AY2022/23 Semester 2

Data Protection Scene in SouthEast Asia

IS4231 Tutorial 1 Group 1

Ivan Tan Jia An	A0200141J
Ibrahim Sharul	A0225864X
Li Hao	A0217205R
H Mohamed Hussain	A0199425R
Haziq Hakim Bin Abdul Rahman	A0216481H

Table of Contents

1. Introduction

The onset of digitalisation and the proliferation of online services has resulted in data becoming a currency. The voluminous data generated is a gold mine being used by companies to analyse their data and even sell it to third parties as a revenue stream. This has come under scrutiny with Data Protection (DP) laws being introduced in many countries, following the strengthening and publicising of the European Union's (EU) General Data Protection Regulation[1] (GDPR) that governs the Collection, Use and Disclosure (CUD) of EU residents.

In Asia, apart from Singapore's Personal Data Protection Act[2] (PDPA), there is a lack of awareness of the various DP regulations specific across countries, which is important for compliance when enabling cross-border data transfer. With a burgeoning economy possessing optimistic growth, especially among South East Asian (SEA) countries[3] and an increasing awareness from consumers regarding the protection of their personal data, it is crucial to examine the laws governing personal data, which is not so commonly known. Specifically, we have chosen to focus on three countries namely, Singapore, Philippines and Indonesia. This report will outline the **varying principles influencing the laws, the difference in laws across countries and the landscape impacting the enforcement of these DP laws**. While privacy is a subset of data protection, for simplification purposes, we do not distinguish between privacy and data protection when referring to the law and are used interchangeably in this report.

2. Principles and Philosophy Governing the Laws

Among the first seeking the protection of the rights of consumer's privacy and protection originates from the Organisation for Economic Co-operation and Development (OECD) Privacy guidelines[4] established in 1980, serving to guide countries in safeguarding the privacy of individuals which each country has adopted the fundamental principles but tailored their law according to their needs, values and goals. Below lists the history and justifications that were used to conceptualise and implement the relevant DP laws of the three countries.

2.1 Singapore

Established in 2012 and administered by the Personal Data Protection Commission (PDPC), Singapore's PDPA is built on the Data Protection Code[5] released in 2002 for voluntary adoption and is now mandatory for all private companies. This follows the exponential growth of Infocomm technologies which can involve the processing of personal data. The law governs the CUD of these data, to alleviate concerns surrounding the misuse of personal data, and to maintain individuals' trust in organisations with the culminating goal of positioning Singapore as a viable trusted e-commerce hub[6]. The Singapore government, having studied DP practices from various jurisdictions worldwide,

chose to adopt a middle-ground approach of balancing between protecting the interests of consumers and enabling businesses to utilise the data responsibly to innovate. This is a unique pragmatic approach that aims to balance between "privacy as a fundamental human right" adopted by the European Union (EU) and a laissez-faire-plus-sectoral-patches approach found in the United States[7].

The government has decided to exempt the public sector from the PDPA but instead be subject to its own data privacy standards, primarily Public Sector Governance Act (PSGA), Instruction Manual 8 (IM8) and other adjacent laws such as the Official Secrets Act (OSA), the Banking Act, the Income Tax Act (ITA) and the Statistics Act. This has been explained to be intentional to enable the government to work as one (best known as the Whole-of-Government approach) to serve its citizens well and the standards are high, if not higher than the PDPA[8].

To simplify compliance among private companies, specifically Small and Medium Enterprises (SMEs) who might lack the budget and expertise to be PDPA compliant, the Singapore Government has decided to avoid stringent enforcement by choosing a vague definition of personal data, providing clauses to get non-explicit consent and reducing the responsibilities and obligations required by data intermediaries (the equivalent of data processors in GDPR). The PDPA has since been updated in 2020, to keep up with the changing landscape, introducing stricter fines for violations, data breach notifications and the introduction of the data portability obligation. While PDPA is the primary DP law in Singapore, these adjacent laws listed below collectively help enable personal data to be better safeguarded by providing a robust cyber security landscape.

Adjacent / Complementary Laws
1. Computer Misuse Act[9] - An act to help with enforcements pertaining to unauthorised access to computer material and other forms of cybercrime and includes a provision when personal data is being used or transmitted for nefarious uses.
2. Electronic Transactions Act[10] - An act to provide regulations on the security and use of electronic records to comply with the UNCITRAL Model Law on Electronic Transferable Records, for a better-regulated digital world
3. Cybersecurity Act[11] - A prescriptive law to enforce concretise taking of measures to prevent, manage and respond to cyber incidents of Critical Information Infrastructure (CII) to safeguard the national security of Singapore.
4. Official Secrets Act[12] - An act concerning unlawful disclosure of official documents and

information, primarily government data

Table 1: Adjacent laws of the PDPA Singapore

It seems highly probable that in the years to come, owing to heightened awareness of consumers and businesses alike, the PDPA might converge to adopt stricter rules employed by the GDPR.

2.2 Philippines

For the Philippines, the Data Privacy Act (DPA) of 2012[13] was the first comprehensive law introduced to regulate the processing of personal information in the country. First introduced in Congress in 2011, it was signed into law on 15 August 2012 and came into effect on 8 September 2012.

