Department of Trade and Industry **POLICY PAPER***

Working Paper Series PP No. 2021-02

Government Pursuit Towards A Mature Data Privacy Framework

Abstract

The Fourth Industrial Revolution and digitalization have emphasized the growing importance of advances in data collection, processing, and analytics. This, however, has raised concerns over the protection of the privacy of individuals. This paper explores the way forward in advancing a mature data privacy framework to create a clearer compliance environment, reduce barriers to the flow of data and investments, and accord an adequate level of protection for individuals. Specifically, the Philippine data privacy framework is analyzed through the Global System for Mobile Communications (GSMA) Mature Privacy Framework. Through the assessment, this paper recommends the formulation of a national strategy on data privacy, advocating for the participation of other Association of Southeast Asian Nations (ASEAN) member states into the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System, supporting the growth of the local data protection ecosystem, and intensifying public education and training.

Bureau of Trade and Industrial Policy Research (BTIPR) - Department of Trade and Industry
5F HPGV Bldg., 395 Sen Gil Puyat Avenue, Makati City
BTIPR@dti.gov.ph

Working Paper Series PP No. 2021-02

Contents **Page**

I. Introduction 1
II. Data Privacy Considerations 1
- **a. Privacy as a Human Right** 1
- **b. Industrial Policy** 2
- **c. Cost of Compliance** 3
- **d. National Security** 3
- **e. Cross-Border Data Flows** 4

III. Regional Data Privacy Frameworks 5
- **a. APEC Privacy Framework** 5
- **b. ASEAN Privacy Framework** 6

IV. Philippine Privacy Framework 7
V. Recommendations 12
VI. Conclusion 15
References 16

I. Introduction

The Fourth Industrial Revolution and digitalization have given rise to frontier technologies such as artificial intelligence, augmented reality, robotics, and the Internet of Things, emphasizing the significance of harnessing data for industrial development. Traditional industries such as manufacturing and retail as well as those that are emerging like creative and knowledge-based industries are benefiting from advances in data collection, processing, and analytics to gain insights for the provision of improved products and services. These have also led to the creation of a secondary market for data to be monetized, such as targeted advertisements and market research by further processing data beyond their initial purpose.

With the increasing reliance on data collection and analysis for innovation and efficiency, creating an environment of trust through data protection has become paramount. While data protection and data privacy have been used interchangeably in literature, a nuance is provided by the Storage Networking Industry Association (SNIA, n.d.) as it defines data protection as the process of safeguarding important data from corruption, compromise, or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable. Data protection encompasses three (3) broad categories, including: (a) traditional data protection; (b) data security; (d) data privacy.

Traditional data protection covers the replication, restoration, and retention of data, while data security is focused on protecting data from compromise by external attackers and malicious insiders. Data privacy, which is the focus of this paper, is concerned with the proper handling of sensitive data to meet regulatory requirements as well as protecting the confidentiality and immutability of the data. Nonetheless, the existence of some overlaps in approaches and regulations among these categories may be noticed.

This paper looks into data privacy policies as a means to uphold privacy as a fundamental human right and as part of a country's industrial policy. It further explores how to advance a mature data privacy framework to attain these objectives and maximize the benefits to consumers, industries, and government. The rest of the paper is organized as follows: Chapter 2 scans the literature on key considerations in data privacy; Chapter 3 outlines the data privacy frameworks relevant to the Philippines; Chapter 4 delves into the data privacy framework of the Philippines through the lens of the GSMA Mature Privacy Framework; Chapter 5 provides the recommendations stemming from this analysis; and Chapter 6 concludes the entire discussion.

II. Data Privacy Considerations

This section covers some motivations in establishing data privacy regulations, such as upholding the right to privacy and as part of industrial policy. In pursuing these objectives, considerations on the cost of compliance, national security, and cross-border data flows are also discussed.

a. Privacy as a Human Right

Upholding the right to privacy remains to be one of the main reasons for data privacy policies. Privacy as a fundamental human right has been recognized by international treaties and domestic legislations. Most prominently, the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his

privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations, 1948, Art. 12).

Further, the International Covenant on Civil and Political Rights emphasized that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and that "Everyone has the right to the protection of the law against such interference or attacks" (United Nations, 1966, Art. XVII).

For the Philippines, the 1987 Constitution provides the foundation for privacy with the policies of the state and the bill of rights stipulating:

- "The State values the dignity of every human person and guarantees full respect for human rights" (Const., Art. II § 11);
- "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized" (Const., Art. III § 2); and
- "The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law" (Const., Art. III § 3).

This was later emphasized in Republic Act (RA) No. 10173 as it declared "It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth" (Data Privacy Act of 2012, § 2).

Varying privacy regulations across countries may be attributed to the different values each attach to privacy, with regulations tending to be more stringent in jurisdictions where privacy is considered a human right (Casalini & López González, 2019; Pasadilla, 2020).

b. Industrial Policy

Another motivation is in viewing data privacy as part and parcel of industrial policy, which encompasses the strategic effort of governments to encourage and promote specific industries or sectors (White, 2008). Specifically, the development of emerging digital industries and electronic commerce. Building on the phrase "data is the new oil", the World Economic Forum (2018) advances "data as the oxygen that fuels the fire of the Fourth Industrial Revolution."

As revealed in the research by Anant et al. (2020), there is a lack of trust among their consumers in the handling of data and protection of privacy, providing an opportunity for companies to gain a competitive advantage by taking deliberate measures in data protection and privacy. As consumers become increasingly aware and trusting of how their information is being handled and used, a richer set of data is circulated to aid in developing digitally intensive industries.

To balance leveraging on the use of consumer data and addressing consumers' increasing concern in the collection, use, and protection of their personal data, it becomes imperative for the country's industrial strategy to embed responsible data stewardship and governance and ultimately create a conducive environment for data sharing and protection.

