The current issue and full text archive of this journal is available at
https://muwafaqat.kuis.edu.my/index.php/journal

A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries

Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN

NAWAL SHOLEHUDDIN
(Corresponding Author)
SURIANOM MISKAM
FARAH MOHD SHAHWAHID
TUAN NURHAFIZA RAJA ABDUL AZIZ
NAQIBAH MANSOR
Faculty of Syariah and Law
Selangor Islamic University (UIS)
Malaysia
nawal@uis.edu.my, surianom@uis.edu.my
farahms@uis.edu.my, tuan.nurhafiza@uis.edu.my
mansornaqibah7@gmail.com

Submitted: 20 December 2023
Revised: 25 April 2024
Accepted: 30 April 2024
E-Published: 30 April 2024

ABSTRACT

Personal data has become susceptible to data breaches following the drastic rise in data processing worldwide. Consequently, data protection issues have been addressed using personal data protection (PDP) laws. The current article compared the PDP regulations in Malaysia, Indonesia, Singapore, and the Philippines by assessing the salient features of every law on PDP components via content analysis. As law enforcement varies based on each nation's requirements and situations, their similarities and differences were highlighted in the research outcome. Findings from this study show that each country is committed to ensure the protection of personal data and does so by using ways that most suit the needs and legal requirements of their respective countries.

Keywords: ASEAN, Data Processing, Laws, Personal Data Protection

ABSTRAK

Data peribadi semakin mudah terdedah kepada pelanggaran data berikutan peningkatan drastik dalam pemprosesan data di seluruh dunia. Isu perlindungan data peribadi telah ditangani dengan pelaksanaan undang-undang perlidungan data peribadi. Artikel ini menganalisis perbandingan undang-undang perlindungan data peribadi di Malaysia, Indonesia, Singapura dan Filipina dengan menilai ciri-ciri unik setiap undang-undang dengan mengguna pakai kaedah analisis kandungan. Memandangkan penguatkuasaan undang-undang berbeza berdasarkan kepada kehendak setiap negara, persamaan dan perbezaan

antara negara-negara ini dibincangkan dalam kajian ini dengan terperinci. Dapatan kajian menunjukkan bahwa setiap negara yang dikaji memandang serius komitmen keperluan perlindungan data peribadi dan menggunakan cara yang paling sesuai mengikut keperluan dan memenuhi syarat-syarat perundangan negara mereka.

Kata Kunci: ASEAN, Pemprosesan Data, Undang-Undang, Perlindungan Data Peribadi

INTRODUCTION

Rapid advancements in information and communication technology have both opportunities and complexities. Individuals in current times actively engage with companies that provide digitised information services (Mangku et al., 2021). Hence, the digital economy is projected to dominate ASEAN by 2025 with a contribution of USD 100 billion to national development (Rosadi, 2018). Third-party organisations often collect users' data without their knowledge. For example, internet users who make online purchases, create email accounts, schedule appointments, pay taxes, and sign contracts are compelled to divulge personal data (Privacy International, 2013) for identity verification. Data leakage occurs when short message service (SMS) credit offers, pictures and videos, credit card details, and private company information are discovered, gathered, exchanged, processed, stored, and sold by organisations as a commodity (Nugroho et al., 2020).

Low-cost technological innovations with optimal service delivery have also benefited the education sector, specifically educational establishments. Nevertheless, wider access to novel learning avenues, online forums, virtual learning environments (VLEs), and mobile technologies posed data security threats (Flores & Ching, 2018). Despite the need to comprehend data privacy to deter information leakage, awareness alone proves inadequate. Individuals must consciously exercise caution by internalising data privacy provisions (Tanate-Lazo & Cabonero, 2021). Users are entitled to keep their data private by determining the need for information gathering and processing, privacy preferences, and the means by which companies manage personal data.