The act was motivated by the raised concerns about the potential misuse of personal data due to the increasing use of technology and the internet in the Philippines. Another driving force behind the legislation was the need to align with international privacy standards, such as the GDPR, which sets standards for the processing of personal data. The DPA was drafted with reference to international data privacy standards and other international privacy laws, particularly the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the GDPR and the US Privacy Act[14]. The DPA was enacted to safeguard the fundamental human right of privacy, adopting a similar approach as the EU's GDPR by establishing almost similar guidelines and standards for entities that process personal data, including the collection, use, and disclosure of personal information. It also gives data subjects rights to access, correct, delete or forget their personal data.

The National Privacy Commission (NPC), an independent body, was established in early 2016 under the DPA to administer and enforce the provisions of the act. The NPC is also responsible for ensuring compliance of both the public and private sectors for DP, including investigating complaints and data breaches and imposing penalties for violations. In 2016, the NPC published the Implementing Rules and Regulations for DPA, along with a number of Circulars that support the DPA and adopt international standards and practices in data privacy and protection.

In recent years, parliamentary debates about the DPA in the Philippines have increased and revolve around the issues of implementation, enforcement, and possible amendments of the current DPA to address emerging concerns. In 2017, a hearing on the implementation of the DPA was held by the Philippines Senate. Throughout the hearing, senators expressed doubts about the effectiveness of the law in safeguarding personal information, specifically in light of the biggest government data breach that occurred on 27 March 2016[15]. During the incident, 55 million voters' personal data, containing

names, gender, dates of birth, place of birth, height, weight, marital status, postal addresses and parents' names, were leaked as the entire database of the Commission on Elections (Comelec) was hacked by a group self-named Anonymous Philippines[16]. Apart from it, the senators also questioned the capacity of the NPC in enforcing the law and proposed possible solutions to address its flaws.

In 2019, the 52nd Asia Pacific Privacy Authorities Forum was held by the NPC to discuss the need to strengthen the Data Privacy Act's provisions, specifically in the context of emerging technology trends such as artificial intelligence and the Internet of Things (IoT). They also explored the possibility of new policy directions that would widen the scope and coverage of the law, and provide more support for compliance and enforcement[17].

On the 4th February of 2021, the Committee on Information and Communications Technology in the House of Representatives passed a proposed amendment to the Data Privacy Act[18] (Table 11). In the same year, the NPC plans to improve the accountability and resilience of Personal Information Controllers and Personal Information Processors in data privacy by introducing administrative fines. The NPC also presented its measures for preventing poor handling of citizens' personal data. These measures include the Commission's issuances and guidance for COVID-19 response, and the Kabataang Digital advocacy campaign that promotes a safe online environment for teenagers. In addition, the Commission presented guidelines that prohibit harassment-based debt collection and promote the use of videoconferencing or e-hearing technology, along with the amended Rules of Procedure to streamline complaints processing. In general, these parliamentary debates and forums about the Data Privacy Act in the Philippines demonstrate the country's commitment to protecting its citizens' privacy rights as well as ensuring appropriate use of personal data.

Although the Data Privacy Act of 2012 is the primary law in the Philippines that governs the protection of personal data, there are several other laws in place that complement or are adjacent to the DPA. These laws provide additional regulations and guidance on specific aspects related to data protection.

Adjacent / Complementary Laws
1. Data Privacy Act Implementing Rules and Regulations[19] - This regulation complements the DPA by providing additional guidance on the implementation of the DPA and a detailed framework to ensure compliance with the law.
2. Electronic Commerce Act (Republic Act No. 8792)[20] - This act governs electronic

commercial and non-commercial transactions in the Philippines. It complements the DPA by providing additional provisions on data protection and privacy, such as requiring online merchants to disclose their privacy policies and obtain consent from users before collecting personal data.
3. Cybercrime Prevention Act of 2012 (Republic Act No. 10175)[21] - This act provides a legal framework for the prevention, investigation, suppression and imposition of penalties for cybercrime offences. It complements the DPA by enforcing sanctions for offences such as data interception, hacking, and cyber identity theft, which may also involve the processing and management of personal data.
4. National ID System Act (Republic Act No. 11055)[22] - This act creates a nationwide ID program for all Filipinos and non-native residents, which involves the collection of personal data such as name, biometrics and address. It complements the DPA by providing guidelines on safeguarding personal information collected under the system.
5. Anti-Wiretapping Act of 1965 (Republic Act No. 4200)[23] - This act prohibits and penalises the interception of any private communication by wiretapping or using any other device. It complements the DPA by providing additional protections for the confidentiality of communication, which may encompass personal information.
6. Consumer Act of the Philippines (Republic Act No. 7394)[24] - This act protects consumers from unfair trade practices and provides directives for consumer dealings. It complements the DPA by providing supplementary regulations on consumer privacy, such as requiring businesses to obtain consent from consumers before using their personal information for marketing purposes.

Table 2: Adjacent laws of the DPA Philippines

2.3 Indonesia

The data privacy law in Indonesia is guided by the Constitution of the Republic of Indonesia[25], established in 1945. Article 28G (1) of the Constitution states that "each person shall have the right to the protection of his/her self, family, honour, dignity, and property, and shall have the right to feel secure and free from fear." This interpretation can be extended to the right to privacy, as a right of protection. Below shows the multiple laws mentioning the term personal data over the years. However, the earlier attempts to ensure data protection for consumers were rather disjointed and this prompted Indonesia to ramp up and create a unified data protection law that is in effect since 17 October 2022, known as Law No. 27 Protection of Personal Data (PDPL). The PDPL, a stronger law,

takes precedence over its predecessors when there are conflicts[26]. As a nascent law, the commission overseeing personal data enforcement has not been fully and appropriately set up.