This is especially relevant with the rise of e-commerce amidst the Corona Virus Disease 2019 (COVID-19) pandemic ushering industries to depend greatly on data as they accelerate digital adoption and transformation. In building consumer confidence, data protection policies help increase digital payments utilization and e-commerce purchases.

For the Philippines and the DTI, in particular, advancing data privacy benefits its priority sectors, including a robust Information Technology-Business Process Management (IT-BPM) industry that generated revenues amounting to USD26.7 billion in 2020 (Crismundo,2020). This industry is composed of the contact center and voice and non-voice Business Process Outsourcing (BPO), engineering services outsourcing (ESO), animation and game development, medical, financial, and health information management service, global in-house centers, software development, shared services, and IT, among others. Another priority sector of DTI that will greatly gain is a thriving startup ecosystem ranging from financial technology (fintech), electronic commerce (e-commerce), and medical and healthcare technology, with an ecosystem value[1] of USD584 million (Startup Genome, 2021).

c. Cost of Compliance

The most immediate consideration for data privacy regulations is the compliance cost. This includes data protection and enforcement activities, incident response plans, compliance audits and assessments, policy development, communication and training, staff certification, redress activities, and investments in specialized technologies (Ponemon Institute, 2017).

These may be perceived as additional burdens to enterprises and offset the intended benefits of industrial development. As demonstrated in Abraham et al. (2021), the cost of data privacy compliance in certain jurisdictions may be quite significant, incentivizing companies to avoid these jurisdictions or simply ignore the laws. The cost of compliance is found to be especially challenging for micro, small, and medium enterprises (MSMEs) with limited resources.

However, Ponemon Institute (2017) found that the cost of compliance is outweighed by the cost of non-compliance, covering business disruption, productivity loss, revenue loss, fines, and penalties. This highlights the critical role of government in enforcing data privacy regulations while ensuring clear rules with special attention given to MSMEs.

d. National Security

Another consideration is national security, which is defined in the context of the Philippines as "a state or condition wherein the people's welfare, well-being, ways of life; government and its institutions; territorial integrity; sovereignty; and core values are enhanced and protected" (Office of the President, 2017).

[1] *The ecosystem value was computed as the total exit valuation and startup valuations over two-and-a-half years*

Concerns over national security most commonly revolve around sensitive personal information, which "refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
(4) Specifically established by an executive order or an act of Congress to be kept classified" (Data Privacy Act of 2012, § 3).

The processing of sensitive personal information is generally prohibited except when the data subject has given consent or when it is necessary to protect life and health, for purposes of medical treatment, and the protection of lawful rights and interests (Data Privacy Act of 2012, §13).

Concerns over privacy in relation to national security was under the spotlight as Edward J. Snowden, a former contractor of the US National Security Agency (NSA), leaked the NSA's mass surveillance of citizen's communications over the internet, creation of big data centers to gather and store information for analysis, and the Prism Program; which provides detailed search capability on any individual through social media platforms (Jawaid, 2020).

This issue has become more prominent with the occurrence of the large-scale data breach involving Cambridge Analytica, which harvested private information from 50 million Facebook profiles (Cadawalladr & Graham-Harrison, 2018). The Philippines was identified to be the 2nd most affected country in terms of data subjects with 1.2 million users affected (NPC, 2018a).

With these developments, there has been a perceived trade-off between upholding privacy and national security, arguing that the cost of security is giving up the right to privacy (Jawid, 2020).

Further, national security has been used as a justification for localization measures, such as explicit requirements for data to be stored in local servers or processed within the territory of a specific national jurisdiction (Cuevas et al., 2018). Arguments for localizing data are based on threats to national security should data be allowed to flow freely to hostile regimes. On the other hand, the rationale against data localization to promote national security is grounded on data localization as a tool to limit democracy and human rights, restrict collaboration among security actors, and introduce risks and complexities to enterprises' cybersecurity operations (Ramos et al., 2021).

e. Cross-Border Data Flows

Facilitating the free flow of data is now a central feature of economies as it enables enterprises to flourish by being able to operate and access markets, solutions, and support across borders. This is exemplified by the McKinsey Global Institute's (2016)

estimates that the contribution of data flows to world gross domestic product (GDP) has already surpassed the impact of global trade in goods.[2]
However, certain data privacy policies, such as requirements on data localization and restrictions on the transfer of personal information to foreign jurisdictions may increase trade costs and act similar to non-tariff measures.

In addition to the explicit requirements for localization mentioned previously, implicit measures include limits on public procurement of foreign goods and services, requirements on domestic ownership, intellectual property controls, and online censorship (Cuevas et al., 2018).

However, compliance to these localization measures, which restrict data flows has been found to have a significant negative effect on a country's economy due to losses in firm-level productivity, higher prices, lower competitiveness, and lesser investment attractiveness (Bauer et al., 2016; Cory, 2017).

As raised in the APEC Digital Trade Policy Dialogue (DiPaula-Coyle, 2021), data localization does not ensure data protection, which is dependent on the manner and process of data storage and not on the location. Further, interventions that will more effectively protect data require advanced cybersecurity technology, encryption, monitoring and intrusion detection, access authorization, security procedures, and user education.

Given the detrimental effects of certain data privacy measures, upholding data privacy must be pursued with consideration of its potential effect on cross-border flows of data. This may be achieved through regional efforts towards harmonization underpinned by national level initiatives to establish a mature data privacy framework.

III. Regional Data Privacy Frameworks

Regulatory frameworks for data privacy provide the foundation in maintaining an adequate level of protection while upholding privacy as a human right and/or as part of its industrial policy. For the Philippines, the two (2) main privacy frameworks it abides by are the APEC Privacy Framework and the ASEAN Framework on Personal Data Protection.

a. APEC Privacy Framework

The APEC Privacy Framework, which had its first and second iterations published in 2004 and 2015, respectively, recognizes the role of a framework to protect privacy in industrial development as it states "APEC member economies realize the enormous potential of the digital economy to continue to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce" (APEC, 2015, p.2).