National regulations emphasize data gathering, processing, sharing, archiving, and omission (Ameed & Natgunanathan, 2016). As the first comprehensive personal data protection law in Malaysia, the Personal Data Protection Act (PDPA) 2010 was approved by the Malaysian Parliament. On 14 February 2020, Public Consultation Paper No. 01/2020 - Review of PDPA 2010 (PC01/2020) was released by the Personal Data Protection Commissioner (PDPC) under the Ministry of Communications and Multimedia Malaysia released to gain public feedback on the 22 concerns listed. The PDP Department outlined five concerns as key PDPA modifications. Although the amendments were due to be presented to the Parliament in October 2022, the subsequent dissolution of the Parliament leaves the implementation of these amendments unaddressed (Chia, 2023).

Meanwhile, a new and holistic framework was structured for the Indonesian PDP with the passing of Law No. 27 on 17 October 2022. Data controllers and processors and relevant parties who process personal data are given two years from the enforcement of PDP law or until 17 October 2024 for compliance. All parties involved must adhere to the PDP law regulations post-transition period or risk facing legal action in case of any infractions (Tumbuan & Ngantung, 2022).

The PDPA 2012 (Law No. 26) in Singapore was passed on 15 October 2012 and subsequently amended by the PDPA (Amendment) 2020. This Act includes all physical companies and those registered as corporations that gather, utilise, or divulge personal data in Singapore. Hence, the stipulation denotes an extraterritorial effect. The PDPC in this country has established general, sector-specific, or industry-specific guidelines, which constitute the Singapore data protection policy apart from PDPA. Despite the lack of legal force, these advice-oriented recommendations depict how PDPC potentially interprets the Act. The aforementioned guidelines must be stringently complied with. The Public Sector (Governance) Act and Government Instruction Manual 8 (IM8), which governs the public sector, are exempted from the data protection provisions of the Act. Overall, the rules offer the same data protection level, inquiries, and sanctions as the Act for data security infractions (Bigg, Lee & Cho, 2023).

The Republic Act No. 10173 (R.A. 10173) or the Data Privacy Act (DPA) 2012 was enacted by the Philippines to protect users' personal data in public or private bodies. An independent agency named the National Privacy Commission (NPC) was introduced in 2015 to enforce DPA 2012 and ensure compliance with the right to data privacy and protection (Pitogo & Ching, 2018). Furthermore, the Implementing Rules and Regulations (IRRs) of the DPA 2012 were introduced following the NPC's mandate to implement the DPA 2012 provisions, monitor national compliance with global data protection standards, and efficiently enforce the Act provisions.

METHODOLOGY

This legal research aimed to achieve the research objectives via content analysis. Based on Moore and McCabe (2005), this study type entails classifying empirical data into themes and sub-themes for comparison. Meanwhile, content analysis allows for quantitative data organisation to attain the research objectives. The current work, which gathered materials through library research methods, only selected four ASEAN nations (Malaysia, Indonesia, Singapore, and the Philippines). These four countries were selected as they represent the diversity in the practice of personal data protection in the ASEAN region. While countries like Malaysia and Singapore have introduced personal data protection laws for more than a decade, Philippines and Indonesia represent ASEAN countries who have only recently enacted specific personal data protection laws.

DISCUSSION

The ASEAN nations of Malaysia, Singapore, and the Philippines first introduced PDP laws from 2010 to 2012. Indonesia had considered and drafted the laws at the time, pending the parliamentary process (Sargunaraj, 2020). The Law No. 27 of 2022 involving PDP law was finally passed on 17 October 2022. This sanctioning led to the development of a novel and holistic framework for PDP in Indonesia. In terms of registration, only Malaysia, Indonesia, and the Philippines stipulated the requirements needed to register for data users. Notably, Singapore had no such registration requirements. Registration requirements in the Philippines applied if the process entailed accessing at least 1,000 individuals' sensitive personal details. With regards to assigning a DPO, Singapore and the Philippines highlighted the requirement to appoint a DPO. The EIT laws in Indonesia necessitated data users to provide contact details of the person to be reached by the data owner. No DPO appointment was needed in the Malaysian context requirement.