The PDPL is motivated by a combination of economic and ethical reasons. First, the rapid growth of the digital economy and e-commerce in Indonesia requires a clear and consistent legal framework for data protection and governance[27]. Next, there is increasing awareness and demand of data subjects for their rights and control over their personal data, especially in the context of cross-border data transfers and online platforms. Thirdly, the need to harmonise the existing sectoral laws and regulations on data protection, such as the Electronic Information and Transactions Law, the Telecommunications Law, and the Health Law, and to address the gaps and inconsistencies among them. Lastly, the aspiration to align with the international standards and best practices on data protection, such as the General Data Protection Regulation (GDPR) of the European Union, and to enhance the trust and cooperation with other countries and regions on data-related matters[28].

PDP Law is the first comprehensive data protection law in Indonesia that addresses a variety of issues:

- Data controller and data processor obligations
- Data subject rights
- Special categories of data and how they can be processed
- Appointment of data protection officer
- Monetary fines and imprisonment for violating the law

Adjacent / Complementary Laws
1. Electronics Information and Transactions Act (Law No. 11 of 2008)[29] - This law mandated that personal data for 'public services' must be processed and stored only in Indonesia, also known as data localization. Public services are defined as activities or a series of activities for the purpose of fulfilling goods and services needs for every citizen and resident in accordance with the laws and regulations, and/or administrative services provided by public services providers.
2. Government Regulation No. 82 of 2012[30] - Mandates that the storage of data localization is arranged based on the classification of electronic data which is divided into three groups: strategic electronic data, high-risk electronic data and low-risk electronic data. The regulation provides that electronic systems operators (ESOs) that provide public services must establish a local data centre.
3. Amendments to Electronics Information and Transactions Act (Law No. 19 of 2016)[31] -

	Amends Law No. 11. Contains several new provisions that mainly concern law enforcement, sanctions and privacy issues, and clarify the meaning of various terms in the existing data protection laws.
4.	Protection of Personal Data in an Electronic System (Kominfo Regulation No. 20 of 2016)[32] - Establishes consent as the core foundation of data privacy protection under Indonesian data privacy laws. Electronic system users and operators within Indonesia are responsible for adhering to a number of principles when collecting or processing personal data. These include respecting personal data as privacy.
5.	Amendment of Electronic Systems and Transactions Law (Government Regulation No. 80 of 2019)[33] - This act requires e-commerce businesses to obtain a business licence, report taxes, and uphold consumer protection and rights. Foreign businesses will be subject to Indonesian law if they actively engage with Indonesian consumers and meet the criteria on transaction volume, transaction value, or the amount of traffic.
6.	Implementation of Electronic Systems and Transactions (Government Regulation No. 71 of 2019)[34] - This act revokes parts of Government Regulation No. 82. Provides a legal framework for data protection in Indonesia and requires companies to obtain consent from individuals before collecting, processing, or transferring their personal data. It also requires companies to implement appropriate security measures to protect personal data.

Table 3: Adjacent laws of the PDP Indonesia

Overall, unlike Singapore which has chosen to adopt a business-friendly stance, Indonesia and the Philippines strictly aim to safeguard the fundamental right of privacy of its citizens, which can be evidenced by the compliance requirements of the law, as explained in the next section. Analysing the mention of personal data in the multiple laws of Indonesia also reveals the lack of consolidated forward thinking when creating them, especially with their fiasco of first enforcing data localisation but repelling it in future laws. This chaos underscores how being clear in the the goals of having alaw is helpful to ensure legitimacy of that law and can influence how likely it will be followed and enforced.

3. Key Differences in the Laws

3.1 Affected Parties

Country	Singapore	Philippines	Indonesia
Whom it Affects	Any **private company** that deals with personal data in Singapore **Individuals** in a personal capacity are not included	Applies to any **person** or **entity** that is involved in the processing of personal information, both private and public sector. 1. Person or entity is found or established in Philippines 2. Personal information relates to a Philippines resident/citizen 3. Processing is done in Philippines 4. The act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines	Applies to any **person** or **entity** that is involved in the processing of personal information, both private and public sector 1. Person or entity is found or established in Indonesia 2. Personal information relates to a Indonesia resident/citizen

Table 4: Comparison of Affected Parties

The Philippines' and Indonesia's data protection laws are seen to emulate the EU's GDPR in terms of their aim to protect individuals' personal data and their application to both the public and private sectors. However, Singapore's PDPA has decided to omit the public sector from compliance under the PDPA as it has other laws governing it. Additionally, unlike the PDPA, both the DPA and PDPL apply to any individual acting in a personal or domestic capacity, which can be more onerous.