It further sustains that "the Framework specifically addresses the importance of protecting privacy while maintaining information flows" (APEC, 2015, p.3). The APEC Privacy Framework does this through the establishment of a voluntary accountability

[2] *Cross-border data flows were estimated to have contributed USD2.8 trillion in 2014, higher than the contribution of trade in goods at USD2.7 trillion*

mechanism for protecting personal data privacy, the APEC CBPR System and Privacy Recognition for Processors (PRP) System. These are APEC member economy/government-backed data privacy certification systems that companies can join to demonstrate compliance with internationally-recognized data privacy protection. These provide a means for organizations to transfer personal information across borders in a manner that protects privacy.

The CBPR System focuses on data controllers defined as those who determine the purpose and means of processing data, whereas the PRP System deals with data processors or those who simply process data on behalf of the controllers, such as telecommunications and logistics providers and data management companies.

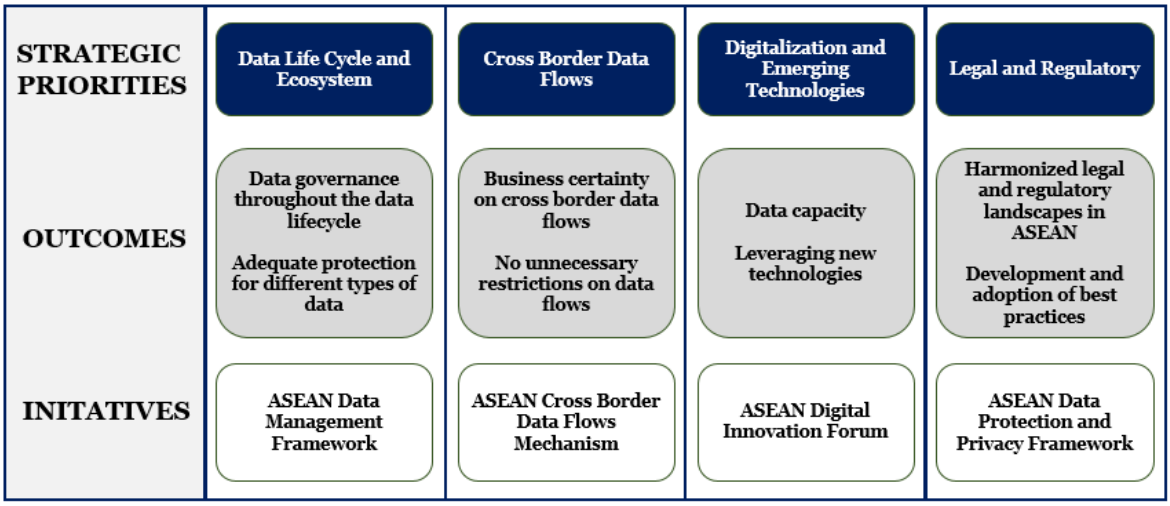
b. ASEAN Privacy Framework

The ASEAN Framework on Personal Data Protection emanated from the ASEAN Economic Community (AEC) Blueprint 2025[3] and the ASEAN Information and Communications Technology (ICT) Masterplan 2020[4], which called for the development of a comprehensive personal data protection framework in the ASEAN region.

Based on the published documents, the ASEAN Framework on Personal Data Protection also emphasizes the role of data privacy protection in industrial development with the objective "to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information" (ASEAN, 2016, p.2), while "Recognising the different levels of development of the Participants" (ASEAN, 2016, p.6). Through this, the ASEAN solidified its commitment towards a secure, sustainable, and transformative digitally-enabled economic community.

This is complemented by the ASEAN Framework on Digital Data Governance published in 2018, with four (4) strategic priorities and their respective outcomes listed in Figure 1.

Figure 1. ASEAN Framework on Digital Data Governance



Source: ASEAN (2021)

[3] *Adopted by the ASEAN leaders at the 27th ASEAN Summit on 22 November 2015*
[4] *Approved by the 15th ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN) on 27 November 2015*

Under its strategic priority of data life cycle and ecosystem is the initiative of the ASEAN Data Management Framework (DMF) while under cross-border data flows is the initiative of the ASEAN Cross Border Data Flows (CBDF) Mechanism.

In pursuing these initiatives, the ASEAN adopted the ASEAN DMF and ASEAN Model Contractual Clauses (MCCs). The ASEAN DMF offers guidance for businesses to put in place an effective system to manage data throughout its lifecycle while the ASEAN MCCs are voluntary standards based on best practices and fundamental privacy principles. The ASEAN MCCs set out contractual terms and conditions that may be implemented by enterprises as a legal basis for cross-border data transfers.

IV. Philippine Privacy Framework

This section examines the data privacy framework of the Philippines through the GSMA Mature Privacy Framework (2018), which identifies the essential elements of a mature data privacy regime, including (a) data protection law/s, (b) implementation guidelines, (c) an enforcement authority, (d) public-private consultation, (e) guidelines or rules on cross-border data flow, (f) training, (g) public education, (h) multilateral and bilateral engagement, (i) coordination mechanism for government agencies, (j) self-regulation, and (k) a national strategy.

The GSMA categorizes a country' data privacy framework as (a) nascent, (b) progressing, or (c) advanced depending on whether the country has some, most, or all of the components.

A mature data privacy framework at the advanced stage creates a clearer compliance environment for businesses that seek to operate in a specific jurisdiction, reduces barriers to the flow of data and investments, and accords an adequate level of protection for individuals. Moreover, this provides a solid foundation for harmonization with regional frameworks.

Data Privacy Law

Most of the identified elements of a mature privacy framework have already been established in the Philippines beginning with the development and application of legislation through the enactment of its data protection law, Republic Act (RA) No. 10173 or the Data Privacy Act of 2012. As previously discussed, this law emphasizes the citizens' fundamental human right to privacy.

