Further at (iv), regarding the onward transfers of sensitive data, it stipulates that data subjects have given their unambiguous "consent" to the onward transfer.

These provisions for the contractual consent of data subjects, while still early in their inception, provide a regulatory framework within which parties to data contracts can regulate their mutual dealing, within a supervisory framework. These provisions for consent also assist adjudicators, and ICA tribunals in particular, to assess whether a data user has breached a data contract or otherwise violated the data subject's privacy or IP rights.

In Singapore, the Guide on Data Protection Clauses for Agreements relating to the Processing of Personal Data[114] ("the Guide") was established in 2016 to provide guidance on data protection between organizations. However, a notable omission from the Guide is any reference to disputes and to ICA. Australia does not provide any specific guidance on the processing of personal data.

It is our view that ICA can facilitate the resolution of disputes over data use, given legal developments, notably in the EU, to regulate the transmission of personal data across national and regional boundaries. The key operative requirement, however, is for the data contract to provide clearly for the choice of arbitration. That contract, guided by regulatory and interpretive rules, should also enable the parties, and failing that, an arbitration tribunal, to effectively manage the transnational trade in personal data on a continuing basis.

VIII. Final Remarks

The article has sought to provide an understanding of some of the key elements that need to be considered in an emerging area of law that is seminal to commerce, and to state, regional and transnational regulation. Key to that regulation is guidance in the resolution of disputes over the use of personal data. Given these interlocking attributes in the regulation of data privacy across national boundaries, the article has argued for greater resort to, and reliance upon ICA. It has so argued in light of different conceptions of consent that prevail nationally and regionally and the virtual absence of international regulation on the transmission of personal data. It has stressed the prospect of greater conflict between data subjects and data users over the use of personal data, the likelihood of such conflicts leading to formal disputes, and the perceived preference for ICA in resolving those disputes.

A key focus of the article has been on how data contracts between data subjects and users can be used to improve on the management of personal data in cross-border trade. It has argued that such contracts, supported by suitable regulatory mechanisms and model clauses, can facilitate sustainable data usage contracts that function expeditiously but also fairly in regulating the transmission of personal data. Contract clauses can also provide for investor-state dispute settlement (ISDS), by which investor-state arbitrators resolve disputes over state regulation of the use of personal data. However, to do so efficiently, both ICA and ISDS

[113] Ibid cl II(g).

[114] Personal Data Protection Commission, *Guide on Data Protection Clauses for Agreements relating to the Processing of Personal Data* (20 July 2016) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-on-dp-clauses-for-agreements-related-to-processing-of-personal-data-v1-0-(200716).pdf>.

arbitrators need to function within a viable regulatory framework. Regulators need to provide arbitrators with an appreciation of the central issues that are likely to arise in disputes over the protection of personal data. These include, among others, the definition of personal data, along with the application of consent to others using that data, and limitations of consent to afforded to data subjects.

In responding to these needs, the article has explored the elongated chain of data users, the limits of express consent in managing such use, and methods of resolving ensuing disputes over such use. One regulatory response to resolving disputes over down-streamed data use is to extend the scope of consent to resolve disputes between data subjects and data collectors, miners and processors. Thus, the combination of contractual and legal regulation of personal data is important in resolving disputes over data use through ICA in which one is insufficient to do so in the absence of the other.

The European Union, Australia and Singapore all have regulatory regimes that provide for the resolution of international commercial disputes through arbitration. However, in addressing the first question posed by this article, it is necessary to delineate the elements of data protection law that are relevant to the initiation and conduct of ICA proceedings. How is ICA employed most effectively to resolve transnational disputes in personal data trade? The IBA Rules on the Taking of Evidence in ICA (the IBA Rules) address this question as follows: pursuant to Article 9(2)(b) of the IBA Rules, the arbitral tribunal shall exclude from production any document if such production is unlawful. However, Article 9(3)(e) of the IBA Rules expressly acknowledges the need to maintain fairness and equality between the parties, particularly if they are subject to different legal or ethical rules. The result is that, while these Rules do not definitively regulate the taking of evidence in ICA disputes over the use personal data, they do provide guidance in establishing reasons for arbitrators denying the production of documents into evidence.

Particularly challenging, too, is the need for arbitrators to recognize the importance of confidentiality in ICA proceedings, as they relate to the very nature and use of personal data. In addressing this challenge, regulators and arbitrators should restrict the disclosure of confidential documents even if they are likely to have high evidentiary value and relevance to arbitration awards. In addition, parties to arbitration should be required to implement a strict document retention policy prior to initiating arbitration. Subject to the general retention obligations of the parties, the assumption is that, the less personal data a party stores, the fewer conflicts are likely to arise over the application of data protection laws.

Finally, ICA is an important medium through which to protect personal data without unduly trammeling the transmission of data across national boundaries. The value of ICA in regulating such transmission is to mediate, effectively and fairly, among the freedom to protect personal data, the freedom to transact in data, and the public's right to know.