3.2 Key Terminologies

Country	Singapore	Philippines	Indonesia
Personal data	Data, whether true or not, about an individual who can be identified from that data	*R*efers 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.	Data of any person who is identified or can be identified individually or in combination with other information, directly or indirectly through an electronic or non-electronic system.
Sensitive Personal Data	No mention	About an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations; biometric and genetic data, as well as political affiliation; About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; Government issued details but not limited to, social security numbers, previous or current health records, licences or its denials, suspension or revocation, and tax returns; and; Specifically established by executive order or an act of Congress to be kept classified.	**No mention of sensitive data but the following are mentioned separately as crucial to maintain** - Health data - Biometric data - Personal financial data
Data Controller	Uses term Data Organisation	*Personal information controller (PIC)* refers to a person or organisation who controls the collection, holding, processing or use of	Any individual, public entity, or international organisation, acting

	instead	personal information, including a person or organisation who instructs another person or organisation to collect, hold, process, use, transfer or disclose personal information on his or her behalf	individually or jointly to determine the purpose and control of Personal Data processing
Data Processor	Uses term data intermediary with reduced obligations	*Personal information processor (PIP)* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.	Any individual, public entity, or international organisation, acting individually or jointly to process the Personal Data on behalf of the Controller

Table 5: Comparison of Key Terminologies

The Philippines leads in being strict by listing what constitutes personal and sensitive personal data. They require PIPs and PICs to be registered with the commission if they process Sensitive Personal Information of at least 1,000 individuals and the processing is likely to pose a risk to the rights and freedoms of data subjects, particularly for Government contractors[35] [36]. Interestingly, the Philippines has added a clause that allows future forms of data to be classified as sensitive personal data if Congress agrees to it, which is a notable smart move given the quick pace of development in the digital space. Indonesia talks about other kinds of data such as health data but does not categorise it as sensitive data. Meanwhile, Singapore has steered clear of defining any form of sensitive data or even listing the specifics in the law but has chosen to generically define what is personal data in the first place as something that can identify someone. Indonesia and the Philippines adopt similar conventions to GDPR for the data controller and processor but Singapore has used a different terminology (Data Organisation and Data Intermediary), which has reduced obligations, making it easier for organisations to comply[37].

3.3 Penalties

Country	Singapore	Philippines	Indonesia
Fines for	Up to 10% of the	A maximum fine	Individuals can face imprisonment

violations	organisation's annual turnover in Singapore OR $1 million, whichever is higher	of PHP 5 million and imprisonment of up to 6 years.	for up to 6 years and up to IDR 6 billion fine. Corporations only face fines but up to 10 times the amount of individuals and face further penalties such as confiscation of profits, etc.
Fines for severe offences	Not applicable	Not applicable	Not applicable

Table 6: Comparison of Penalties

While the Philippines and Indonesia specify the actual fines, Singapore opts for a percentage system for calculating the fines, similar to GDPR. There exists a glaring difference where Singapore's PDPA applies only for local turnover profits and not its global revenue, most likely to entice big organisations to set up headquarters in Singapore which does not apply to the other countries due to the fixed fines available. Indonesia has fines from the complementary laws that deal with personal data but it was quite messy due to the lack of consolidation of the laws initially, which the PDPL strives to reduce confusion about.

3.4 Consent

Country	Singapore	Philippines	Indonesia
Explicit consent	Yes	Yes, consent shall be evidenced by written, electronic or recorded means. Minors (below 18) cannot validly provide consent, require parental or guardian consent	
Non-explicit consent exists	Yes, deemed consent exists contractual necessity, Under the First and Second schedule, no consent exists	No	

Table 7: Comparison of Consent

Consent, the cornerstone of ensuring privacy, has led to the Philippines and Indonesia emphasising that only explicit consent by consumers is allowed. Singapore has chosen a more liberal approach beyond just explicit consent, allowing for deemed consent through word of mouth and contractual necessity. The first and second schedules of the PDPA also highlights the areas where consent is not

needed, including news activity, legitimate business interest and improvement efforts, as long as risk assessment is duly done. The Philippines has chosen to be more specific, providing exemptions though less than Singapore, when processing personal data in certain situations such as journalistic or research purposes or to aid anti-money laundering efforts.

3.5 Rights

Country	Singapore	Philippines	Indonesia
Right to be forgotten	Not Applicable	Applicable	Applicable under adjacent law (Kominfo Regulation No. 20)
Right to withdraw consent	Applicable	Applicable	Applicable
Right-to-object automatic processing	Not applicable	Applicable	Applicable

Table 8: Comparison of Key Rights

Singapore's PDPA does not include provisions for the right to be forgotten or the right to object to decisions based solely on automated processing. The reasons for this are not explicitly stated in the law, but perhaps due to Singapore's posture on establishing itself as an e-commerce and tech hub. In contrast, the Philippines and Indonesia have a stronger focus on human rights guiding their laws. Indonesia's PDPL does not include a provision for the right to be forgotten, but this right is applicable under an adjacent law (Kominfo Regulation No. 20). Nonetheless, all three countries - Singapore, the Philippines, and Indonesia - have included the right to withdraw consent in their respective data protection laws.

3.6 DPO

Country	Singapore	Philippines	Indonesia
Data Protection Officer (DPO) required	Yes for all organisations , big or small	Required for any person or organisation processing data to	Data controllers and data processors must have a DPO if they: - process personal data for public

		designate a DPO and register with the commission	service purposes - have main operations that involve large-scale, frequent and systematic monitoring of personal data - have main operations that involve large-scale processing of specific personal data or personal data related to criminal activity

Table 9: Comparison of DPO requirement

While all organisations mandate the presence of a DPO, the Philippines requires all DPOs to be registered, likely to streamline processes in a suspected data breach and could help know the DPOs for each company and help to facilitate random compliance checks. Responsibilities wise, they are rather similar to each other but the Philippines seems to provide a rather comprehensive set of requirements to execute regarding ensuring data is protected while Singapore interestingly emphasises how fostering a data protection culture is the onus of the DPO.