Implementing Rules and Regulations

The official guidelines for how the privacy law will take effect, including the timelines, definitions, and regulatory interpretations were achieved through the promulgation of the Data Privacy Act of 2012's implementing rules and regulations (IRR) in 2016. Both the DPA and its IRR are based on and consistent with the international frameworks discussed in the previous section.

Enforcement Authority

Through the Data Privacy Act of 2012, the National Privacy Commission (NPC) was established serving as the country’s enforcement authority; mandated to carry out the

provisions of the law and monitor and ensure compliance with international data protection standards. The NPC has been accredited as a member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), a premier global forum for data protection authorities, recognizing that the NPC has met the stringent standards for protecting personal data and privacy (NPC, 2015).

Guidelines on Cross Border Data Flows

The voluntary and/or mandatory rules governing the transfer of data across national borders are also covered by the Data Privacy Act of 2012. Subject to the application of other regulations for financial and government data, the law does not prohibit the transfer of personal information across borders and does not implement data localization measures. Part of the mandate of the NPC is to perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection and negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of their respective privacy laws.

To further facilitate cross-border data flows, the NPC released Advisory No. 2021-02 or the Guidance for the Use of the ASEAN MCCs and ASEAN DMF. This provides additional guidance to local personal information processors and controllers.

In addition, the NPC has launched the Philippine Privacy Trust Mark (PPTM) in November 2021 to increase trust and confidence in businesses and public offices. Certified organizations that have met the requirements and have completed the process are determined to have the highest level of assurance on data privacy compliance and secure cross-border data transfers (NPC, 2021d).

Public-Private Consultation

Formal and informal dialogues among stakeholders in government, the private sector, and civil society have been done by the NPC as it actively consulted with and engaged stakeholders from the formulation of the IRR of the Data Privacy Act of 2012 to its involvement in committees and working groups on issues and developments that require scrutiny through a privacy lens (NPC 2016a; 2016b). This includes the conduct of Data Privacy Council assemblies that employs a multi-stakeholder-based approach in promoting data privacy accountability across all sectors.

Training

The NPC has also conducted capacity-building programs, such as the Data Protection Officer (DPO) experiential compliance workshop (COMPLex) for government appointed DPOs (NPC, 2019d); the Health Sector Forum to improve privacy and protection protocols (NPC, 2020c); and the DPO Accountability, Compliance, and Ethics (ACE) Program aimed at establishing a skills benchmark for local privacy professionals (NPC, 2018b).

Public Education

Campaigns to inform the public about privacy risks, rules, and compliance by the NPC include the Privacy, Kabataang Digital (KD) Campaign under its banner Safety, Security, and Trust Online (PSST!) advocacy campaign (NPC, 2021e); the dissemination of the NPC Privacy Toolkit serving as the official handbook of data privacy professionals in the

public and private sector (NPC, 2018c); and the release of the online learning guidelines amidst the COVID-19 pandemic (NPC, 2020b).

Multilateral and Bilateral Engagement

The Philippines has sought deeper partnerships to exchange best practices in data governance beyond its engagement in international bodies as it signed a memorandum of understanding with Singapore's Personal Data Protection Commission in 2019 and with the United Kingdom's Information Commissioner's Office in 2021 (NPC, 2019b; 2021a). As a testament to the progress of the country's privacy regime, the NPC has also been appointed as the chair of the Global Privacy Assembly's COVID-19 Taskforce, which was formed to drive practical responses to privacy issues emerging from the pandemic (NPC, 2020a).

Coordination Mechanism for Government Agencies

The NPC also coordinates with other government agencies and ensures that data privacy concerns are given attention as a resource agency for the Task Force on Big Data and member of the Joint Cybersecurity Working Group. Moreover, the NPC has been involved in the Subcommittee on IT for learning, education, and training; Technical Committee on IT; and technical working group on National Security Issues on Government-Issued Documents (NPC, 2018d; 2019a).

Self-Regulation

While the country did not introduce its own self- regulatory mechanism, the Philippines has formally joined the APEC CBPR System in 2019, becoming the 9th economy to join the system (NPC, 2019c).[5] This serves the intention of certifying local companies, including MSMES, as CBPR-compliant through APEC-recognized Accountability Agents to gain a seal of privacy compliance and accountability. The NPC has called for the applications of local Accountability Agents, which will certify the compliance of companies' privacy policies and practices with the APEC CBPR System, from 15 October 2021 to 29 November 2021 (NPC, 2021c).

As summarized in Figure 2, the Philippines has most of the elements of a Mature Privacy Framework identified by the GSMA. With this, the country's data privacy framework is categorized at the progressing stage.

The only missing element in the country's privacy framework is the national strategy that sets the goals and provides for a coordinated approach across government agencies, initiatives, and compatibility with related policies.

[5] Other participating economies are the US, Mexico, Japan, Canada, Republic of Korea, Australia, Singapore, and Taiwan.

