INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Dec 2023
ISSN: 2582-6433

INTERNATIONAL COMMERCE AND DATA PROTECTION: THE SINGAPORE MEDIATION CONVENTION

AUTHORED BY: ISHAAN DEEPAK JOSHI
Institutional Affiliation: MIT-WPU Faculty of Law

Abstract

This article explores the evolving landscape of mediation as a pivotal alternative to traditional dispute resolution methods, particularly in the realm of personal data conflicts. Singapore, at the forefront of advocating for mediation in Southeast Asia, actively contributes to the development of the Singapore Convention, recognizing mediation as an efficacious avenue for resolving data-related issues. In contrast, Indonesia, China, and Australia lack explicit inclusion of mediation or alternative dispute resolution in their data protection legislation. The EU's 2008 Directive on Certain Aspects of Mediation addresses inconsistent legal frameworks, while the UN-approved Model Law on International Commercial Mediation underscores the global need for mediation standards. The Singapore Mediation Convention (SMC) serves as a legal framework, delineating criteria for execution and reflecting court refusal grounds akin to arbitration results. The EU GDPR and Australia's Privacy Act govern personal data, emphasizing consent, while Indonesia and China define personal data within comprehensive legislative frameworks. Sensitive personal data, biometrics, and consent intricacies are discussed across jurisdictions, highlighting nuances in regulatory approaches. The global flow of personal data, governed by diverse regulations, necessitates an understanding of the EU's intricate data transfer mechanisms, including the "white list." The proposed Singapore Mediation Convention (SMC) seeks to streamline global commerce and enhance trust in data exchange practices, presenting an intriguing trajectory for international dispute resolution.

Keywords: Mediation, Personal Data, Data Protection, Singapore Mediation Convention, GDPR

ISSN: 2582-6433

Introduction

Mediation has become an essential alternative to conventional methods of resolving disputes, especially in the field of personal data conflicts, due to the constantly changing landscape of data protection legislation. The Southeast Asian area clearly demonstrates this significant change in thinking, with Singapore playing a leading role in promoting mediation and actively contributing to the advancement of the Singapore Convention.[1] It is worth mentioning that Singapore has a strong legal system, which includes the Personal Data Protection Act 2012. This act specifically acknowledges mediation as a very effective method for addressing issues relating to data. On the other hand, the Philippines takes a similar approach by including alternative dispute resolution within its data privacy laws. Nevertheless, countries such as Indonesia, China, and Australia now do not officially include mediation or alternative dispute resolution methods in their strategies for resolving problems pertaining to personal data.

The differences in regulatory methods between the European Union's General Data Protection Regulation (GDPR) and the data protection regulations of China, Australia, Indonesia, and Singapore become evident as the global community deals with the intricacies of data protection. The General Data Protection Regulation (GDPR), implemented in 2017, is designed to protect individual rights and privacy when it comes to the management of personal data. In contrast, China's Cyber Security Law primarily emphasises cybersecurity and the protection of national sovereignty. In light of this context, this introduction explores the subtleties of data protection laws in different countries, providing insights into the complexities of mediation, consent, and the changing landscape of regulations concerning personal data.

Mediation in Personal Data Conflicts: Insights from Singapore and Southeast Asia

Mediation has surfaced as a substitute for settling legal conflicts, enabling parties to pinpoint contested matters, formulate viewpoints, explore alternatives, and endeavor to achieve a consensus. The confidential method of dispute resolution is highly regarded for its effectiveness in resolving complicated and long-distance legal conflicts, both domestically and internationally.[2]

[1] P De Hert and S Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the lndividual 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).

ISSN: 2582-6433

Nevertheless, when it comes to personal data and data protection regulations, mediation has only lately been acknowledged as a viable choice for resolving disputes. Singapore, a leading advocate for mediation and arbitration in Southeast Asia, has been actively involved in the development of the Singapore Convention. The Personal Data Protection Act 2012 (Singapore) (PDPA) explicitly recognizes mediation as a very effective technique for resolving data-related concerns. Section 27 of the Personal Data Protection Act (PDPA) outlines the authority of the Commission for the settlement of complaints. The Commission has the authority to instruct a complainant or an organization to remedy the individual's complaint in the manner specified by the Commission.
The Philippines has adopted a similar approach to Singapore by implementing alternative dispute resolution as a mechanism for the Commission to settle disputes under data protection legislation. However, none of the countries, namely Indonesia, China, or Australia, explicitly mention alternative dispute resolution or mediation as a method for addressing conflicts related to personal data. The Singapore case offers people and organizations clear and definite guidelines. Other nations may contemplate incorporating comparable measures into their own data protection and privacy legislation.