Obtaining consent from a data subject to process their personal data and the organisational prerequisites to obtain express consent from the individual (pre-data gathering, use, or disclosure) are integral to gathering and processing the prerequisites for data users. Meanwhile, the PDPA in Malaysia necessitates data users to obtain consent from a data subject to process their personal data, excluding when consent is required from those under 18 years old. In this case, the parent, guardian, or individual with parental responsibilities over the data subject provides consent. Personal data processing in Indonesia includes derivation and collection, processing and analysing, storage, correction and updates, display, announcement, transference, dissemination or disclosure, and access to or omission. In Singapore, organisations must obtain express consent from the individual prior to data gathering, use, or disclosure. Collecting and processing personal data in the Philippines requires compliance with a general principle: information must be gathered for specified and legitimate purposes, processed fairly and legally, displayed accurately, held relevant, and be up to date.

Laws that govern personal data transfer overseas are enforced in Malaysia, Indonesia, Singapore, and the Philippines. Data users are not authorised to transfer personal data outside Malaysia, unless allowed by the Minister in the Gazette or the situation comes under the exemptions provided in the Act. Meanwhile, Singaporean companies can transfer personal data overseas if they adhere to the Act and the recipient is legally bound by enforceable laws. The DPA 2012 in the Philippines does not restrict personal data transfer outside the Philippines, while no such regulations exist in Indonesia. Data users in Malaysia, Indonesia, Singapore, and the Philippines are responsible for undertaking practical measures to safeguard their personal data. Specifically, data users in Malaysia are required to develop and implement a security policy.

Meanwhile, counterparts in Indonesia are accountable for keeping their personal data confidential, safeguarding it from misuse, being liable in case of misuse, enforcing an internal regulation on PDP, and leaving an audit trail of the entire electronic system being managed. Companies in Singapore must make reasonable and appropriate

security arrangements to safeguard personal data. In the Philippines, personal information controllers and processors must incorporate security measures for PDP.

Data breach notifications in Malaysia, Indonesia, Singapore, and the Philippines differ significantly. Data breach cases in Malaysia need not be reported to the authorities. Contrarily, the electronic system provider in Indonesia must inform the data owner of a data leakage within 14 days along with the underlying reasons. The PDPC Breach Guide in Singapore necessitates companies to inform the PDPC or affected individuals of large-scale violations that may lead to negative implications. In the Philippines, the NPC and affected data subjects must be notified within 72 hours of a personal data breach. The PDP Regulations 2013 authorises the PDPC of Malaysia to enforce PDP laws.

Meanwhile, the MOCI in Indonesia serves to monitor and regulate PDP in electronic systems. This agency, which is authorised to request data and information from the electronic system operator (data controller or processor) to safeguard protecting personal data, may also impose written warnings, a temporary restriction or suspension of its business activities, and administrative fines on non-adherent parties. In Singapore, the Commission enacts the Act by instructing companies to halt gathering, using, or disclosing personal data in contravention, eliminate such data, provide or deny access to or rectification of personal data, and pay a financial penalty of up to 10% of its yearly turnover. The Filipino NPC is required to receive complaints, conduct investigations, make judgements, grant indemnification, and document the investigation outcomes.

The PDPA relates to electronic marketing activities, such as personal data processing for commercial transactions. In Malaysia, PDPA stipulates that a data subject may require the data user to cease or not begin processing their personal data for direct marketing. The law denotes direct marketing as communication by any means of any advertising or marketing materials that targets specific people, albeit with no specific reference to electronic marketing. Arguably, this connotation involves electronic marketing. The PDP law and GDPR in Indonesia do not specifically addresses electronic marketing. Notwithstanding a legal basis must exist to perform electronic marketing activities. This right to withdraw consent served to enable personal data subjects to avoid incidents of personal data breach following direct marketing practices.

