THE ROLE OF INTERNATIONAL MEDIATION IN DATA PROTECTION AND PRIVACY LAW - CAN IT BE EFFECTIVE?

SINTA DEWI, ROBERT WALTERS, BRUNO ZELLLER AND LEON TRAKMAN

(2019) 30 *Australian Dispute Resolution Journal* 61
[2019] *UNSWLRS* 77

UNSW Law
UNSW Sydney NSW 2052 Australia

The Role of International Mediation in Data Protection and Privacy Law – Can It Be Effective?

Sinta Dewi, Robert Walters, Bruno Zeller and Leon Trakman*

The role of international mediation and mediation more generally in data protection and privacy law can be an effective tool to resolving data disputes. This article will examine the data protection laws of Indonesia, Australia, Singapore, the Philippines, European Union and China. This comparative examination is timely, with the creation of the Convention on Enforcement of International Settlement Agreements Resulting from Mediation (Singapore Convention) which opened for signing on 7 August 2019 and the associated Model Law. If implemented and utilised, the Singapore Convention has the potential to become an effective legal mechanism to assist in resolving cross-border personal data disputes.

I. INTRODUCTION

Personal data is being traded nationally and internationally. Regulating the protection of personal data[1] by the law, underpins the protection of personal privacy over the internet.[2] With the vast expansion in the collection and sharing of personal data crossing many country boundaries, disputes on data privacy and data protection is likely to involve potentially the law of several jurisdictions. To date trans-border disputes need to resort to arbitration under the framework of the United Nations Commission for International Trade Law (UNCITRAL). The issue is that arbitration is only applicable as a contractual term implemented either before or after the disputes arise. However, the proposed *Convention on Enforcement of International Settlement Agreements Resulting from Mediation* (*Singapore Convention on Mediation*) which will be open for signing in Singapore on 7 August 2019 and the associated Model Law[3] – and will be an appropriate tool to assist in mediation of personal data disputes in cases where no dispute resolution mechanism has been agree on. At issue is whether there will be enough signatories to enable it to be ratified and fully implemented.

The introduction of the *General Data Protection Regulation* (*GDPR*) by the European Union (EU) in 2018[4] has in our view resulted not only in countries having to consider personal data in cross-border transactions, but also beginning to influence how parties will resolve disputes. The International Council

* Sinta Dewi Rosadi: LLB (Unpad), LLM (Washington College of Law, American University), PhD (Unpad), Associate Professor in Law at Faculty of Law University of Padjadjaran, Bandung, Indonesia. 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. 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. 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.

[1] P De Hert and S Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power" in E Claes, A Duff and S Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia, 2006) 61–104.

[2] R Walters, L Trakman and B Zeller, *Data Protection: A Comparative Analysis of Asia-Pacific and Europe* (Union Springer, 2019).

[3] *Model Law International Commercial Conciliation* (Model Law) 2002. The Model Law seeks to revise this, primarily by replacing the term "conciliation" with "mediation".

[4] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation) OJ L 119.

for Commercial Arbitration (ICCA) and International Bar Association (OBA) have recently announced a joint taskforce to produce a guide to one of the most challenging current issues in international arbitration – data protection.[5] Even though these organisations focus on arbitration, any guidance and practice notes will also be relevant to international mediation and dispute resolution.

Part II will determine whether the respective laws preclude or provide for mediation and dispute resolution. It also highlights the need for states to follow Singapore's lead and establish specific provisions within the law that provide for dispute resolution. This part also briefly looks at contractual disputes under the proposed *Singapore Convention on Mediation*. Part III introduces the data protection laws of the various jurisdictions that will be examined. Part IV identifies what are considered the key concepts of data protection law. Finally, Part V concludes by determining a pathway forward for mediators and dispute resolution practitioners.

II. MEDIATION AND DISPUTE RESOLUTION

Mediation has emerged as an alternative to resolving legal disputes instead of through the judiciary. It is a process in which the parties to a dispute, with the assistance of a dispute resolution practitioner (the mediator), identify the disputed issues, develop options, consider alternatives and endeavour to reach an agreement. More importantly, mediation is a confidential process, which serves well for parties of a dispute. Today, it is widely seen as being very effective in reducing complex and long drawn out costly legal disputes both nationally and internationally. However, in the context of personal data and data protection law, mediation has only recently been considered as an effective option for dispute resolution.

Singapore being one of the most pro-mediation and arbitration countries throughout Southeast Asia has been working for some time to develop the proposed Singapore Convention. Moreover, pertaining to data protection, *Personal Data Protection Act 2012* (Singapore) (*PDPA*), is distinctly different to that of its regional and European counterparts. The *PDPA* specifically refers to mediation as an effective mechanism to resolve data issues. Section 27 of the *PDPA* sets out the Commission's powers in relation to the resolution of complaints.[6] Section 27(1) of the *PDPA* states that if the Commission is of the opinion that any complaint by an individual against an organisation may be more appropriately resolved by mediation, the Commission may, with the consent of the complainant and the organisation, refer the matter for mediation. Furthermore, s 27(2) goes onto say that the Commission may direct a complainant or an organisation or both to attempt to resolve the complaint of the individual in the way directed by the Commission. The Personal Data Protection Commission has broad power to direct the parties involved in a dispute over personal data, to establish a mediation process to resolve the dispute.