Navigating Global Enforcement with the Singapore Convention

The exchange of personal data has emerged as a significant economic endeavour, akin to the global trade of tangible products and intangible services. In 2008, the EU addressed the issue of the inconsistent legal framework for enforcing mediated agreements by introducing the Directive on Certain Aspects of Mediation in Civil and Commercial Matters. As stated in the Preamble to Article 6(1), the Directive places restrictions on the enforceability of mediation.[3] This restriction aligns with legal precedent that upholds the notion that arbitration decisions are not enforceable when a contract including an arbitration provision simultaneously includes a choice of law clause. Mediation is often seen as a more efficient and cost-effective alternative to arbitration, even when it comes to enforcing an arbitration ruling. The key factor in mediation is the implementation of methods that are efficient in terms of time and expenses. Otherwise, the agreement reached by the mediating parties, as shown by the mediation settlement agreement, may be jeopardised.

The problem lies in the protracted and safeguarded implementation process of mediation agreements. Within an arbitration agreement, the involved parties mutually agree to choose an

[3] B Zeller and L Trakman, "Mediation and Arbitration -The Process of Enforcement" (2019) 24 Uniform ww Review 449.

ISSN: 2582-6433

arbitration tribunal, which then issues a final decision known as an award. The award is contingent upon the parties' mutual consent to engage in an arbitration procedure and their commitment to accept the final and binding outcome.[4]

The 51st session of UNCITRAL concluded the finalisation of a draft legislative framework for international business mediation in June 2018. The Commission granted approval to the Model Law on International Commercial Mediation and International Settlement Agreements arising from Mediation. This effectively permits parties to enforce their mediated settlement agreements in other legal jurisdictions. The significant ruling follows a lengthy period of three years dedicated to talks and writing, which included contributions from up to 85 nations and 35 non-governmental organisations (NGOs). The approval of the UN General Assembly in December 2018 is still necessary, and its ratification next year by a sufficient number of nations is still pending.

On one side, there is a possibility of reducing the difference in enforceability between arbitral awards and judgements when arbitral awards have a certain advantage. Conversely, there is a need for mediated contracts to be implemented with more effectiveness and efficiency, similar to the enforcement of arbitration rulings. Arts 419 and 5w of the Draft Mediation Convention are significant because they provide provisions for settlement agreements.

Practically speaking, merging issues resolves a number of conflicts, and occasionally certain items may only have received preliminary approval.[5] Therefore, any issues that have initial approval within the agreement will need further explanation and verification when the mediation process is completed.

The Singapore Mediation Convention (SMC) is a legal framework that facilitates the execution of settlement agreements resulting from mediations held in other jurisdictions. The provision states that the mediator might provide evidence to affirm that mediation took place or sign the settlement agreement, as long as the mediation process is well recorded. Article 4(b) of the SMC specifically emphasises the criteria by which a state might reject the execution of arbitration rulings.

[4] On the development of the Singapore Mediation Convention, see The Singapore Mediation Co11ve11tion: An Overview
[5] The Australian Dispute Resolution Research Network, A Trib,ute to Mediation's Grassroots

ISSN: 2582-6433

Articles 5(1) and 5(2) provide the criteria that a state might use to reject the execution of arbitral rulings. If a contracting state seeks relief under Article 4, the remedy may only be denied if that party provides the competent authority with evidence that the party involved in the settlement agreement was incapacitated in some way. For this to apply, the settlement agreement must be legally invalid, ineffective, or impossible to carry out according to the law that both parties agreed to follow, or, if that law is not clear, it must be the law decided by the competent authority of the contracting state where relief is being sought under Article 4.[6]

According to Article 5(1)(b)(ii) of the SMC, relief might be denied if the mediated settlement agreement is not legally binding or conclusive as specified in its contents. Therefore, the parties have the option to reach a preliminary agreement via mediation. However, the party seeking enforcement will also have the additional obstacle of having to show the binding nature of the agreement in principle. The key difference between the SMC and the New York Convention lies in the fact that Article 5(f) of the SMC mandates that the mediator's lack of impartiality or independence not only be present throughout the process but also have a tangible impact on the final result. Unlike the New York Convention, it is not necessary for a party to prove that the circumstances had a significant impact on the judgement.