In Singapore, the data protection principles in the Act encompass any marketing activities that entail personal data gathering, utilisation, or disclosure. Companies or individuals intending to participate in any telemarketing activities must adhere to DNC provisions. The NPC in the Philippines issued Joint Administrative Order No. 2022-01 or the Guidelines for Online Businesses Reiterating the Laws and Regulations Applicable to Online Businesses and Consumers. Essentially, the guidelines characterise online sellers', merchants', or e-retailers' responsibilities following DPA 2012.

The four ASEAN nations in this study consider online privacy a key barrier. Although the PDPA in Malaysia does not specifically address digital privacy, e-personal data processing in Malaysia is subject to this Act. Cookies and location data in Indonesia are

not bound by laws and regulations but must be used following current PDP laws if personal data is involved. Singaporean companies are required to adhere to the general data protection obligations under the Act by seeking consent before using cookies. The NPC in the Philippines deems cookies as personal information when integrated with other pieces of information.

In Malaysia, breaching the PDPA and PDP Regulations 2013 are punishable with criminal liabilities of fines, imprisonment, or both. Specific provisions cover the offences and penalty. Directors, CEOs, managers, or other officers demonstrate joint liabilities that are subject to a due diligence defence. Following the Indonesian banking law, any commissioner, director, or employee can be imprisoned for not less than two years (but not more than four years) and fined at least IDR 4 billion (but not more than IDR 8 billion). Singaporeans who violate the Act would be penalised up to 10% of an organisation's yearly turnover. In the Philippines, NPC can issue cease and refrain orders and temporarily or permanently ban personal information processing. However, the agency is not authorised to prosecute violators.

Summarily, Malaysia is one of the ASEAN nations that practically enforces PDPA laws (Sholikhah et al., 2021). Nevertheless, the prevalence of data leakage indicates much room for improvement. Reference can be made to Singapore, which adopts prompt responses, integrity, and problem-solving methods (Ramadhan et al., 2022). High data breach cases in Malaysia should be addressed by notifying relevant authorities and data subjects, not unlike the EU GDPR (Chia, 2023) and the Philippines. Such measures could be incorporated into Malaysian law. As Indonesia remains in the preliminary stages of enacting the law, the Indonesian government has given data controllers and processors and relevant parties who process personal data a period of two years (or until 17 October 2024) to comply with the law.

At last, but not least, the comparative legal analysis between four ASEAN countries i.e. Malaysia, Indonesia, Singapore, and Philippines are summarizing as Table 1 below.

Table 1: Comparative Legal Analysis between Four ASEAN Countries

	Malaysia	Indonesia	Singapore	Philippines
Legislation	Personal Data Protection Act 2010 (PDPA)	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Personal Data Protection Act of 2012	Data Privacy Act of 2012 (DPA of 2012) or Republic Act No. 10173 (R.A. 10173)
National Data Protection Authority	Personal Data Protection Commissioner (PDPC)	Ministry of Communications and Information (MOCI)	Personal Data Protection Commission (Commission)	National Privacy Commission (NPC)