The Philippines have followed the same path as Singapore. Section 7 (b) of the data protection law provide that alternative dispute resolution, as a process may be used by the Commission to resolve disputes in data protection law. It must be noted that it is out of the scope of this paper to examine the procedural steps for concluding and implementing any decision from such a dispute resolution procedure. On the other hand, neither Indonesia,[7] China or Australia specifically refer to alternative dispute resolution or mediation as a process for resolving personal data disputes. However, just because the respective legislations in these states do not specifically state that mediation is an option, does not mean it cannot be used to resolve data protection disputes. It is our view that the Singapore example provides individuals and entities with clarity and certainty. It is our further view that the other states should consider adopting similar provisions within their respective data protection and privacy laws.

[5] International Council for Commercial Arbitration and International Bar Association <https://www.arbitration-icca.org/news/2019/418/icca-and-iba-establish-task-force-on-data-protection.html>.

[6] *Personal Data Protection Act 2012* (Singapore) s 27 is entitled "Alternative dispute resolution".

[7] In Law Number 30 year 1999 on Arbitration and Alternative Dispute Resolution stipulated that to settle dispute can use ADR and Arbitration and the similar approach also takes by EIT Law.

A. Personal Data Forming Part of Contracts – Mediation

The trade in personal data has evolved into an important economic activity. It comes with many challenges, and similar to the international trade in goods and services, the trade in personal data can be included into contracts.[8] The EU attempted to resolve the lack of a consistent legal framework governing the enforcement of mediated agreements by releasing the *Directive on Certain Aspects of Mediation in Civil and Commercial Matters* in 2008.[9] Interestingly the Directive also includes a limitation on the enforceability of mediation in the Preamble to Art 6(1). Sentence 2 notes:

> [I]t should only be possible for a Member State to refuse to make an agreement enforceable if the content is contrary to its law, including its private international law, or if its law does not provide for the enforceability of the content of the specific agreement.[10]

This limitation on the enforcement of mediated agreements is consistent with jurisprudence maintaining that arbitration awards are also not enforceable if the applicable choice of law clause so stipulates in a contract providing for arbitration. Nevertheless, mediation is distinguishable from arbitration, both as a process and in light of the purposes that are attributed to it. Even though both arbitration and mediation are directed at resolving a dispute, mediation is perceived to be more time- and cost-efficient than arbitration including in the enforcement of an arbitration award.

The essential element in mediation involves the enforcement procedures that do not consume too much time and costs. Otherwise, the consensus between the mediating parties which is reflected by the mediation settlement agreement might be at stake.[11] At issue has been the long and protected enforcement proceedings of mediation agreements. As highlighted by Zeller and Trakman, the issue is that the parties to an arbitration agree to appoint an arbitration tribunal, and the tribunal then renders an award. The award is a product of the agreement between the parties only insofar as they agree upon an arbitration process, including to abide by the result (final and binding).[12] The parties to a mediation enter into an agreement to mediate. In that agreement, they ordinarily appoint a mediator and, possibly, determine the mediation process. However, they do not ordinarily agree to reach a final agreement through mediation. The mediated agreement they conclude at the end of the mediation may entail an agreement on all, or only some, issues in dispute. It may also include an agreement to forego the benefits that one party, or both parties, sought through mediation. If they are able to do so, they conclude a mediated agreement in the form of a contract.[13]

However, and should the proposed *Singapore Mediation Convention* (*SMC*)[14] be ratified, this issue should be potentially resolved depending on which states are ratifying the Convention.[15] It is argued that the proposed 2019 *SMC*[16] could be for mediation what the *1958 New York Convention* currently is for arbitration. In effect, this will be a positive step, by narrowing the gap between the expeditious enforcement of arbitration awards and less expeditious judicial enforcement proceedings of mediated

---

[8] B Zeller and L Trakman, "Mediation and Arbitration – The Process of Enforcement" (2019) 24 *Uniform Law Review* 449.

[9] *Directive 2008/52/EC Certain Aspects of Mediation in Civil and Commercial Matters.*

[10] *Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008*, Preamble [19].

[11] *Directive 2008/52/EC.*

[12] *Directive 2008/52/EC.*

[13] *Directive 2008/52/EC.*

[14] *Proposed Singapore Mediation Convention*, Art 1.

[15] On the development of the Singapore Mediation Convention, see *The Singapore Mediation Convention: An Overview* <https://www.globalpound.org/2018/07/12/the-singapore-mediation-convention-an-overview/>.