Ultimately, the suggested SMC mirrors many grounds for a court's refusal to uphold an arbitration result, as outlined in the UNCITRAL Model Law and the New York Convention (NYC). However, the SMC offers the tools necessary to put settlement agreements reached during mediations held in other countries into effect, mirroring the success the New York Convention had in enforcing arbitration awards. Hence, mediation is a viable and recommended approach for resolving international conflicts related to personal data, irrespective of the implementation of the SMC.

Comparative Data Protection Laws: EU, China, Australia, Singapore, Philippines

The European Union (EU) introduced the General Data Protection Regulation (GDPR) 2016/679 in 2017. The purpose of this regulation is to guarantee that the handling of personal data is intended to benefit humanity and uphold all basic rights. In 2017, China introduced the Cyber

[6] Nadja Alexander (ed), "Singapore Convention on Mediation"' on KlmverMediationBlog (24 July 2018)

ISSN: 2582-6433

Security Law, which serves as a comprehensive data privacy standard. Its purpose is to protect cybersecurity, uphold national sovereignty and security, and preserve social and public interests. The Privacy Act 1988 (Cth) of Australia is the main law that governs privacy, personal data, and personal information. The Australian Privacy Principles (APP) are in support of it. The applications (APPS) provide organisations with a governance framework to effectively and openly handle personal data, and they may be enforced. Conversely, Indonesia has just begun implementing regulations for data protection and privacy.[7] The Indonesian Parliament passed Electronic Information and Transactions Law No. 11/2008 (EIT) in 2008, and it was later modified in 2016 by Regulation No. 19 of 2016.

Ensuring the safety and privacy of individuals while their personal data is being handled is a basic entitlement, as explicitly mentioned in Article 8(I) of the Charter of Fundamental Rights of the European Union (the Charter) and Article 16(I) of the Treaty on the Functioning of the European Union (TFEU). The Privacy Amendment (Private Sector) Act 2000 (Cth) expanded the scope of the Privacy Act in December 2000 to include some private sector organisations. This amendment included 10 National Privacy Principles (NPPs) into the Privacy Act.

The Personal Data Protection Act 2012 (PDPA) was implemented in Singapore to establish the baseline requirements for safeguarding personal data across the country. The PDPA acknowledges the equilibrium between safeguarding people's personal data and the need for organisations to gather, use, transmit, or reveal personal data. Like Singapore, the Philippines introduced its data protection legislation in 2012, enacting the Data Privacy Act 2012 (Philippines) (DPA). The regulations have given rise to fundamental ideas and principles in data protection legislation, which play an increasingly crucial role in governing an individual's personal data. These concepts must be taken into account in cross-border mediation and conflict resolution procedures.[8]

Defining Personal Data

An accurate understanding of personal data and information is essential in the context of data protection legislation. Australia and Singapore classify generic personal data as including an individual's complete name, alternative name, birth date, gender, present residence, and driver's

[7] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C364/5.
[8] T Magee, China's Data Privacy Law Came into Effect This May - and It Was Inspired lry GDPR (2018)

ISSN: 2582-6433

licence information. Crucial identifying details include an individual's present and previous employment. Australia lacks a national identity card similar to Singapore. However, persons in Australia are required to possess a tax file number while commencing employment or engaging in company activities, regardless of their age. This figure is only applicable to those who are registered to pay taxes, unlike Singapore, which does not include every individual.

The concept of "personal data" in the European Union has substantial consequences as a result of the emergence of new technologies in the 1970s, which prompted the creation of a framework for safeguarding data.[9] According to the GDPR, personal data is defined as any information that pertains to a specific individual (referred to as the data subject) and can be directly or indirectly linked to them through factors such as their name, identification number, location data, online identifiers, or characteristics that are specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

In the case of Client Earth and Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (Client Earth), the Court of Justice of the European Union determined that the classification of the information as personal data cannot be disregarded: (1) based on the fact that the information is shared as part of the experts' professional duties; (2) considering that the experts' identities and comments were previously disclosed on the EFSA website; and (3) regardless of whether the individuals affected have expressed any objections. This case offers insight into the EU's criteria for identifying individuals online and serves as the foundation for the inclusive definition in the GDPR, which takes into consideration scenarios similar to those presented in the Client Earth case.