Registration	Registration is necessary for data users in the prescribed sectors of communications, banking and financial institutions, insurance, health, tourism and hospitality, transportation, education, direct selling, services (legal, audit, accountancy, engineering, and architecture), real estate, utilities, pawnbroker, and money lenders.	Data used for public and private purposes must be MOCI-registered.	No registration requirements.	No requirements are needed for data users' registration. Nevertheless, registration is necessary if the processing entails accessing or requiring at least 1,000 individuals' sensitive personal information.
Data Protection Officers	Currently, there is no requirement to appoint a DPO.	No DPO requirements. Regardless, the Electronic Information and Transactions (EIT) Regulations require data users to provide contact details to be contacted by the data owner.	An organisation needs to designate a DPO.	The DPA requires people involved in personal data processing to appoint a DPO.
Collection and Processing	The PDPA necessitates data users to obtain consent from a data subject and process their personal data, excluding where consent is required from counterparts under 18 years old. The consent must be obtained through a form that can	Regarding the PDP law, personal data processing includes obtainment and collection, processing and analysing, storing, correction and updates, displaying, announcing, transferring or transmitting, distributing, disclosure, or providing access, and deletion or removal.	Organisations must obtain express consent from the individual pre-data collection, use, or disclosure, provide a data protection notice, or obtain consent from the individual under the Act. Exclusions entail key interests, matters affecting the public, legitimate interests, business	Personal data collection and processing must comply with the general principle: it must be gathered for specified and legitimate purposes, processed fairly and legally, and kept accurate, relevant, and

	be documented and maintained by the data user. For data users under 18 years old, this consent must be obtained from the parent, guardian, or person with parental responsibility towards the data subject.		asset transactions, and business improvement purposes.	up to date. Inaccurate or incomplete data must be rectified, supplemented, or omitted. Otherwise, their further processing must be restricted. The information must prove adequate in relation to the purposes for which they are collected and processed. The data must only be retained for as long as necessary to fulfill the purposes for which such information was obtained (the establishment, exercise, or defence of legal claims or legitimate business). The data must be retained in a form that permits data subjects' identification for no longer than is necessary (for the purposes for which the information was gathered and processed).

Transfer	Data users are not allowed to transfer personal data outside Malaysia, unless otherwise authorised by the Minister in the Gazette or the situation falls under the exemptions stipulated in the Act.	Cross-border (overseas) data transfer requires collaboration with MOCI and adherence to prevailing laws on cross-border data transfer. Indonesia does not have such regulations.	Organisations can transfer personal data overseas if they comply with the Act and the recipient is legally bound by enforceable obligations to provide similar protection.	The DPA does not restrict personal data transfer outside the Philippines.
Security	Data users are responsible for taking 'practical' measures to safeguard personal data, which entails security policy development and implementation.	Data users must keep their personal data confidential, safeguard it from misuse or being liable in case of misuse, issue an internal regulation on personal data protection, and provide an audit trail of the whole electronic system managed. The data holder is further accountable for having the data centre/server and disaster recovery centre located in Indonesia if the information is used for public purposes.	An organisation must make adequate security arrangements in the circumstances to protect personal data and prevent unauthorised access, collection, use, disclosure, copying, modification, and disposal or similar risks.	Personal information controllers and processors must implement organisational, physical, and technical security measures to safeguard personal data and ensure that any individual acting under their authority has access to the data and does not process it, except when legally required.
Breach Notification	Data breaches were not reported to authorities.	The electronic system provider must inform the data owner within 14 days of a data breach and the reasons underpinning the breach.	The PDPC's Guide to Managing Data Breaches 2.0 (PDPC Breach Guide) requires organisations to notify the PDPC and/or affected individuals of large-scale data breaches (personal data of	The NPC and affected data subjects must be notified within 72 hours of a personal data breach or when there is reasonable belief in its occurrence.