[16] In June 2018, a draft legal framework for international commercial mediation was finalised at UNCITRAL's 51st session. The Commission approved the Model Law on International Commercial Mediation and International Settlement Agreements resulting from Mediation, essentially allowing parties to enforce their mediated settlement agreements across jurisdictions. The Commission also endorsed proposals for the signing ceremony to be held in Singapore on 1 August 2019, and for the Convention to be referred to as the "Singapore Mediation Convention". The landmark decision comes after three years of negotiations and drafting, a mammoth task that involved input from as many as 85 countries and 35 NGOs. It still pends approval by the UN General Assembly in December 2018 and, once approved, remains subject to there being sufficient countries ratifying it next year.

settlements.[17] On the one hand, "the gap may be narrowed between the enforceability of arbitral awards and the enforceability of judgments in which arbitral awards enjoy an advantage".[18] On the other hand, there is the need for mediated contracts to be enforced a lot more effectively and efficiently, not unlike the enforcement of arbitration awards. Of importance are Arts 4[19] and 5[20] of the proposed Mediation Convention as they provide provision for settlements agreements. Therefore, a party seeking to enforce an international settlement agreement pursuant to the *SMC* must provide a signed copy of the international settlement agreement; and evidence that the international settlement agreement resulted from mediation. While on paper this can be achieved quite easily, in practice many disputes are concluded by combining matters, and in some cases certain matters may only have obtained in principle support. Thus, any matters within the agreement that have in principle support will need to be clarified and confirmed following the conclusion of the mediation process. However, this could pose issues to concluding signed agreements in accordance with Art 4.

Notwithstanding the above, Art 4(b) of the *SMC* also becomes important because there are no restrictions on what evidence can be provided to prove a settlement agreement from mediation. That is, Art 4(b) provides that proof may be provided by the mediator confirming mediation occurred, or signing the settlement agreement. It requires that any mediation is well documented. More importantly, Art 5(1) and 5(2), following the lead of the *New York Convention on the Recognition and Enforcement of Foreign Arbitration Awards* (*NYC*), outline the grounds under which a state might refuse enforcement. Where relief is sought under Art 4 by the contracting state that, relief may be refuse only if that party furnishes to the competent authority proof that party to the settlement agreement was under some incapacity. That is, where the settlement agreement sought to be relied upon:

- is null and void, inoperative or incapable of being performed under the law to which the parties have validly subjected it or, failing any indication thereon, under the law deemed applicable by the competent authority of the contracting state where relief is sought under Art 4;
- is not binding, or is not final, according to its terms;
- has been subsequently modified;
- the obligations in the settlement agreement have been performed, or are not clear or comprehensible; granting relief would be contrary to the terms of the settlement agreement;
- there was a serious breach by the mediator of standards applicable to the mediator or the mediation, without which breach that party would not have entered into the settlement agreement; or
- there was a failure by the mediator to disclose to the party's circumstances that raise justifiable doubts as to the mediator's impartiality or independence and such failure to disclose had a material impact or undue influence on a party, without which failure that party would not have entered into the settlement agreement.

In addition, Art 5(1)(b)(ii) of the *SMC* provides for refusal of relief if the mediated settlement agreement is not binding, or is not final, according to its terms. Thus, the parties may conclude mediations with an agreement in principle. Therefore, notwithstanding that a party in this situation is unlikely to have a signed mediated settlement agreement, a party seeking enforcement will also be faced with an additional hurdle of having to establish that the agreement in principle is binding. Furthermore, and as Nadja Alexander highlights:

> "[T]he penultimate and last grounds" relating to mediator conduct under Article 5(e) and to impartiality and independence under Article 5(f) "aligns with Articles 5(4), 5(5) and 6(3) of the 2002 Model Law on International Commercial Conciliation".[21]

---

[17] The Australian Dispute Resolution Research Network, *A Tribute to Mediation's Grassroots* <https://adrresearch.net>.

[18] Chief Justice Robert French AC, *Arbitration and Public Policy 2016 Goff Lecture* (18 April 2016) 5 <http://www.hcourt.gov.au/assets/publications/speeches/current-justices/frenchcj/frenchcj18Apr2016.pdf>.

[19] *Proposed Singapore Mediation Convention*, Art 4.

[20] *Proposed Singapore Mediation Convention*, Art 5.

[21] Nadja Alexander (ed), "Singapore Convention on Mediation" on *KluwerMediationBlog* (24 July 2018) <http://mediationblog.kluwerarbitration.com/2018/07/24/singapore-convention-mediation>.

It is worth noting the distinction between the *SMC* and the *New York Convention*. That is, unlike the *New York Convention*, Art 5(f) of the *SMC* requires not only the mediator's lack of impartiality or independence in the process, but also that this mediator's lack of impartiality or independence had a material effect on the outcome. This is an important point, because in contrast, under the *New York Convention*, a party does not need to demonstrate that the circumstances had a material effect on the award. It is sufficient under Art V(1)(b) of the *New York Convention* to establish that a party not given proper notice of the appointment of the arbitrator or of the arbitration proceedings or was otherwise unable to present his case.

The proposed *SMC* has replicated several reasons for a court refusing to enforce an arbitration award as provided for in the UNCITRAL Model Law (Model Law) and the *NYC*. What is significant about the *SMC* is that it will offer enforcement of settlement agreements to be achieved from mediations conducted in foreign jurisdictions, in the same way as the *New York Convention* has achieved for arbitration awards. Therefore, in our view mediation can and should be used to resolve cross-border disputes involving personal data. This is on the back of whether the *SMC* comes into effect or not.