Figure 2. Elements of a Mature Privacy Framework

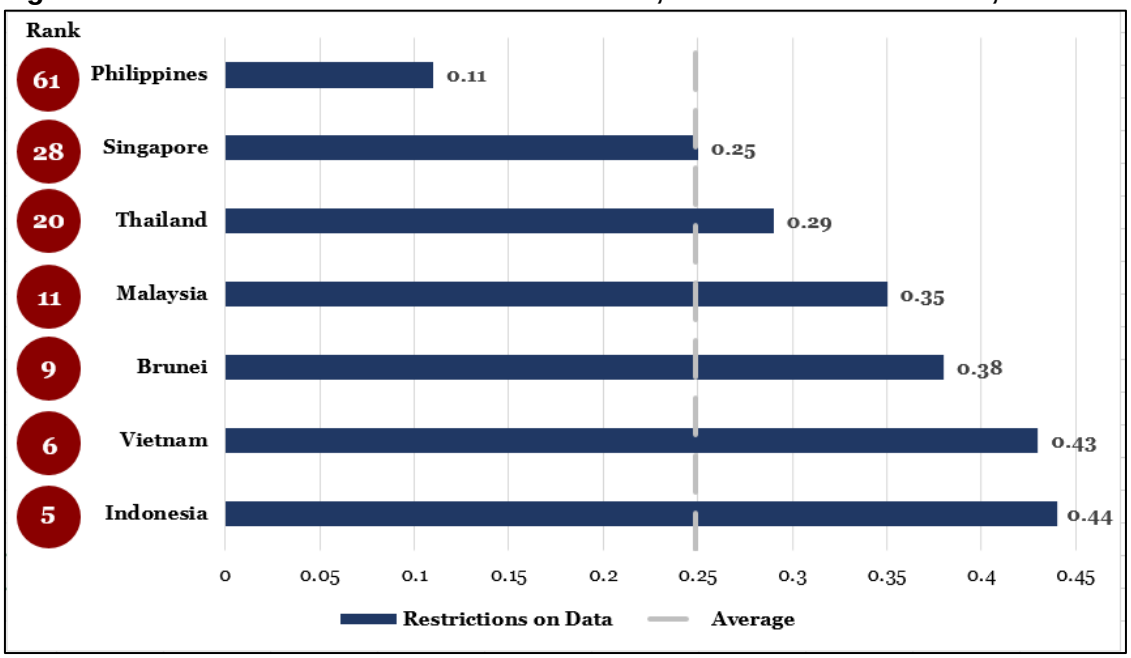
ELEMENT	PHILIPPINES
Data Protection Law/s	Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA)
Implementation Guidelines	Implementing rules and regulations (IRR) of the DPA and various advisories and circulars released by the NPC
Enforcement Authority	National Privacy Commission (NPC)
Guidelines or Rules on Cross-Border Data Flow	Covered by the Data Privacy Act of 2012 NPC Advisory No. 2021-02
Public-Private Consultation	Actively engages with civil society and the private and public sector on issues [e.g., public consultation and stakeholders meetings on the Data Privacy Act of 2012, its IRR, and various issuances and conduct of Data Privacy Council assemblies]
Training	Organizes capacity building trainings [e.g., Data Protection Officer Accountability, Compliance, and Ethics Certification Program (DPO ACE), DPO COMPLex Workshop, Health Privacy Forum]
Public Education	Organizes awareness drives and national campaign on privacy issues for stakeholders (e.g., Annual Privacy Awareness Week; Privacy toolkit; Privacy, Safety, Security, and Trust Online (PSST!) communication campaign; and release of Online Learning Guidelines]
Multilateral and Bilateral Engagement	Interacts with other data protection authorities [e.g., MoU with UK Information Commissioner's Office and Singapore Personal Data Protection Commission; Chairing of the Global Privacy Assembly's (GPA) COVID-19 Taskforce; and Engagement with the Asia Pacific Privacy Authorities (APPA), ASEAN Data Protection and Privacy, and International Association of Privacy Professionals (IAPP)]
Coordination Mechanism for Government Agencies	Resource agency for the Task Force on Big Data, member of the Joint Cybersecurity Working Group, and involvement in the Subcommittee on IT for learning, education and training (SC 2), the Technical Committee on Information Technology (TC 60), and Technical Working Group (TWG) on National Security Issues on Government-Issued Documents
Self-Regulation	Joined the APEC Cross-Border Privacy Rules (CBPR)
National Strategy	----------

Source: GSMA 2018; Philippine initiatives updated by Author

With its privacy framework at the progressing stage, the Philippines is at an advantageous position as supported by the European Centre for International Political Economy's Digital Trade Restrictiveness Index (DTRI), which measures how countries restrict trade.[6] Specifically, the data restrictions cluster[7] reveals that the Philippines has attained the highest ranking or the least restrictive regime among ASEAN member states *(See Figure 3)*. Further, the country's index score of 0.11 on restrictions covering data policies, intermediate liability and safe harbor for intermediaries, and online content access, is well below the average index of 0.25 of all the included economies.

[6] The overall index scores are taken as the weighted average of the clusters and range from the least restrictive (0) to the most restrictive (1).
[7] The other three (3) clusters are: (a) Fiscal Restrictions; (b) Establishment Restrictions; and (c) Trading Restrictions.

Figure 3. DTRI Cluster C – Restrictions on Data, ASEAN Member States, 2018

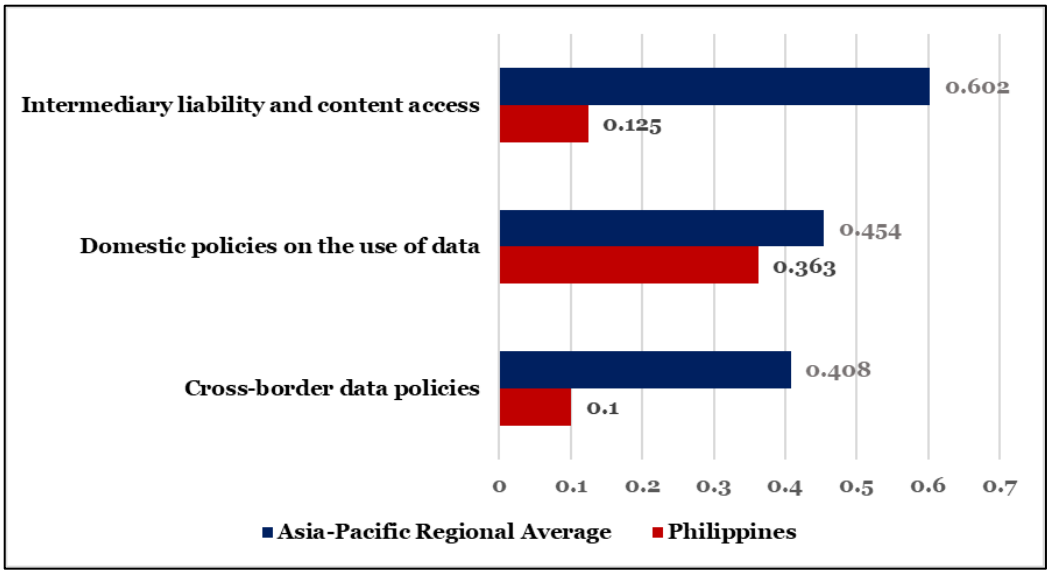


Note: Ranking is across 64 economies from the most restrictive (1st) to the least restrictive (64th)
Source: Ferracane, M., Lee-Makiyama, H., and van der Marel, E. (2018)