			500 or more individuals) or face significant harm or negative impacts. These requirements resemble those under the PDP (Amendment) Bill 2020 (PDP Bill), which entails a mandatory data breach notification regime.	
Enforcement	The PDPA authorises the PDPC to enact PDP regulations and monitor compliance with their requirements. The PDP Regulations 2013 authorises PDPC to inspect the systems employed to manage personal data. Data users are accountable for rendering the systems accessible to PDPC or any inspection officer at all reasonable times.	The MOCI is currently accountable for monitoring and regulating data protection with regards to personal data in electronic systems and can request data and information from the electronic system operator (data controller/processor), safeguard personal data, and penalise non-complying parties via administrative sanctions: written warnings, temporary restriction/suspension of business activities, and administrative fines.	The Commission enacts the Act by instructing organisations to stop personal data collection, use, or disclosure in contravention, destroy the data gathered in contravention, provide or refuse access to or rectification of personal data, and pay a financial penalty of up to 10% of an organisation's annual turnover (for those with an annual turnover exceeding SGD 10 million or SGD 1 million).	To ensure that the personal information controller complies with DPA 2012 with NPC intervention. It is authorised to receive complaints, launch investigations, assist in or resolve complaints, make judgements, grant indemnification, and generate and publicise reports on the outcome of any investigations conducted.
Electronic Marketing	The PDPA applies to electronic marketing activities, which entail personal data processing for commercial transactions. No	Although PDP law and GDPR do not specifically address electronic marketing, a legal basis must be available to perform electronic marketing	Data protection principles in the Act apply to any marketing activities that involve personal data collection, use, or disclosure.	The NPC and other government bodies issued Joint Administrative Order No. 2022-01 or the

	specific provisions are identified in the PDPA that manages electronic marketing. Notwithstanding, the PDPA details that data subjects may require data users to cease or refrain from processing their personal data for direct marketing. The PDPC may provide data users with a guideline on the digital and electronic marketing mechanism and obtain feedback on a proposed requirement for data users to provide a clear mechanism for data subjects to unsubscribe from digital services.	activities, such as the personal data subject's consent. This right to withdraw consent served to enable personal data subjects to avoid further incidents of personal data breach following direct marketing practices.	Furthermore, any organisation or person that intends to participate in telemarketing activities must adhere to DNC provisions. A person or organisation must first obtain an individual's clear and unambiguous consent to send marketing messages to a Singaporean telephone number. This consent must be in written or other form, not be a condition for supplying goods, services, land, interest, or opportunity, and not be obtained through false or misleading information and deceptive or misleading practices.	Guidelines for Online Businesses Reiterating the Laws and Regulations Applicable to Online Businesses and Consumers in 2022. The guidelines outline online sellers', merchants', or e-retailers' responsibilities under DPA 2012 and seek to ensure privacy protection and transparency, legitimate purpose, and proportionality in data gathering and processing.
Online Privacy	Although PDPA does not specifically address online privacy, any electronic personal data processing in Malaysia is subject to the Act. The PDPC may provide further guidance.	Cookies and location data are not subject to laws and regulations. Nevertheless, they must be used in compliance with prevailing PDP laws if they do contain personal information.	Organisations that intend to engage in any online activity that entails personal data collection, use, or disclosure must adhere to the general data protection obligations under the Act. For example, an organisation that aims to use cookies to collect	The law in the Philippines does not define the term 'cookies' or regulate their use. Regardless, the NPC deems that cookies may allow an individual to be distinguished from others (personal

			personal data collection must obtain consent before use. The Commission has published non-binding guidelines that offer practical tips on securing electronic personal data, building websites, identifying IP addresses, and using cookies.	data) when combined with other pieces of information. In this vein, cookies are considered personal information. The DPA 2012 may be applicable, with data subjects' consent secured pre-collection and processing.
Penalties	Violations of the PDPA and PDP Regulations 2013 are punishable with criminal liabilities of fines, imprisonment, or both. Directors, CEOs, managers, or other officers demonstrate joint liabilities that are subject to a due diligence defence.	According to banking law, bank commissioners, directors, employees, or affiliates who deliberately provide confidential information may be (i) imprisoned for not less than two years but not more than four years and (ii) fined at least IDR 4 billion but not more than IDR 8 billion.	Individuals who violate the Act would pay a financial penalty of up to 10% of an organisation's annual turnover in Singapore (for those with an annual turnover exceeding SGD 10 million or SGD 1 million).	The NPC can issue, cease, and refrain orders and impose a temporary or permanent ban on personal information processing, but is not authorised to prosecute offenders for violating DPA 2012. The Department of Justice is accountable for prosecuting the violations of DPA 2012, which is punishable with criminal sanctions: imprisonment with varying durations and a fine.