III. Data Protection Law

The year 2017 and 2018, were both significant years for data protection law. The EU finally implemented its long awaited *GDPR 2016/679*.[22] The EU believe that the processing of personal data should be designed to serve mankind. In other words, the *GDPR* respects all fundamental rights and observes the freedoms and principles recognised in the EU Charter of Fundamental Rights.[23] A year earlier in 2017, China released the final version of a new data privacy standard on data.[24] In China, the Cyber Security Law[25] was formulated in order to ensure cybersecurity; safeguard sovereignty and national security, and social and public interests.[26]

Australia's *Privacy Act 1988* (Cth) is the principal legislation that regulates privacy, personal data and personal information. The Privacy Act is underpinned by the Australian Privacy Principles (APP).[27] The APPs provide organisations with a governance framework to transparently manage personal data, and are enforceable.[28] Indonesia, on the other hand, is a relatively new country in regulating data protection and privacy. Indonesia takes a sectorial approach, and in 2008 the Indonesian Parliament approved the *Electronic Information and Transactions Law No 11 of 2008* (EIT) and amended in 2016 by *Regulation No 19 of 2016*. In the same year the Minister of Communication and Information (MCI) *Regulation No 20 of 2016 on Personal Data Protection in the Electronic System* was also established. This is the first law in Indonesia that goes some way in regulating personal data and privacy, however, it is restricted to data in electronic form. *Regulation No 20 of 2016*, implements *Regulation No 82 of 2012* on Implementation of Electronic Transactions and Systems.[29]

---

[22] The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the *Charter of Fundamental Rights of the European Union* (the Charter) and Art 16(1) of the *Treaty on the Functioning of the European Union* (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

[23] *Charter of Fundamental Rights of the European Union*, Official Journal of the European Communities C364/5.

[24] T Magee, *China's Data Privacy Law Came into Effect This May – and It Was Inspired by GDPR* (2018) <https://www.computerworld.com/article/3427753/china-s-data-privacy-standard-came-into-effect-this-may---inspired-by-gdpr.html>.

[25] *Translation: Cybersecurity Law of the People's Republic of China* (effective 1 June 2017) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>.

[26] *Cybersecurity Law of the People's Republic of China*, n 25, Art 1. Article 1 states that the law aims to protect the lawful rights and interests of citizens, legal personal, and other organisations: and promote the healthy development of the informatisation of the economy and society.

[27] Office of information Commissioner, in December 2000, the *Privacy Amendment (Private Sector) Act 2000* (Cth) extended coverage of the Privacy Act to some private sector organisations. The amendments commenced on 21 December 2001. These amendments introduced 10 National Privacy Principles (NPPs) into the Privacy Act, which set out standards in relation to private sector organisations collecting, using and disclosing, keeping secure, providing access to, and correcting personal information.

[28] *Privacy Act 1988* (Cth) s 6. Australian Privacy Charter Council "The Australian Privacy Charter" (1995) *Privacy Law and Policy Reporter* 31; 1995, 2(3) *Privacy Law and Policy Reporter* 44. *Data-matching Program (Assistance and Tax) Act 1990* (Cth) regulates the commonwealth government data-matching using tax file numbers.

[29] A Aditya Rahman, *Indonesia Enacts Personal Data Regulation, Privacy Laws and Business* (Data Protection and Privacy Information Worldwide, 2017) Issue 145.

In Singapore, the *Personal Data Protection Act 2012* (No 26 of 2012) – (*PDPA*) was introduced and arguably strengthens Singapore's business and trade competitiveness in the region.[30] The *PDPA*, provides the minimum standard for the protection of personal data across Singapore society.[31] The *PDPA* recognises the balance between the need to protect individuals' personal data and the need of organisations to collect, use, transfer or disclose personal data.[32] Similar to Singapore, the Philippines implemented their data protection laws in 2012 – The *Data Privacy Act 2012* (Philippines) (DPA).[33]

What has emerged from these laws are key concepts and principles in data protection law that are increasingly becoming very important to controlling a data subject's personal data. The next part highlights some of those key concepts and principles that will need to be considered in cross-border mediation and dispute resolution process.

IV. Key Concepts of Data Protection Law

Data protection law is complex and this part has been limited to what the authors consider the most important concepts that a mediation will need to consider and address. It deliberately highlights in detail the variables within the law.

A. Definition of Personal Data

The definition of personal data and personal information, has arguably, become very important to data protection law. Without such a definition, there is little to no starting point to determine what constitutes personal data and information.

Australia and Singapore specifically state what and 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, gender, current or last known address, and driver's licence. An important identifying information under Australian law also includes a person's current and last employer. Australia does not have a national identification card, as is the case in Singapore. However, once a person has begun working or undertaking business, no matter what age, that person does have a Tax File Number. But, unlike Singapore, that tax file number does not capture every person, because it only applies to those people that are registered to pay tax.[34]

The use of the term "personal data" in the EU may have some significance, as it was the advent of new technology in the 1970s that resulted in easily accessible datasets that served and the catalyst for the establishment of a data protection framework.[35] The *GDPR* defines personal data to 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.[36] 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.[37] It is our view that this broad definition takes into consideration many different issues

[30] *Report of the Committee on the Future Economy Pioneers of the Next Generation*, <https://www.gov.sg/~/media/cfe/downloads/cfe%20report.pdf?la=en>.

[31] S Chesterman, *Data Protection Law in Singapore, Privacy and Sovereignty in an Interconnected* (World, Academy Publishing, 2014) 208–218.

[32] *Personal Data Protection Act 2012* (Singapore) s 3.