Building on the DTRI, the United Nations Economic and Social Commission for Asia and the Pacific developed the Regional Digital Trade Integration Index (RDTII)[8] and used by Albert et al. (2021) to assess the readiness of countries for regional digital trade integration. A focus on the pillars relating to data provides similar results of the Philippines having a less restrictive regime with index scores of 0.125, 0.362, and 0.100 in intermediate liability and content access, domestic policies on the use of data, and cross-border data policies, respectively, falling below the Asia-Pacific regional average *(See Figure 4)*.

[8] *The RDTII has 11 pillars: (A) Tariffs and trade defense measures applied on intraregional imports of ICT-related goods; (B) Public procurement related to digital goods and services; (C) Foreign direct investment in sectors relevant for digital trade (D) Intellectual Property Rights; (E) Telecommunications infrastructure and competition; (F) Cross-border data policies; (G) Domestic policies on the use of data; (H) Intermediary liability and content access; (I) Quantitative trade restrictions; (J) Standards; and (K) Online sales and transactions. Similarly, the overall index scores are taken as the weighted average of each pillar and range from the least restrictive (0) to the most restrictive (1).*

Figure 4. RDTII Pillars 6, 7, and 8, Philippines and Asia-Pacific, 2020



Note: The study covers 22 economies in the Asia-Pacific region, including New Zealand, Singapore, Hong Kong, Vanuatu, Australia, Turkey, Nepal, Malaysia, Lao PDR, Brunei Darussalam, Japan, Republic of Korea, Kazakhstan, Thailand, Cambodia, Pakistan, Russia, Viet Nam, Indonesia, India, and China; country breakdown not available
Source: Albert, J., Calizo, S., Carlos, J., and Quimba, F. (2021)

The DTRI and RDTII scores of the Philippines reveal that the country has relatively lower barriers to digital trade and greater openness to regional integration with measures that are non-discriminatory and not excessively burdensome. This facilitative environment is crucial as the value of digital-trade induced benefits of the country in 2018 was estimated to be at 1.8% (USD3 billion) of the country's GDP and is projected to grow by almost 12-fold (USD36.2 billion) by 2030 (Hinrich Foundation, 2019).

V. Recommendations

With the enabling laws and regulations in place and a proactive NPC that engages with stakeholders, participates in international fora, and provides for training and public education, the Philippines is in an opportune condition to elevate its data privacy regime from the progressing stage into the advanced stage based on the GSMA Mature Privacy Framework. This fosters greater trust from consumers and facilitates international harmonization, thus enhancing the development of industries.

To attain its development objective, the Philippines must formulate a national strategy on data privacy in order to have all of the elements of a mature privacy framework. As recommended by the Organisation for Economic Co-operation and Development Privacy Framework (OECD, 2013) the national strategy should set the goals and reflect a coordinated approach across governmental bodies. A national strategy underpinned by the DPA elevates the importance of data privacy protection to the highest levels within government and aids in improving the coherence and effectiveness of initiatives.

The national strategy may aid in ensuring a consistent level of protection across government institutions that make use of personal data and a compatible policy development in related areas, providing an active role in shaping policies and programs that pose a threat to privacy. This may guide stakeholders in addressing emerging data privacy issues such as the implementation of RA No. 11055 or the Philippine Identification System Act; RA No. 11223 or the Universal Health Care Act, which calls

for the establishment of a health information system; and Executive Order (EO) No. 2, s. 2016 or the Freedom of Information (FOI) Program.

This is also especially relevant to realign the national strategy as governments and industries have harnessed technology amidst the COVID-19 pandemic. The proliferation of various software, such as contact-tracing applications, must be met not only with secure technologies and tools but also with well-informed and well-equipped data protection officers to ensure the right to privacy of individuals and mitigate the risks to privacy.

The national strategy is especially timely as the NPC seeks to amend the DPA, which has been in place for almost a decade, to redefine sensitive personal information by including biometric and genetic data, clarify extraterritorial application of the law, modify criminal penalties, strengthen the rights of data subjects, and expand the NPC's mandate, among others (NPC, 2021b). The proposed legislations on these amendments have yet to fully progress in the 18th Congress, initially with two (2) House Bills[9] filed in 2019, substituted by House Bill No. 9651, which was approved by the House of Representatives (HOR) on 24 August 2021. On the other hand, one (1) Senate Bill[10] filed in 2020 remains pending with the Committee on Science and Technology. With less than a year left in the 18th Congress, a national strategy that contains the objective and necessity of these reforms may aid in influencing the policy agenda setting to gain high priority in the next administration.