The European Union General Data Protection Regulation (EU GDPR) does not have jurisdiction over the manual processing of personal data that is not intended to be included in a structured system for easy retrieval. The EU has taken measures to safeguard the personal data of people processed by automated methods, including online identifiers like IP addresses and cookie identifiers that generate individual profiles and identification. These fundamental principles are not novel and are often included in passports and other official identification papers provided by governments.

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

ISSN: 2582-6433

Indonesia's current legislation takes a comprehensive approach by defining personal data as individual information that is saved, maintained, and preserved for accuracy and safeguarded for secrecy. According to Article 1 of Regulation 20/2016, personal data refers to specific information about individuals that is saved, maintained, and preserved to ensure accuracy and safeguard confidentiality. Additionally, according to applicable laws and regulations, "particular individual data" refers to any precise and current information that relates to an individual and may be associated with that individual either directly or indirectly.[10]

China's cybersecurity legislation defines personal information in a wide manner, including any forms of electronically recorded or otherwise obtained information that may be used, either on its own or in combination with other data, to identify an individual's identity. Nevertheless, the phrase "so forth" has several potential interpretations, permitting the inclusion of any further data and information that might potentially identify an individual.

In the context of the Philippines, personal information encompasses any data, regardless of its physical form, that allows the identification of an individual either directly or with reasonable certainty by the entity in possession of the information. Additionally, personal information may also include data that, when combined with other information, unequivocally identifies an individual.

Safeguarding Sensitive Personal Data: A Global Regulatory Perspective

The classification of sensitive personal data has been established to exert a greater degree of authority over that data. Certain countries have explicitly included this data in their laws, while others have classified it as general data.[11] Sensitive personal data is differentiated from other personal data that is considered less confidential and is seen as a crucial aspect in shaping an individual's impression of privacy. Individuals who have had their sensitive personal data exposed or are in danger of exposure are greatly concerned about the potential loss of this information.

[10] S Chesterman, Data Protection Law in Singapore, Privacy and Sovereignty in an Interconnected (World, Academy Publishing, 2014) 208-218.
[11] Report of the Committee on the Future Economy Pioneers of the Next Generation

ISSN: 2582-6433

The concept of sensitive personal data is seen as the fundamental aspect of both privacy and data protection regulations, necessitating more stringent safeguards. Only Australia and the Philippines have explicitly defined the criteria for sensitive personal data. In accordance with Philippine legislation, sensitive personal data is defined as "personal information" that includes an individual's race, ethnic origin, marital status, religious, philosophical, or political affiliations, as well as their health, education, sexual life, or involvement in any criminal offence, whether committed or alleged, including the outcome of legal proceedings or court sentences.

One must consider if health information may be classified as biometric data. The meaning of this is ambiguous. Although most other states and the European Union have included most of these particular domains, they do not stipulate the need for an act or executive order from Congress to maintain confidentiality.[12] The Philippines' capacity to provide more information through this method enables a possibly more comprehensive approach to other countries.

Although Singapore, China, Indonesia, and the EU often classify sensitive and personal data under a broad definition, there are several commonalities among them. However, the main concern arises when some states use general terminology while others provide particular definitions. In such cases, it is crucial for the practitioner to ascertain if the concept of biometrics encompasses identical matters across different jurisdictions. Biometrics include several forms of identification, such as face, iris, fingerprint, and DNA scans and data. Currently, Indonesia stands out as an exception.

The definition of personal data is intrinsically linked to the notion of permission, which is closely associated with the idea of consent.

Consent and Personal Data: A Cross-Border Perspective

Consent is an essential element of data protection and privacy legislation, in addition to the definition of personal data. In Australia, consent is defined as either "express consent" or "implied consent" and encompasses four essential components: (1) the individual is sufficiently informed prior to granting consent; (2) the individual provides consent willingly; (3) the consent is up-to-date and clearly stated; and (4) the individual possesses the ability to comprehend and express

[12] "H Harkrisnowo, H Juwana and Y Oppusunggu, Law and Justice ina Global/zed World (World Editors Faculty of Law, Universitas Indonesia, 2016).

ISSN: 2582-6433

consent.