3.7 Other articles/sections of interest

Country	Singapore	Philippines	Indonesia
Data Protection Impact Assessment (DPIA)	Not mentioned	Not required, but recommended as a mitigating factor in reducing fines	Required by default
Data Breach Notification	3 Calendar days	72 hours	72 hours
Cookie laws	No	No	No
Do-Not-Call (DNC) Registry	Yes	Similar concept is covered under Consumer Act, allowing marketing calls only between 9 am to 7 pm	No

Table 10: Comparison of other interesting aspects

As expected, Indonesia and the Philippines mention DPIA when implementing new processes and by default, similar to GDPR but only Indonesia makes it mandatory. The Philippines encourages it and serves as a mitigating factor to reduce the severity of fines. The data breach notification timeline is 72

hours for Indonesia and the Philippines similar to GDPR but Singapore adopts an interesting period of 3 calendar days, believed to cater to breaches that occur over the weekend, though it is unclear why 3 days and not 72 hours is adopted.

All 3 countries do not express anything on managing cookies, likely for simplicity purposes and reducing the burden of compliance. Singapore has a dedicated DNC registry to opt out of marketing messages and calls. The Philippines covers something similar under the Consumer Act, only allowing marketing calls from 9 am to 7 pm, an unusual provision perhaps targeted to still allow businesses to promote products and services via call while Indonesia ignores completely.

4. Enforcement and Landscape

4.1 Data Protection Commission and its Reputation

In Singapore, the PDPC helps to promote and enforce personal data protection so as to foster an environment of trust among businesses and consumers, contributing to a vibrant Singapore economy. They administer the PDPA and the DNC registry. The stringency of the PDPA and PDPC's strict fines and decisions imposed from its 230 cases[38] thus far, with the highest metered fair in the Singhealth breach where SingHealth and IHiS were fined a total of $250,000 and $750,000 respectively[39], has led to its reputation as a renowned institution that is determined and strict in ensuring that the personal data is protected reasonably well.

Singapore's PDPC approach is to "maximise the use of facilitation and mediation in seeking a resolution between the complainant and the organisation concerned" as far as possible. Should this not be appropriate, such as a large-scale disclosure of personal data or involving data likely to cause significant harm, PDPC will intervene and investigate[40]. It serves to enhance public awareness of lapses in data protection resulting in breaches this posting on their website the list of cases investigated together with the PDPC's decision, establishing PDPC's role as a trusted regulator. There is a provision called voluntary undertaking under section 48L[41], whereby companies can avoid or reduce fines if they can show a satisfactory remediation plan to rectify the immediate breach and address systemic shortcomings to ensure continued compliance. So far, PDPC has accepted undertakings from 25 companies, even prominent companies such as GrabCar[42]. Regardless, in a severe breach, the PDPC has powers to enter without a warrant provided some conditions are met[43].

The Philippines' NPC is serious about safeguarding the right to privacy of its people. Mandated to administer and implement the DPA, and to monitor and ensure compliance of the country with international standards set for personal data protection, it has done well. The NPC adopts both an

active and passive approach, when necessary investigating and prosecuting violations and non-compliance and places a strong emphasis on voluntary compliance and works with organisations to address any issues or concerns related to their data privacy practices such as using a DPIA. It conducted 895 proactive compliance checks in 2021, including 685 privacy sweeps, leading to 50 notices of documentary submission and 160 warning letters. Its Complaints and Handling Investigation handled 363 complaints, conducted 24 voluntary investigations, addressed 8487 data privacy concerns and even imposed temporary bans on several online lending applications that were found to be violating the Data Privacy Act[44]. Thus far, it has issued 129 decisions, resolutions, and orders and strives to respond to investigations within five working days but it depends on the case severity, complexity and workload of the NPC.

Indonesia, given the nascency of its PDPL, does not have its commission set up as of yet. Currently, the Ministry of Communications and Informatics of the Republic of Indonesia (MOCI) will mostly keep the authority and oversee data privacy matters that are processed electronically according to the laws before PDPL till the new commission is set up. Although there have been many instances of data breaches in Indonesia, we could not find any instances of penalties given out by the MOCI, hinting at the lack of strict penalties imposed. Indonesia has had many alleged data breaches with six major data breaches from 2020 to 2021 alone[45], including on its Covid-19 screening app. It remains to see how strict the new commission might be in enforcing the law. No deadline has been announced for the establishment of the commission but given its transitory period of the law, Oct 2024, it could be perhaps next year.

4.2 Data Protection Scene

To aid the enforcement of their own DP law, we now examine how the landscape in each country enables privacy to be upheld. In Singapore, given that DPO is mandatory for all organisations, awareness is increasingly growing and more courses, even advanced diplomas and certificates in Data Protection Excellence and Operation[46] [47] have been introduced. In fact, the PDPC does not conduct its own training but instead provides a competency framework and links to training providers[48], likely to stimulate the economy. The NPC tries to take a step further by providing its own training programme titled the DPO ACE Programme[62] but seems limited to government agencies and government-controlled corporations. The training courses are outsourced to be executed by organisations internally or to other private entities such as Straits Interactive, whom also provides training to Indonesia and Singapore. Both Singapore and the Philippines do have a vibrant ecosystem of DPOs, hosting their own yearly conferences such as Privacy Awareness Week[49] [50] and Personal Data Protection Week[51], something that we hope Indonesia would have as it would help establishe the

legitimacy of the commission and helps to enhance the DP landscape through increased awareness among its population.