[33] *Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector Creating for this Purpose a National Privacy Commission and for Other Purposes* <http://www.dict.gov.ph/wp-content/uploads/2014/10/20120815-RA-10173-BSA.pdf>. Section 2 sets the policy direction for data protection and privacy.

[34] *Privacy Act 1988* (Cth).

[35] Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, (20 June 2007) European Commission, Art 29 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

[36] Data Protection Working Party, n 35, Art 4.

[37] Data Protection Working Party, n 35, Art 4.

and scenarios where a person might be identified by or over the internet and computer through its search engines, websites, systems and platforms. In *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority* (*ClientEarth*)[38] the Court of Justice of the European Union ruled that the characterisation as personal data cannot be excluded: (1) by the fact that the information is provided as a part of the professional activity; and (2) by the circumstance that the identity of the experts and the comments were previously made public on the EFSA website; and (3) by the circumstance that the persons concerned do or do not object.[39]

Arguably, this case, while it preceded the *GDPR*, provides a level of guidance as to what the EU consider how a person might be identified over the internet. Furthermore, it provides the basis for the broad definition within the *GDPR* to account for situations as highlighted in the *ClientEarth* case. Moreover, the EU *GDPR* does not apply to non-automated processing of personal data which is not intended to be part of a filing system.[40] The EU in its *GDPR* has responded to these rapid technological developments by seeking to protect personal data of "natural" persons processed by "automated means", including online identifiers such as internet protocol (IP) addresses and cookie identifiers that create profiles on individuals and identify them.[41] These basic concepts are also not new and were commonly found in a passports and other identity documents issued by states.

Indonesia's existing regulations have adopted a broad approach and define personal data as individual data that is stored, maintained and kept for correctness[42] and protected for confidentiality.[43] That is, defining *personal information* has been outlined in both *Government Regulation 82/2012*[44] and *MCI Regulation 20/2016*.[45] Article 1 of *Regulation 20/2016* defines personal data as individual data that is stored, maintained and kept for correctness and protected for confidentiality.[46] Additionally, the "particular individual data" means any correct and actual information that relates to any individual and is identifiable directly or indirectly to be changed under the laws and regulations. This definition could be either viewed restrictively or very broadly, and could include those other elements of personal data that other countries have defined as sensitive personal data.[47]

The Cybersecurity laws of China[48] identify personal information broadly, as all kinds of information, recorded electronically or through other means that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural person's full name, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth.[49] An important point to note from this definition is the broad use of the term biometric, as it does not specify what constitutes biometric data or information, in a similar way to the EU, Australia and Singapore. Furthermore, the term "so forth" could be interpreted in a number of different ways, and taking such an approach, it can be argued that this allows for any other data and information that can identify a data subject. Therefore, in a mediation or dispute resolution procedure,

[38] *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority* (Case C-615/13, 16 July 2015) [29-30].

[39] *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority* (Case C-615/13, 16 July 2015) [29-30].

[40] *General Data Protection Regulation 2016/679*, Art 2.

[41] *General Data Protection Regulation 2016/679*, Art 2.

[42] *Electronic Information and Transaction 20/2016*.

[43] Implementation of the Electronic System and Transaction 82/2012.

[44] Implementation of the Electronic System and Transaction 82/2012.

[45] *Electronic Information and Transaction 11/2008*.

[46] *MCI Regulation 20/2016*, Art 1.

[47] H Harkrisnowo, H Juwana and Y Oppusunggu, *Law and Justice in a Globalized World* (World Editors Faculty of Law, Universitas Indonesia, 2016).

[48] *Cybersecurity Law of the People's Republic of China*, n 25.

[49] *Cybersecurity Law of the People's Republic of China*, n 25, Art 76(5).

the practitioner may need to seek further clarification on and of these terms, because they have, arguably, been established to account for the sovereign needs of China.

In the Philippines personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[50] This definition arguably is the broadest of the jurisdictions examined. It could include just about any personal information/data that can identify a person over the internet such as IP addresses, web browser history, including the standard name, date of birth and residential address.

B. Sensitive Personal Information

The categorisation of sensitive personal data has in our view been determined to place a higher level of control over that data. Some jurisdictions have specifically accounted for this data within their legislation while others have retained this data within the category of general data.

The starting point is the fact that some data is perceived as being more sensitive than other data.[51] Sensitive personal data is distinguished from other personal data that is deemed to be less private.[52] Furthermore, sensitivity personal data is in our view one of the most important factors in determining an individual's perception of privacy. On the one side, the gradation of sensitivity could decide the security level that controls access to such data.[53] On the other side hand, the loss of sensitive data is a significant concern for individuals whose sensitive personal data may be at risk of or has been disclosed.[54] The idea of sensitive personal data is, today, considered as the core[55] of both privacy and data protection law and requires stricter protection in legislation. Australia and the Philippines are the only jurisdictions to have specified what constitutes sensitive personal data.[56]

The Philippine laws define sensitive personal data as "personal information" pertaining to a person's race, ethnic origin, marital status, and religious philosophical or political affiliations, in addition to an individual's health, education, sexual life or to any proceeding of any offence committed or alleged to have been committed by such person, the disposal of such proceedings or the sentence of any court proceedings.[57] This is an interesting addition to sensitive personal information by the Philippines, as no other state or the EU either preclude it or include such information into their respective laws. The extensive approach taken by the Philippines also includes that information issued by government agencies such as social security numbers, health records, licences or its denials, suspension or revocation and tax returns all constitute sensitive personal information. The question arises – does health information constitute biometric data? This is not clear. While the other states and the EU have included most of these specific areas, they do not specify an act or executive order of Congress to be kept confidential. The ability for

[50] *Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector Creating for this Purpose a National Privacy Commission and for Other Purposes* <http://www.dict.gov.ph/wp-content/uploads/2014/10/20120815-RA-10173-BSA.pdf>.