In Australia, consent is deemed to exist where it may be properly deduced from the actions of the person and the APP entity. However, it is not suggested if an individual's aim is unclear or there is justifiable uncertainty about the individual's objective.

Within the European Union, consent includes several factors such as agreement, fulfilment of the agreement, adherence to a legal duty, safeguarding essential interests, advancing public interests, and preserving a lawful interest pursued by the controller.[13] According to Article 7(4) of the GDPR, permission is considered not freely given if it is conditioned. Article 6 mandates that the processing of personal data is considered legitimate only if it is essential to fulfil one of four specific requirements.

The General Data Protection Regulation (GDPR) mandates that the data controller must gather data only for a clearly defined, unambiguous, and lawful purpose, sometimes referred to as the purpose restriction. The Organisation for Economic Cooperation and Development (OECD) Guidelines, established in 1980, have a comparable approach to the principle of purpose limitation.[14] However, these guidelines provide more detailed specifications regarding the specific timing at which the purpose of data collection must be specified.

In Singapore, obtaining permission is mandatory for the gathering and sharing of personal information. Section 13 of the Personal Data Protection Act (PDPA) forbids organisations from gathering, using, or revealing an individual's personal information unless that individual explicitly or implicitly grants permission for the gathering, utilisation, or revelation of personal data. Deemed consent in Singapore statutory law refers to implicit permission, potentially broadening the reach of statutory consent under Singapore law.

In Indonesia, the individual to whom the data pertains must provide agreement for the use and manipulation of their personal data. The procedure of acquiring permission entails the use of a

[13] A Etzioni, "A Cyber Age Privacy Doctrine: More Coheren1t, 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.
[14] 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-disclos111re" (2014) 19(2) Journal of Computer-Mediated Communication 270.

ISSN: 2582-6433

standardised document in Bahasa Indonesia, together with the pursuit of an agreement from the individual who owns the personal data. Article 9(2) enhances the rights of data owners by stipulating that their personal data must be handled as secret after they provide their permission. In Indonesia, the Civil Code has precedence over all other laws regarding children. According to Article 21, it is mandatory to seek permission before displaying or publishing any personal data. This encompasses all personal information stored inside an electronic system that is visible, shared, sent, distributed, or retrieved by various electronic system providers and users. Personal data may only be used and controlled for the specific reason for which it was first gathered, processed, and examined. Consequently, the personal data obtained for health-related reasons cannot be altered or used without the explicit permission of the individual to whom the data belongs.

The Electronic Information Protection Act 2012 (Singapore) mandates that obtaining prior agreement from the data subject is necessary, and such consent may only be applicable to the specific extent of the processing involved. Processing of personal data may be restricted to biometrics, only allowing the processing of such data under the Personal Data Protection Act (PDPA). Consent must be explicitly communicated by written means, including electronic or physical documentation, or may be inferred from the circumstances.[15] Data subjects' capacity to revoke their permission for the utilisation and manipulation of their personal data enhances their authority over such data. This requires comprehension by an intermediary in the event that it is brought up.

Data subjects in the EU, Australia, and Singapore have the right to withdraw their permission at any given moment. The procedure for withdrawal should be simple and readily available to the data subject. Once an individual has revoked permission, an organisation is no longer permitted to use or disclose that individual's personal information based on previous consent. Nevertheless, in reality, the process of revoking one's permission is not straightforward unless the organisation has explicitly informed the individual that they have the choice to do so. Withdrawing permission as a data subject might have consequences, such as being denied access to the service. According to Section 16 of the Singapore PDPA, people have the right to withdraw their permission for an organisation to collect, use, or disclose their personal data for any reason, at any time.

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

ISSN: 2582-6433

In China, obtaining permission for the gathering and processing of user information is a multifaceted matter that necessitates the employment of specialised methodologies. In China, the entity offering a network product or service is required to acquire permission for the use of the obtained data, while network operators must seek agreement from the individuals from whom the data is collected. Furthermore, they are prohibited from revealing, altering, or obliterating the gathered personal data and are forbidden from sharing personal information with other parties without the explicit approval of the individual whose information was obtained. In the Philippines, consent is legally defined as the "consent of the data subject," which encompasses any voluntary, explicit, and well-informed expression of intention. This may be provided by an authorised agent acting on behalf of the data subject. Nevertheless, the Philippines lacks clear specifications regarding the scope and functioning of consent, potentially resulting in misunderstandings during mediation procedures concerning personal data.[16]

Once data is traded beyond the first moment of tradeability, the data subject loses control over the data, and further trading may lead to the data subject being unaware of their personal data and its utilisation. The definition of consent exhibits significant variability, and the precise moment at which permission is granted and the degree to which it empowers third parties and beyond remain ambiguous. This aspect must be taken into account in any mediation approach.