In general, throughout SEA and ASEAN, there is a glaring demand for DPO officers. Indonesia recently estimated a need for 100,000 new DPOs minimally in the next three to five years and is amidst formulating a roadmap[52] to recognise international certifications such as from OCEG and the International Associations of Privacy Professionals (IAPP). While Singapore and the Philippines do not provide statistics on this growing need, likely because it has been about 11 years since the laws were established, currently many of the DPOs are double hatting on top of their current non-DPO role, such as lawyers or being the technical lead, but this is slowly changing to include sole DPO roles due to increased demand need to support DP efforts. The pandemic has also led to more DP job roles posted, due to the accelerated rate of digitalisation[53].

Adopting good DP practices is hard and companies tend to depend on their country's respective commission for guidance or frameworks to follow. In Singapore, the PDPC, on top of advisory guidelines to clarify the obligations of the PDPA, provides two frameworks to benchmark for protecting data well, namely Data Protection Essentials[54] (DPE) which is targeting SMEs primarily and Data Protection TrustMark[55] (DPTM) for all organisations. Voluntary in nature and valid for 3 years, it helps establish good DP practices and be certified for it, proving useful as mitigating factors in event of a Data Breach. It has been marketed more crucially as a symbol of trust in protecting the personal data of consumers, again to increase the competitiveness of Singapore companies when providing services in this global business landscape. The NPC provides only guidelines and advisories [56] [57] [58] [59] on employing DP practices such as a Privacy Management Programme, though are not as robust as Singapore's DPE and DPTM. Nevertheless, what they notably excel in is in awarding companies that employ good data privacy practices[60]. Again, Indonesia lacks such guidelines apart from analysis by private organisations, but we can expect them to release it in due time as the deadline for the transition period nears.

5. Conclusion

This report has analysed the data protection scene in 3 SEA countries, Singapore, the Philippines and Indonesia, namely regarding the philosophy and principles in conceptualising the law, the nuances in the requirements to meet by law and the landscape in each country in terms of the commission's enforcement, awareness and training of DP among consumers and professionals. Such a study is unprecedented and is useful in comprehending how the laws are structured and the societal structures in bolstering a Data Protection centric landscape. Particularly, it is interesting to observe how vastly different the laws can be in various aspects listed in section 3 and how the enforcement is contingent on the commission, its reputation and the resources and incentives it provides to comply with the law. With other ASEAN countries introducing or slated to introduce new DP laws such as Thailand, Vietnam and India[61] and a lack of DPOs, the prospects in this realm are lucrative and worth entering to collectively ensure a safe haven when dealing with personal data. Furthermore, it sparks a question on whether a unified ASEAN DP law is needed and if yes, whether it can be reached, similar to the EU, given the differing principles and interests of the countries, which future research can explore further.

6. Appendix

Proposed Amendment
1. Sensitive personal information has been redefined to include biometric and genetic data, as well as political affiliation, due to their innate sensitivity.
2. The extraterritorial application of the DPA has been clarified, specifying instances when processing personal data of Philippine citizens and residents is concerned.
3. The digital age of consent has been increased to more than 15 years for processing personal information.
4. The performance of a contract has been added as a new lawful basis for processing sensitive personal information.
5. Personal Information Controllers outside of the Philippines can authorise Personal Information Processors in the country to report data breaches to the Commission on their behalf.
6. The criminal penalties under the DPA have been modified, giving the proper courts the option to impose either imprisonment or a fine based on their sound judgement.

Table 11: Proposed Amendments to the DPA in 2021

7. References

1. “Lex - 02016R0679-20160504 - En - EUR-Lex.” EUR, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.
2. “PERSONAL DATA PROTECTION ACT 2012.” Singapore Statutes Online, sso.agc.gov.sg/Act/PDPA2012.
3. “ADB Sees Brighter Outlook for Southeast Asia.” SEADS, seads.adb.org/news/adb-sees-brighter-outlook-southeast-asia.
4. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.
5. “Report On A Model Data Protection Code For The Private Sector.” CommonLII, www.commonlii.org/sg/other/SGLRC/report/R5/5.html.
6. Singapore Parliamentary Debates, Official Report (15 Oct. 2012), Sitting No. 8, Personal Data Protection Bill
7. Simon Chesterman, After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012, [2012] SJLS 391 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2042144
8. Singapore Parliamentary Debates, Official Report (2 Nov. 2020), Sitting No. 11, Personal Data Protection (Amendment) Bill.
9. “COMPUTER MISUSE ACT 1993.” Singapore Statutes Online, sso.agc.gov.sg/Act/CMA1993.
10. “ELECTRONIC TRANSACTIONS ACT 2010.” Singapore Statutes Online, sso.agc.gov.sg/Act/ETA2010.
11. “CYBERSECURITY ACT 2018.” Singapore Statutes Online, sso.agc.gov.sg/Acts-Supp/9-2018/.
12. “OFFICIAL SECRETS ACT 1935.” Singapore Statutes Online, sso.agc.gov.sg/act/osa1935.
13. “Republic Act 10173 – Data Privacy Act of 2012.” National Privacy Commission, 11 Nov. 2021, https://www.privacy.gov.ph/data-privacy-act/#7.