[51] A Etzioni, "A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational" (2015) 80(4) *Brooklyn Law Review* 1263; DT Pesciotta, "I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century" (2012) 63 *Case Western Reserve Law Review* 187.

[52] M Taddicken, "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-disclosure" (2014) 19(2) *Journal of Computer-Mediated Communication* 270.

[53] S Al-Fedaghi, *How Sensitive is Your Personal Information?*, Proceedings of the 2007 ACM Symposium on Applied Computing (2007) 165–169.

[54] C Photopoulos, *Managing Catastrophic Loss of Sensitive Data: A Guide for IT and Security Professionals* (Syngress, 2011) 3.

[55] T Ojanen, "Privacy is More Than Just a Seven-letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others" (2014) 10(3) *European Constitutional Law Review* 528.

[56] *Privacy Act 1988* (Cth) s 6.

[57] *Data Privacy Act 2012* (Philippines).

the Philippines to specify further information by this means, allows for potentially a broader approach to the other jurisdictions. This is something a mediation practitioner will need to be aware of.

Nonetheless, and while Singapore, China, Indonesia and the EU have generally grouped sensitive and personal data together, within the general definition, there are many similarities. However, at issue, is where states use broad terms, and others define specifics, the practitioner will need to understand whether the meaning of biometrics covers the same issues from state to state. For example, biometrics can include, but are not limited to facial, iris, finger prints and DNA scanning and data. Even so, at a glance it appears that most states would cover these specific terms under biometrics generally, at this stage, Indonesia is a stand out that does not.

Notwithstanding the above, the definition of personal data is coupled with consent. The two concepts go hand in hand. However, at issue, is what constitutes consent.

C. Consent (Actual, Implied and Withdrawal)

Consent, along with the definition of personal data, is considered the other cornerstone of data protection and privacy law. Consent in Australia[58] is conceived broadly. The 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 authorised by law. The APPs define consent as "express consent or implied consent".[59] The four key elements of 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. Consent is implied in Australia when it is reasonably inferred from the conduct of the individual and the APP entity.[60] However, it is not implied if an individual's intent is ambiguous, or if there is reasonable doubt about the individual's intention.

Throughout the EU consent encompasses the following elements; consent, performance of the contract, compliance with a legal obligation, protecting vital interest, promoting the public interest, and protecting a legitimate interest pursued by the controller.[61] Article 7(4) of the *GDPR* affirms that the consent is not freely given, if it is conditional.[62] Article 6 requires that processing of personal data is lawful only if, and to the extent that, processing is necessary to satisfy one of four criteria.[63] 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.[64] This requirement of informed consent removes some ambiguity about the purpose of that consent by eliminating the complexities surrounding what constitutes an agreement. Recital 32 of the *GDPR* has reinforced this point, which requires consent to be provided by a data subject in a clear affirmative act, so that it can be demonstrated that the consent was freely provided.[65]

---

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

[59] 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.

[60] Office of Australian Information Commissioner <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts>.

[61] *Council Regulation (EU) 2016/679*, Art 6(1)(a).

[62] *Council Regulation (EU) 2016/679*, Art 7.

[63] *Council Regulation (EU) 2016/679*, Art 6.

[64] *Council Regulation (EU) 2016/679*, Art 6(a).

[65] *Council Regulation (EU) 2016/679*, Recital 32 <http://www.privacy-regulation.eu/en/recital-32-GDPR.htm>. 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 Organisation 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.

In Singapore, consent is required for the collection and disclosure of personal data.[66] Section 13 of the *PDPA* prohibits organisations from collecting, using or disclosing an individual's personal data, unless that individual gives, or is deemed to have given, his consent for the collection, use or disclosure of personal data. Deemed consent constitutes implied consent by statute under Singapore statutory law, which arguably extends the scope of statutory consent in Singapore Law.[67] Section 15 of the *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 purpose. Under s 15(1), an individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose, if that individual voluntarily provides the personal data to the organisation for that purpose and if it is reasonable that the individual would do so. According to s 15(2), if an individual gives, or is deemed to have given, consent for disclosure of his/her personal data for a specified purpose, the individual is deemed to consent to the collection of his/her personal data, for that purpose.[68] The data subject must be notified of the purpose for which the data will be collected.