Mediators handling cross-border conflicts must possess a comprehensive understanding of the variances in domestic legislation between countries in the Australasian area and the European Union. The classification of sensitive personal data has been established to exert a greater degree of authority over that data. Certain countries have explicitly included this data in their legal framework, while others have classified this data as part of a broader category of general data.[17] Sensitive personal data is differentiated from other personal data that is considered less confidential and is seen as a crucial aspect in shaping an individual's impression of privacy. Individuals who have had their sensitive personal data exposed or are in danger of exposure are greatly concerned about the potential loss of this information.

[16] C Photopoulos, Managing Catastrophic Loss of Sensitive Daira: A Guide for rr and Security Professionals (Syngress, 2011) 3.
[17] 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 Europeam 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.

ISSN: 2582-6433

The concept of sensitive personal data is seen as the fundamental aspect of both privacy and data protection regulations, necessitating more stringent safeguards. Only Australia and the Philippines have explicitly defined the criteria for sensitive personal data. In accordance with Philippine legislation, sensitive personal data is defined as "personal information" that includes details about a person's race, ethnic origin, marital status, religious, philosophical, or political affiliations, as well as information about their health, education, sexual life, or any criminal offences they have been involved in, including the disposal of such proceedings or the outcome of any court sentences.

One may wonder if health information may be classified as biometric data. This statement lacks clarity. Although the other states and the EU have included most of these particular domains, they do not stipulate the need for an act or executive order of Congress to be maintained in secrecy. The Philippines' capacity to provide more information through this method enables a possibly more comprehensive approach to other countries.

Although Singapore, China, Indonesia, and the EU often classify sensitive and personal data under a broad definition, there are several commonalities among them. However, the main concern arises when some states use general terminology while others provide particular definitions. In such cases, it is crucial for the practitioner to ascertain if the concept of biometrics encompasses the same matters across different jurisdictions.[18] Biometrics include several forms of identification methods, such as face recognition, iris scanning, fingerprint analysis, and DNA profiling. Currently, Indonesia stands out as an exception.

The definition of personal data is intrinsically linked to the notion of permission, which is closely associated with the idea of consent itself.

Harmonizing Mediation and Data Protection

The global flow of personal data is growing; however, the regulations and measures governing this transnational transfer are extensive and diverse. The European Union (EU) took the initiative to develop Jaws for data transfer to other countries. This process is complex and requires a proposal from the European Commission, an opinion from the European Data Protection Board,

[18] 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

ISSN: 2582-6433

acceptance from EU member states, and adoption by European Commissioners. The current "white list" comprises the following countries and territories: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United States. At now, Australia, China, Indonesia, the Philippines, and Singapore have not been included on the "white list." It is important to comprehend cross-border mediation issues, since the similarity between them does not guarantee that the data protection laws being analysed will be exactly the same.

Data Controllership: Responsibilities and Challenges

Many nations, including the EU, Australia, Indonesia, and Singapore, determine the duties of a data controller or processor. These personnel have the duty of gathering, retaining, using, and revealing personal data, contingent upon their geographical position. The European Union General Data Protection Regulation (EU GDPR) imposes the most stringent responsibilities on data controllers, resulting in the possibility of multiple and possibly contradictory obligations, each carrying its own responsibility.

This pertains to the handling of personal data in two scenarios: first, when a controller or processor located within the European Union processes personal data as part of their activities; and second, when a controller or processor located outside the European Union processes personal data of individuals who are in the European Union, specifically in relation to offering goods or services or monitoring behaviour within the European Union.[19]

The General Data Protection Regulation (GDPR) mandates that the data controller assumes responsibility for adhering to the regulations and must possess the ability to "demonstrate" their compliance. This entails maintaining comprehensive documentation of the choices taken for the safeguarding of personal data, together with the rationale behind them, and being capable of providing such documentation upon request. A mediator who handles personal data subject to the GDPR must guarantee strict adherence to data protection guidelines throughout the whole mediation process.