The Philippines may take its cue from Japan, which began its endeavor to amend its privacy law, the Act on the Protection of Personal Information of 2003, by releasing the Policy Outline of the Institutional Revision for Use of Personal Data in 2014 (Japan Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, 2014). The outline mapped out the government's direction in recognition of issues on barriers to the utilization of personal data, enforcement of the data privacy system, and harmonization with international standards. In providing a context for pursuing the reform, Japan was able to eventually amend its privacy law in 2015 (Japan Personal Information Protection Commission, 2015).[11] Further, the Philippines may also benefit from the practice of Malaysia and Vietnam in involving the public in initiatives to review and amend their legislations on personal data protection.[12]

The approach may be similar to the various industry roadmaps prepared by the DTI, detailing the current situation of data privacy in the country and outlining the various interventions, process owners, and timeframe in the achievement of industry goals. However, as the data privacy policy is meant to support the growth of various industries, the national strategy may be more directional in nature, emphasizing that the data policy should be facilitative and non-restrictive. By concretizing the objectives of the country in terms of data privacy together with the necessary policy reforms and interventions to be

[9] House Bill No. 1188 entitled, "An Act Amending Republic Act No. 10173, Otherwise Known as the 'Data Privacy Act of 2012', to Adopt a More Systematic, Comprehensive and Effective Protection Program, to Foster the Imposition of All Existing Policies and Guidelines, Increasing Its Penalties and Sanctions, and for Other Purposes" and House Bill No. 5612 entitled, "An Act Amending Republic Act No. 10173, Otherwise Known as the 'Data Privacy Act of 2012'"
[10] Senate Bill No. 1446 entitled, "An Act Amending Republic Act No. 10173, Otherwise Known as the 'Data Privacy Act of 2012'"
[11] Japan has pursued further amendments to the law in 2020 to broaden extraterritorial reach, mandate data breach notifications, and expand personal information concepts and categories.
[12] Malaysia conducted its review from 14 to 28 February 2019 embodied in Public Consultation Paper No. 01/2020 while Vietnam solicited comments on the outline of its draft Decree on Personal Data Protection released in December 2019 and the full text in February 2021.

pursued, this serves as an enhancement to the NPC's Roadmap to Data Compliance (2017), which provides guidance to stakeholders, specifically businesses, to implement the provisions of the DPA.

While the NPC has the institutional mandate and capacity to spearhead the formulation of the national strategy, collaboration and consultation with experts from other government agencies [e.g., Philippine Statistics Authority (PSA), Presidential Communications Operations Office (PCOO)], private sector [e.g., IT and Business Process Association of the Philippines (IBPAP)], civil society [e.g., National Association of Data Protection Officers of the Philippines (NADPOP), Foundation for Media Alternatives (FMA)] may inform the approach and obtain a high-level political buy-in to improve data protection.

This will also aid in maintaining balance by avoiding unjustified restrictions and requirements on the free flow of data, which have been shown to be significant impediment to the adoption and proliferation of emerging technological development by enterprises. (Bauer et al. 2014; UNCTAD, 2016)

An established national data privacy framework in the Philippines may also aid in the country being considered by the European Union (EU)[13] to have an adequate level of data protection and may facilitate the flow of personal data from the EU to the Philippines without requiring any further safeguards, which will be very beneficial in supporting the growth of its domestic sectors.[14,15]

While a mature data privacy framework provides a strong foundation to enable cross-border data flows, it is necessary that the national framework takes into consideration other countries' data privacy laws. While uniform regional data protection legislations may not be feasible given that the ASEAN and APEC privacy frameworks are more flexible than prescriptive in nature, emphasis should be on collaboration among its members given the different levels of data privacy development. With this, the Philippines may instead endeavor to promote cooperation among data privacy authorities and pursue mutual recognition agreements (MRAs) of privacy certifications. While it may do this as a regional bloc together with other ASEAN member states to broaden its application, it should also simultaneously pursue bilateral agreements that may be advanced more quickly.

Given that the country is at the forefront of the data privacy in the region, it may also actively advocate for the participation of other ASEAN member states into the APEC CBPR System. This will strengthen efforts at the international arena as data privacy is increasingly being embedded in free trade agreements (FTAs), such as the e-commerce chapter in the Regional Comprehensive Economic Partnership (RCEP).[16]

The DTI may support the growth of the local data protection ecosystem in line with its startup development initiative as part of the implementation of RA No. 11337 or the Innovative Startup Act. Some of these programs include the **Strategic MSMLE & Startup** (**SMART) Link, which** aims to match leading-edge innovative startups in the Philippines with commercial products to traditional enterprises through conducting

[13] *EU General Data Protection Regulation (GDPR) 2016/679*
[14] *Provided for in Article 45 of EU GDPR 2016/679*
[15] *Currently the EU recognizes the adequacy of data protection standards in the Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan and most recently, the UK.*
[16] *Article 12.8: Online Personal Information Protection*

business-to-business matching sessions or Smart Link Sessions and the **Startup Acceleration and Incubation by DTI (startupAID), which provides** a specialized training program co-developed with partner startup enablers.

Finally, intensifying public education and training to ensure that MSMEs, including startups, are able to understand and comply with data privacy standards will also facilitate scaling up and their participation in global value chains (GVCs).

VI. Conclusion

Opportunities arise for industries to provide targeted products and services to consumers, and for governments to improve public service delivery as economies generate data through the increasing adoption of innovative solutions and digital technology. With this comes a greater responsibility to keep data safe, secure, and protected. A mature data privacy framework resonates with the DTI's dual mandate to enable businesses and empower consumers. A concerted effort of the government to embed data privacy in policies and processes allows for a secure, sustainable, and digitally-enabled economy.

To aid in achieving a mature data privacy framework in the advanced stage, the country must formulate a national strategy on data privacy. Together with this it must continue to advocate for the participation of other ASEAN member states into the APEC CBPR System, support the growth of the local data protection ecosystem, and intensify public education and training.

References

Albert, J., Calizo, S., Carlos, J., & Quimba, F. (2021). How Ready Are We? Measuring the Philippines' Readiness for Digital Trade Integration with the Asia-Pacific. PIDS Discussion Paper No. 2021-17. Philippine Institute for Development Studies.

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). The consumer-data opportunity and the privacy imperative. McKinsey & Company.

Asia-Pacific Economic Cooperation. (2015). Privacy Framework.