14. “NPC Pushes Adoption of International Data Protection Standards on Security Techniques.” National Privacy Commission, 11 Nov. 2021, www.privacy.gov.ph/2021/08/npc-pushes-adoption-of-international-data-protection-standards-on-security-techniques.

15. Press Release - Drilon, PSA, Dispel Fears of Data Privacy Breach in National ID System. legacy.senate.gov.ph/press_release/2017/1204_drilon1.asp.

16. Lago, Cristina. “The Biggest Data Breaches in Southeast Asia.” CSO Online, 18 Jan. 2020, www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html?page=2.

17. “52nd APPA FORUM OPENS IN CEBU.” National Privacy Commission, 11 Nov. 2021, www.privacy.gov.ph/2019/12/52nd-appa-forum-opens-in-cebu.

18. “A Stronger Data Privacy Law Sought in Proposed Amendments.” National Privacy Commission, 11 Nov. 2021, www.privacy.gov.ph/2021/06/a-stronger-data-privacy-law-sought-in-proposed-amendments.

19. “IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE ‘DATA PRIVACY ACT OF 2012.’” National Privacy Commission, 6 Jan. 2023, www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012.

20. Republic Act No. 8792. lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html.

21. Maryclarevillanueva, View All Posts By. “R.A. No. 10175: The Cybercrime Prevention Act: The Net Commandments.” Philippine Legal Research, 5 Dec. 2021, legalresearchph.com/2021/12/05/r-a-no-10175-the-cybercrime-prevention-act-the-net-commandments/#:~:text=The%20Cybercrime%20Prevention%20Act%20of%202012%20focuses%20on%20the%20pre,%2C%20and%20content%2Drelated%20offenses.

22. “Republic Act No. 11055 | GOVPH.” Official Gazette of the Republic of the Philippines, 6 Aug. 2018, www.officialgazette.gov.ph/2018/08/06/republic-act-no-11055.

23. Republic Act No. 4200. lawphil.net/statutes/repacts/ra1965/ra_4200_1965.html.

24. “Republic Act No. 7394 | GOVPH.” Official Gazette of the Republic of the Philippines, 13 Apr. 1992, www.officialgazette.gov.ph/1992/04/13/republic-act-no-7394-s-1992.

25. The Republic of Indonesia. “Law of the Republic of Indonesia regarding the Constitutional Court.” https://www.mkri.id/public/content/infoumum/regulation/pdf/uud45%20eng.pdf. Accessed 12 April 2023.

26. Soemadipradja & Taher. “Indonesia’s Data Protection Law is now official!” Client Update: Technology, Media & Telecommunications Law - November 2022, 22 September 2022, https://www.soemath.com/public/images/page/download1_485_Client%20Update%20-%20Indonesia%20Data%20Protection%20Law(2).pdf. Accessed 11 April 2023.

27. Tiwari, Sailesh. “Digital Economy in Indonesia.” World Bank, 28 October 2021, https://www.worldbank.org/en/news/infographic/2021/10/28/digital-economy-in-indonesia. Accessed 11 April 2023.

28. SAV, DARIA. “Indonesia Data Protection Law Overview (2021).” Sumsub, 20 July 2021, https://sumsub.com/blog/data-protection-law-indonesia/. Accessed 11 April 2023.

29. “ELECTRONIC INFORMATION AND TRANSACTIONS.” ELECTRONIC INFORMATION AND TRANSACTIONS, 21 April 2008, https://platform.dataguidance.com/sites/default/files/ite_english_-_uu_no_11_of_2008.pdf. Accessed 12 April 2023.

30. “ORGANIZATION OF ELECTRONIC SYSTEM AND TRANSACTION.” 12 October 2012, https://www.dataguidance.com/sites/default/files/ite_implementation_english_-_pp_no_82_of_2012.pdf. Accessed 12 April 2023.

31. “UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [JDIH BPK RI].” Peraturan BPK, 25 November 2016, https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016. Accessed 12 April 2023.

32. THE MINISTER OF COMMUNICATION AND INFORMATICS OF THE REPUBLIC OF INDONESIA. “PROTECTION OF PERSONAL DATA IN AN ELECTRONIC SYSTEM.” 20 July 2016, https://platform.dataguidance.com/sites/default/files/data_privacy_english_-_permenkominfo_no_20_of_2016.pdf. Accessed 12 April 2023.

33. “melampaui batas wilayah negara dengan tujuan.” *PERATURAN PEMERINTAH TENTANG PERDAGANGAN MELALUI SISTEM ELEKTRONIK*, 25 November 2019, https://peraturan.bpk.go.id/Home/Download/117172/PP%20Nomor%2080%20Tahun%202019.pdf. Accessed 12 April 2023.

34. “Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.” *JDIH KEMKOMINFO*, 4 October 2019,

https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019. Accessed 12 April 2023.

35. "Data Protected Philippines: Insights." *Linklaters*, www.linklaters.com/en/insights/data-protected/data-protected---philippines. Accessed 12 April 2023.

36. "Republic Act 10173 – Data Privacy Act of 2012." National Privacy Commission, 11 Nov. 2021, https://www.privacy.gov.ph/data-privacy-act/#24. Accessed 12 April 2023.