Moreover, consent in Indonesia requires prior consent of the person to whom the personal data applies. The process for obtaining consent by an electronic system provider is through a standard form in Bahasa Indonesia, and agreement sought by the personal data owner.[69] This consists of the type, purpose and details of the personal data owner. Article 9(2) strengthens the position of data owners, as they, upon providing consent, also request that their personal data be treated as confidential. Furthermore, where consent has not been formally provided for the disclosure of personal data, any person who collects this type of data, including an Electronic Systems Provider, must maintain confidentiality. A minor in Indonesia is considered a person under the age of 21 years. There are significant variances between jurisdictions and how they determine who is a minor and who is not. Nonetheless, a minor must have approval from one or both parents.[70] The Consent Standard Form is considered under the Indonesian Civil Code to be an agreement or contract.[71] Under Indonesian law, the Civil Code prevails over all other laws, when it comes to minors. Article 21 requires that consent is obtained before any personal data is displayed or published. This also includes any personal data that is held within an Electronic System that is either displayed, published, transmitted, disseminated, or, accessed by different Electronic System Providers and Users.

Consent is required from the data owner, for that person's personal data to be manipulated for use when that personal data will be displayed or published.[72] The use and manipulation or the changing of personal data can only be undertaken for the purpose for which that data has been collected, processed and analysed. What this means is that personal data collected for health purposes cannot be manipulated and used, without the consent of the person to whom the data pertains commercial purposes related to consumer behaviour.

Rather than the MCI specify consent for the processing of personal data, the EIT states that prior consent from the data subject must be obtained. The EIT does not distinguish between sensitive or general personal data.[73] The data subject must be informed of the purpose to which the data will be processed, and consent can only apply to the scope that the actual processing will entail. In other words, the processing of personal data may be limited to biometrics, so that only that data can be processed under such a

[66] *Personal Data Protection Act 2012* (Singapore) ss 14–17 (*PDPA*). *PDPA* s 14(1) states how an individual gives consent under the *PDPA*.

[67] 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.

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

[69] *Protection of Personal Data in the Electronic System Regulation*, Arts 6, 9.

[70] *Protection of Personal Data in the Electronic System Regulation*, Art 37.

[71] *Indonesian Civil Code*, Art 330.

[72] *Protection of Personal Data in the Electronic System Regulation*, Art 24.

[73] *Electronic Information and Transactions on the Amendment to Law No 11 of 2008*, Arts 27, 28.

consent. Other data, such as health records could not be used, where the data subject has not provided consent. Consent must be in writing, whether electronically, in hard copy or implied.[74]

The ability of data subjects to withdraw their consent to the use and processing of their personal data, further strengthens their control of that data.[75] This needs to be understood by a mediator, in the event that it is raised. The EU, Australia, and Singapore 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* shall 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 the process of withdrawal should be an easy and accessible to the data subject.[76] Once that individual has withdrawn consent, an entity can no longer rely on past consent for any future use or disclosure of that individual's personal information.[77] Nevertheless, in practice, withdrawing one's consent is not clear, unless the entity has provided information to the data subject that this is an option open to them. The resulting effect is that the data subject is unlikely to know or understand that this option available. However, there are implications for a data subject wanting to withdraw their consent. For instance, they may not be able to access that service. 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 organisation.

Consent in China has taken a very different road. Rather than specify the actual way in which consent is to be obtained, Arts 22, 41 and 42[78] refer to the provider of the network product or service to which has access to the function of collecting user information, its provider shall obtain consent for the use. Furthermore, network operators shall obtain consent of the persons whose data are gathered, and finally, the network operator must not disclose, tamper with, or destroy personal information that are gathered, and absent the consent of the person whose information was collected must not provide personal information to others. Apart from Art 42 that refers to the word "must" in relation to consent, on the other hand Arts 22 and 41 refer to the word "shall" which arguably provide for a fluid arrangement, whereby consent is not absolute. This would need to be reconciled by the mediation practitioner.

Under Philippine law consent is defined as "consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her.[79] It may also be given on behalf of a data subject by an agent specifically authorised to do so on behalf of the data subject. The definition is a stand-alone definition that is not seen in any of the other laws examined. Moreover, s 12 provides that the processing of personal data can only be undertaken with the consent of the data subject. Section 13 goes onto say the consent must be obtained for the processing of personal or privileged information, but can only be provided for a specific purpose. However, the Philippines neither describe to what extent and how consent fully operates. This ambiguity or lack of clarification is something that would need to be clarified very early on in any mediation processes pertaining to personal data.

Once traded, beyond the first tradable point, it appears that the data subject has no control over that data, and the further the data is traded (eg 2nd, 3rd point and beyond), the data subject would not be expected to know anything of their personal data and its use.[80] In summary, the concept of consent varies greatly. The point at which consent is provided and to what extent and how that first level of consent enables

[74] *Electronic Information and Transactions on the Amendment to Law No 11 of 2008*, Arts 27, 28.

[75] *Electronic Information and Transactions on the Amendment to Law No 11 of 2008*, Arts 27, 28.

[76] *Privacy Act 1988* (Cth) "Australian Privacy Principles Guidelines".

[77] *Privacy Act 1988* (Cth) "Australian Privacy Principles Guidelines".

[78] *Cybersecurity Law of the People's Republic of China*, n 25.

[79] *Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector Creating for this Purpose a National Privacy Commission and for Other Purposes*, s 3(b) <http://www.dict.gov.ph/wp-content/uploads/2014/10/20120815-RA-10173-BSA.pdf>.