Source: (Chia, 2023; Bigg et al., 2023; King Kay, 2022; Tumbuan et al., 2022; Sargunaraj, 2020)

CONCLUSION

The outcomes derived from this research revealed several similarities and differences in terms of legislation. Each nation reflects varying situations and interests that must be seriously considered by its laws. Indonesia has followed the lead of Malaysia, Singapore, and the Philippines given their successful enforcement of and adherence to personal data privacy laws. All four countries prioritise PDP and strive to protect their citizens' personal data via pertinent laws. Nevertheless, legal compliance varies across the sample countries. Although Malaysia is the first among the four nations to enact the PDP law in 2010, Singapore has rapidly advanced by amending the existing law, which was only passed in 2012. Indonesia remains in the early stage of implementing the law given the relative novelty of having specific regulations on PDP. This law is under review in the Philippines to amend the current stipulations.

ACKNOWLEDGMENT

This study is funded by the Skim Geran Penyelidikan Inovasi KUIS 2022 (Geran Penyelidikan Sekunder) (2022/P/GPIK/GPS-001).

REFERENCE

Ameed, M., & Natgunanathan. (2016). *Protection of big data privacy*. IEEE access, 1821-1834.

Bakos, Y, Marotta-Wurgler, F. & Trossen, D.R. (2018). Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts. *Journal of Legal Studies,* 43(1).

Bigg, C., Lee, Y.L. & Cho, J.Q. (2023). *Data Protection Laws of the World: Singapore*. DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=law&c=SG

Chia, J. (2023). *Data Protection Laws of the World: Malaysia*. DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=law&c=MY&c2=

Fadhilah, A.G., Syahirah, M.S., Maizatul Akmar, M.R., Nurulhuda, A.R. & Emir, H.A.S. (2020). An Overview of the Personal Data Protection Act 2010 (PDPA): Problems and Solutions. *Global Business and Management Research: An International Journal,* 12(4), 559-564.

Flores, R. T. G., & Ching, M. R. D. (2018). Philippine SUCs compliance performance on RA 10173: a case study on Bukidnon State University. *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government*, 74-78.

Interpol (2021). *ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from The ASEAN Cybercrime Operations Desk.* Singapore: Napier Road.

Islam, M.T., & Karim, M. T. (2019). A Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia. *Journal of History Department, University of Malaya,* 28(2), 169-186.

Jayanti, C. S. (2022). The Issues of Data Protection Against Leaking of Personal Data in Social Security Health Services (A Comparison Between Indonesia and Other Countries Regulations). *International Journal of Business, Economics and Law*, 26.

Jin, W., Aguja, S. E., & Prudente, M. S. (2019, January). Comparing the differences of using mobile devices for learning between Filipino schools and Chinese schools in the Philippines. *Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning*, 216-220.

Kedzior, M. (2021). The Right to Data Protection and the COVID-19 Pandemic: The European Approach. *ERA Forum*, 533–543.

King Kay, C.B.O. (2022). *Data Protection Laws of the World: Philippines.* DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=law&c=PH&c2=

Krippendorff, K., & Bock, M. A. (2008). *The content analysis reader.* Thousand Oaks, CA: Sage.

Lago, C. (2020). The Biggest Data Breaches in Southeast Asia. *CSO Online* (18 January 2020).

Law, S. (2017). At the crossroads of consumer protection, data protection and private international law: Some remarks on Verein für Konsumenteninformation v Amazon EU. *European Law Review,* 42 (5), 751-766.

Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Wirawan, I. G. M. A. S. (2021). The Personal Data Protection of Internet Users in Indonesia. *Journal of Southwest Jiaotong University*, *56*(1).

Moore, D. S., & McCabe, G. P. (2005). *Introduction to the Practice of Statistics (5th ed.)*. New York, NY: W.H. Freeman & Company.