37. *Understanding the Role of Data Intermediaries in Data Protection and Retention*. www.pdpc.gov.sg/-/media/Files/PDPC/New_DPO_Connect/feb_16/pdf/DataIntermedieries.pdf. Accessed 12 April 2023.

38. "PDPC: All Commission's Decisions." *Personal Data Protection Commission*, www.pdpc.gov.sg/all-commissions-decisions. Accessed 12 April 2023.

39. *Grounds-of-Decision---SingHealth-IHiS*. www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/grounds-of-decision---tech-mahindra---060417.pdf?la=en. Accessed 12 April 2023.

40. *Guide on Active Enforcement - PDPC*. www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Active-Enforcement/Guide-on-Active-Enforcement-15-Mar-2021.pdf?la=en. Accessed 12 April 2023.

41. "Personal Data Protection Act - Voluntary Undertakings." *Singapore Statutes Online*, sso.agc.gov.sg/Act/PDPA2012#pr48L-. Accessed 12 April 2023.

42. "PDPC: Undertakings." *Personal Data Protection Commission*, www.pdpc.gov.sg/Undertakings. Accessed 12 April 2023.

43. *Advisory Guidelines on Enforcement of the Data Protection Provisions - PDPC*. www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en. Accessed 12 April 2023.

44. "Data Protected Philippines: Insights." Linklaters, www.linklaters.com/en/insights/data-protected/data-protected---philippines. . Accessed 12 April 2023.

45. TEMPO.CO. "6 Major Data Breach Cases in Indonesia in Past 1.5 Years." *Tempo.co*, 3 September 2021,

https://en.tempo.co/read/1501851/6-major-data-breach-cases-in-indonesia-in-past-1-5-years. Accessed 10 April 2023.

46. Advanced Diploma in Data Protection." *Academy.smu.edu.sg*, academy.smu.edu.sg/advanced-diploma-data-protection-4336. Accessed 12 April 2023.

47. "Advanced Certificate in Data Protection Principles." *Academy.smu.edu.sg*, academy.smu.edu.sg/advanced-certificate-data-protection-principles-2031. Accessed 12 April 2023.

48. "PDPC | DPO Competency Framework and Training Roadmap." Personal Data Protection Commission, https://www.pdpc.gov.sg/help-and-resources/2020/03/dpo-competency-framework-and-training-roadmap. Accessed 13 April 2023.

49. National Privacy Commission. "Privacy Awareness Week 2022." PAW 2022, 2022, https://paw2022.privacy.gov.ph/. Accessed 13 April 2023.

50. PDPC. "PDPC | Privacy Awareness Week 2023." Personal Data Protection Commission, 2023, https://www.pdpc.gov.sg/news-and-events/events/2023/01/privacy-awareness-week-2023. Accessed 13 April 2023.

51. "PDPC: Personal Data Protection Week 2023." *Personal Data Protection Commission*, www.pdpc.gov.sg/news-and-events/events/2023/01/personal-data-protection-week-2023.

52. "The New Indonesian Data Protection Law and Implications for ASEAN – Webinar Summary." *Welcome to the Data Protection Excellence (DPEX) Network*, www.dpexnetwork.org/articles/the-new-indonesian-data-protection-law-and-implications-for-asean-webinar-summary.

53. "DPOs Are in Hot Demand! Data Protection Job Trends 2021 Webinar Summary." Welcome to the Data Protection Excellence (DPEX) Network, www.dpexnetwork.org/articles/dpos-are-hot-demand-data-protection-job-trends-2021-webinar-summary.

54. "Data Protection Essentials (DPE)." *Infocomm Media Development Authority*, www.imda.gov.sg/how-we-can-help/data-protection-essentials.

55. "Data Protection Trustmark Certification." *Infocomm Media Development Authority*, www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification.

56. “PRIVACY IMPACT ASSESSMENT.” National Privacy Commission, www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_PIA_0618.pdf.

57. PRIVACY MANAGEMENT PROGRAM. www.privacy.gov.ph/wp-content/files/attachments/ppt/DPOGOV_PMP.pdf.

58. “Implementing Rules and Regulations of Republic Act No. 10173, Also Known as the ‘Data Privacy Act of 2012.’” National Privacy Commission, 6 Jan. 2023, www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/#20.

59. “NPC Advisory No. 2017-01 – Designation of Data Protection Officers.” *National Privacy Commission*, 11 Nov. 2021, www.privacy.gov.ph/advisories/npc-advisory-no-2017-01-designation-data-protection-officers/.

60. “Paw 2022: NPC Awards Outstanding Data Privacy Practices in Public, Private Sectors.” *National Privacy Commission*, 7 June 2022, www.privacy.gov.ph/2022/06/paw-2022-npc-awards-outstanding-data-privacy-practices-in-public-private-sectors/.

61. “More DPOs Needed in the near Future, and Right Now.” *Data Protection Excellence (DPEX) Network*, www.dpexnetwork.org/articles/more-dpos-needed-in-the-near-future-and-right-now.

62. “NPC's Ace Training to Help Gov'T Officials Develop Data Privacy Codes of Conduct.” *National Privacy Commission*, 11 Nov. 2021, www.privacy.gov.ph/2021/05/npcs-ace-training-to-help-govt-officials-develop-data-privacy-codes-of-conduct/.