[80] L Trakman, R Walters and B Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?* (2019) *International Review of Intellectual Property and Competition Law*, forthcoming.

third parties and beyond is not clear,[81] and will need to be considered in any mediation procedure. Mediators of cross-border disputes need to be familiar with the differences that exist in the domestic laws of counties in the Australasian region and the EU.

D. Privacy Shield and Cross-border Transfer of Personal Data

The international transfer of personal data continues to increase. However, the parameters or controls that have been established to facilitate this cross-border transfer are vast and varied. The EU was the first to establish laws that require an assessment (test) for the transfer of data to third countries.[82] The adequacy decision is complex and involves a proposal from the European commission, an opinion from the European Data Protection Board, approval from EU countries, and the adoption of the decision by European commissioners. To date the "white list", those third countries outside the European Economic Area, only include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States as providing adequate protection. Currently, none of Australia, China, Indonesia, Philippines and Singapore have made the "white list". In resolving cross-border mediation disputes, this is another piece of the jigsaw puzzle that will need to be understood by the practitioner because having recognised equivalency, does not mean that the respective data protection laws being examined will be identical. The importance of the above cannot be underestimated, because controllers and processors have a significant role in facilitating the movement of data.

E. Controllers and Processors

The role of data controller or processor has been defined by relevant jurisdictions. They sit within an organisation and depending on where they are located, these individuals are responsible for collecting, storing, using and disclosing personal data. This section only discusses the EU, Australia, Indonesia and Singaporean approaches. It does not include the Philippines or China. Kathleen Paisley highlights how of all the data protection laws that exist today, the EU *GDPR* places the highest level of obligations on data controllers.[83] Moreover, she notes that this category of persons defined in a manner that includes virtually everyone involved in an arbitration, thereby creating overlapping and potentially conflicting obligations with corresponding liability attaching to each. It is argued that while she is predominantly referring to arbitration, the same can be said toward mediation and the mediator. Briefly looking at the *GDPR* obligations, it applies to: the "processing" of "personal data" in the context of the activities of an establishment of a controller or a processor in the Union, whether or not the processing takes place in the Union; and to the "processing" of "personal data" of data subjects who are in the Union by a controller or processor not established in the Union where the processing relates to the offering of goods or services (whether free or paid for) or the monitoring of behaviour which takes place within the European Union.[84]

Moreover, as noted by Paisley, the *GDPR* makes the data controller accountable for compliance and requires the controller to be able to "demonstrate" compliance.[85] This means keeping records of what decisions were made with respect to the protection of personal data and why, and being able to produce those records if requested. Therefore, a mediator where personal data covered by the *GDPR* may be impacted, and steps will need to be undertaken to ensure that data protection principles are properly respected throughout the mediation process.

The complexity for mediators is to understand the divergent approach. The multi-layered approach taken by the EU has created four core appointments: (1) Data Controller, (2) Joint Controllers, (3) Processor

[81] Trakman, Walters and Zeller, n 80.

[82] *Council Regulation (EU) 2016/679*, Art 45.

[83] Kathleen Paisley, "It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration" (2018) 41(4) *Fordham International Law Journal*.

[84] *Council Regulation (EU) 2016/679*, Art 3.

[85] *Council Regulation (EU) 2016/679*, Arts 5(2), 30.

and (4) Data Protection Officer. However, Australia makes an organisation accountable rather than appoint a particular person to responsible for data protection. Australia does not distinguish between a data controller or data processor. Furthermore, under the laws of Indonesia, there is no legal requirement for a Data Protection Officer to be appointed. Indonesia refers to an Electronic System User (ESU). The ESU is any person, state administrator, or business entity, and the public that uses the benefit of goods, services, facilities, or information that are made available by an Electronic System Provider. Finally, Singapore, being a small island state, only requires an organisation to designate a person to be responsible for the data protection laws. Singapore does not specify the title of the designated individual within an organisation. The issue for mediation is knowing the point of contact within an organisation and whether that point of contact is a formal legal requirement.

The variable obligations and requirement of the law imposing a controller, at a minimum can be best summarised as being confusing, and if the mediator is unaware of these differences, it could pose significant challenges throughout a mediation.

V. Conclusion

Personal data is becoming a key feature of the international economy. Data protection law is being developed at different rates and at different times across the EU, Australia, Singapore, the Philippines, China and Indonesia. The EU have, in our view, led the way and have also had a profound influence on the development of data protection law for the global community. However, at issue is the varied approach taken by states to this area of the law. Mediators resolving cross-border disputes in personal data transactions and other matters, in which personal data forms a part, will need to be skilful in understanding the laws of multiple countries. This is because the mediation process may require the dissemination of information between the parties that contains personal data.

The proposed *SMC* has been prepared to foster international trade, improve access to justice, and increase confidence and certainty across the business community. Arguably, this includes the technology industry that trades in personal data. It aims to assist member states and their respective judiciaries to become more efficient in resolving disputes, especially those of commercial nature, trading in personal data, where parties seek stability and certainty. However, it remains to be seen whether the *SMC* will be approved and signed by the international community so as it can be fully implemented. On the one side, should it be approved, it will provide a valuable tool to resolving cross-border trade disputes in personal data under contracts. On the other side, if not approved, the current issues surrounding mediated settlement agreements and enforcement will continue.