Mediators have the challenge of comprehending the distinct strategy used by the EU, which

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

ISSN: 2582-6433

involves four primary designations: data controller, joint controllers, processor, and data protection officer.[20] In Australia, the emphasis is on holding organisations accountable for data protection rather than assigning a specific individual to be responsible for it. On the other hand, Indonesia does not mandate the appointment of a data protection officer. In Singapore, due to its small size, an organisation is merely required to choose a person who would be responsible for ensuring compliance with data protection rules. However, the specific title of this designated individual inside the organisation is not specified. Unfamiliarity with the distinct responsibilities and requirements of the legislation that mandates a controller might provide considerable difficulties for a mediator during a mediation process.

Balancing Privacy and Economic Interests Worldwide

The worldwide economy is increasingly reliant on personal data, leading to the development of data protection regulations at varying rates and timeframes in different nations. The European Union has had a substantial impact on the worldwide advancement of data protection legislation. Mediators handling cross-border conflicts in personal data transactions must possess expertise in comprehending legislation from several countries, since the mediation process may necessitate the exchange of information between parties that includes personal data.

The primary objective of the proposed Singapore Mediation Convention (SMC) is to facilitate global commerce, enhance the availability of legal remedies, and bolster trust within the corporate community, particularly in the technology sector involved in the exchange of personal data. Its objective is to support member nations and their judicial systems in enhancing their effectiveness in resolving disputes, including those related to economic activities involving the exchange of personal data.[21]

Nevertheless, the endorsement and ratification of the SMC by the global community remain ambiguous. If authorised, it would provide a beneficial mechanism for resolving international trade disputes related to personal data inside contracts. However, if not allowed, challenges about mediated settlement agreements and enforcement will persist.

[20] Kathleen Paisley, "It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration" (20 I 8) 41 (4) Fordham /11ternational law Journal.
[21] Dewi, Sinta and Walters, Robert and Trakman, Leon and Zeller, Bruno, The Role of International Mediation in Data Protection and Privacy Law - Can It be Effective? (September 1, 2019). (2019) 30 Australian Dispute Resolution Journal 61, UNSW Law Research Paper No. 19-77.

ISSN: 2582-6433

Concluding Remarks

The contemporaneous legal landscape surrounding data protection conflicts has witnessed the ascendancy of mediation as an indispensable alternative dispute resolution mechanism, notably in the intricate domain of personal data disputes. The Southeast Asian region serves as a pertinent illustration, with Singapore emerging as a vanguard in championing the efficacy of mediation, as exemplified by its proactive role in advancing the Singapore Convention and fortified by a robust legal infrastructure, prominently embodied in the Personal Data Protection Act 2012. Analogously, the Philippines aligns itself with this mediation-centric approach by incorporating alternative dispute resolution mechanisms within its data privacy legislative framework.

Conspicuously, however, a discernible lacuna persists in the regulatory paradigms of countries such as Indonesia, China, and Australia, wherein mediation or alternative dispute resolution methods remain conspicuously absent from their strategies for adjudicating personal data conflicts. This regulatory heterogeneity is further underscored when scrutinizing the contrasting provisions of the European Union's General Data Protection Regulation (GDPR) against the legislative frameworks of China, Australia, Indonesia, and Singapore.

The escalating reliance of the global economy on personal data underscores the imperativeness of robust data protection regulations, necessitating nuanced understanding and deft manoeuvring of diverse legal frameworks. The envisaged Singapore Mediation Convention (SMC) emerges as a pivotal proposal, seeking to streamline international commerce, fortify legal redress mechanisms, and instil confidence in the technology sector's data exchange practices. However, the prospective efficacy of the SMC is contingent upon global endorsement and ratification, thereby constituting a critical juncture in shaping the trajectory of international data-related conflict resolution.

In light of mediation's burgeoning significance, stakeholders and mediators alike are confronted with the imperative to navigate the intricate contours of divergent data protection laws, discerning nuances pertaining to consent, sensitive personal data, and overarching regulatory frameworks. The evolution towards a harmonized approach in cross-border mediation of personal data conflicts remains an ongoing narrative, with initiatives like the SMC wielding the potential to exert seminal influence on the future landscape of international data-related dispute resolution.