National Privacy Commission. (2017). *NPC Privacy Toolkit: A Guide for Management & Data Protection Officers*. https://privacy.gov.ph/wp-content/uploads/2022/01/3rdToolkit_0618.pdf

Nugroho, A. A., Winanti, A., & Surahmad, S. (2020). Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding*, *7*(7), 183-189.

Pitogo, V., & Ching, M. (2018). Understanding Philippine national agency's commitment on Data Privacy Act of 2012: A case study perspective. *ACM International Conference Proceeding Series* https://doi.org/10.1145/3234781.3234788.

Presbitero, J. V., & Ching, M. R. D. (2018). Assessing compliance of Philippine state universities to the Data Privacy Act of 2012: The case of Caraga State University. *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government* (pp. 90-94).

Ramadhan, K. R., & Wijaya, C. (2022). The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia. *Technium Soc. Sci. J.*, 36, 18.

Reynaldi, F., & Tifana, N. (2020). *Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi: Sebuah Telaah RUU Perlindungan Data Pribadi.* Universitas Padjajaran Press.

Riyadi, Gliddheo. (2021). *Data Privacy in the Indonesian Personal Data Protection Legislation, Policy Brief, No. 7*, Center for Indonesian Policy Studies (CIPS), Jakarta. https://www.econstor.eu/bitstream/10419/249440/1/CIPS-PB07.pdf

Rosadi, S. (2018). Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia. *Brawijaya Law Journal*, 5(1), 143-157.

Sargunaraj, N. (2020). *Personal Data Protection in ASEAN.* ZICO Law: ASEAN Insiders Series, September 2020.

Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, *2*(2), 95-109.

Sholikhah, V. H., Sejati, N. R. F. F., & Shabitah, D. (2021). Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia. *Indonesian Scholars Scientific Summit Taiwan Proceeding*, *3*, 54-63.

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, 29(4), 1443-1457.

Sureani, N. B. N., Qurni, A. S. B. A., Azman, A. H. B., Othman, M. B. B., & Zahari, H. S. B. (2021). The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *6*(10), 488-495.

Tanate-Lazo, R. J. C., & Cabonero, D. A. (2021). Philippine Data Privacy Law: Is it Implemented in a Private University Library, or Not? *Library Philosophy and Practice*, 1-26.

Tham, Y.M., Tan, I. & Zhang, T. (2014). Singapore. In Raul, L.C. (Ed.), *The Privacy, Data Protection and Cybersecurity Law Review* (pp. 204-218). Encompass Print Solutions, Derbyshire.

Thaher, I. (2022a). Politik Hukum: Perlindungan Data Pribadi pada Aplikasi Peduli Lindungi di Indonesia. *Jurnal Pendidikan Tambusai*, 6(1), 1065–1072.

Thaher, I. (2022b). Legal Politics: Personal Data Protection in Peduli Protect Applications in Indonesia. *Journal Research of Social, Science, Economics, and Management*, 1(8), 1195-1206.

Tumbuan, J. & Ngantung, L.S. (2022). *Data Protection Laws of the World: Indonesia*. DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=law&c=ID&c2=

Yap, M. Y. (19 October 2019). Nearly 45,000 University Malaya login IDs and passwords were leaked by an anonymous hacker. *Mashable SE Asia.* https://sea.mashable.com/article/6978/nearly-45000-university-malaya-login-ids-and-passwords-were-leaked-by-an-anonymous-hacker

Yip, M. (2018). Protecting consumers' personal data in the digital world: Challenges and changes. *Personal Data Protection Digest.* 104-117. Research Collection School of Law. https://ink.library.smu.edu.sg/sol_research/2904

Yunus, R. (17 October 2019). Almost 200% Increase in Data Breach Attacks since 2018. *The Malaysian Reserve*. https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/

Zwitter, A., Gstrein, O. J. (2020). Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection. *Journal of International Humanitarian Action,* 5(4).