Association of Southeast Asian Nations. (2016). Telecommunications and Information Technology Ministers Meeting Framework on Personal Data Protection.

Association of Southeast Asian Nations. (2021). ASEAN Data Management Framework.

Bauer, M., Lee-Makiyama, H., Van der Marel, E., & Verschelde, B. (2014). The Costs of Data Localisation: Friendly Fire on Economic Recovery. ECIPE Occasional Paper No. 3/2014. European Centre for International Political Economy.

Bauer, M., Lee-Makiyama, H., Van der Marel, E., & Verschelde, B. (2016). Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States. ECIPE Policy Brief No. 3/2016. European Centre for International Political Economy.

Cadawalladr, C. & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. http://freestudio21.com/wp-content/uploads/2018/04/50-million-fb-profiles-harvested-by-cambridge-analitica.pdf

Casalini, F. & López González, J. (2019). Trade and Cross-Border Data Flows. OECD Trade Policy Papers, No. 220, OECD Publishing, Paris.

Const., Art. II § 11 (Phil.).

Const., Art. III § 2 (Phil.).

Const., Art. III § 3 (Phil.).

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation.

Crismundo, K. (2020, November 20). Local IT-BPM growth seen flat this year. Philippine News Agency. https://www.pna.gov.ph/articles/1122458

Cuevas, M., Nurullaev, R., Szulewski, P., & Ursic, H. (2018). Data Localisation Measures and Their Impacts on Data Science. In Berlee, A., Mak, V., and Tjong Tjin Tai, E. & (2018). Research Handbook in Data Science and Law. Edward Elgar Publishing.

Data Privacy Act of 2012, Rep. Act. No. 10173, § 2 (Phil.).

Department of Trade and Industry. (2017). Philippine Inclusive Innovation Industrial Strategy (i3S) (Policy Brief 2017-05).

DiPaula-Coyle, M. (2021). Digital Trade and Cross-Border Data Flows. [PowerPoint Slides]. http://mddb.apec.org/Documents/2021/CTI/TPD1/21_cti_tpd1_002.pdf

Ferracane, M., Lee-Makiyama, H., & van der Marel, E. (2018). Digital Trade Restrictiveness Index. European Centre for International Political Economy.

Global System for Mobile Communications. (2018). Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation.

Hinrich Foundation. (2019). The Data Revolution: Capturing The Digital Trade Opportunity at Home and Abroad.

Japan Personal Information Protection Commission. (2015). Amended Act on the Protection of Personal Information.

Japan Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society. (2014). Policy Outline of the Institutional Revision for Utilization of Personal Data.

Jawaid, T. (2020). Privacy vs National Security. International Journal of Computer Trends and Technology.

McKinsey Global Institute. (2016). Digital Globalization: The New Era of Global Flows.

National Privacy Commission. (2015, October 21). PH Privacy Commission gets international accreditation. https://www.privacy.gov.ph/2016/10/ph-privacy-commission-gets-international-accreditation/

National Privacy Commission. (2016a, July 19). Invitation to Comment: Proposed Implementing Rules and Regulations of the Data Privacy Act. https://www.privacy.gov.ph/2016/07/invitation-to-comment/

National Privacy Commission. (2016b, July 28). Data Privacy Act. IRR Public Consultation – Cebu, 28 July 2016. https://www.privacy.gov.ph/2016/07/data-privacy-act-irr-public-consultation-cebu/

National Privacy Commission. (2017). Roadmap to Compliance Data Privacy Act of 2012.

National Privacy Commission. (2018a, April 6). Press Statement from Privacy Commissioner Raymund Enriquez Liboro on the Facebook Controversy involving Cambridge Analytica. https://www.privacy.gov.ph/2018/04/press-statement-from-privacy-commissioner-raymund-enriquez-liboro-on-the-facebook-controversy-involving-cambridge-analytica/

National Privacy Commission. (2018b, 12 December). NPC launches DPO ACE Program, sets benchmark for data privacy training in PH. https://www.privacy.gov.ph/2018/12/npc-launches-dpo-ace-program-sets-benchmark-for-data-privacy-training-in-ph/

National Privacy Commission. (2018c). Annual Performance Report 2017.

National Privacy Commission. (2018d). NPC Privacy Toolkit.

National Privacy Commission. (2019a). Annual Performance Report 2018.

National Privacy Commission. (2019b, September 10). PH, Singapore sign MoU on Personal Data Protection. https://www.privacy.gov.ph/2019/09/ph-singapore-sign-mou-on-personal-data-protection/

National Privacy Commission. (2019c, September 20). PH joins APEC privacy system. https://www.privacy.gov.ph/2019/09/ph-joins-apec-privacy-system/

National Privacy Commission. (2019d, November 2019). NPC sets up DPO COMPLex workshop for GOV'T. https://www.privacy.gov.ph/2019/11/npc-sets-up-dpo-complex-workshop-for-govt/

National Privacy Commission. (2020a, June 01). PH to lead global privacy taskforce on COVID-19. https://www.privacy.gov.ph/2020/06/ph-to-lead-global-privacy-taskforce-on-covid-19/

National Privacy Commission. (2020b, October 01). NPC PHE BULLETIN No. 16: Privacy Dos and Don'ts for Online Learning in Public K-12 Classes. https://www.privacy.gov.ph/2020/10/npc-phe-bulletin-no-16-privacy-dos-and-donts-for-online-learning-in-public-k-12-classes/

National Privacy Commission. (2020c, October 17). NPC holds first ever Health Privacy Forum to promote sector compliance. https://www.privacy.gov.ph/2020/10/npc-holds-first-ever-health-privacy-forum-to-promote-sector-compliance/

National Privacy Commission. (2021a, January 14). Privacy Commission firms up collaboration with UK counterpart in sharing best privacy practices. https://www.privacy.gov.ph/2021/01/privacy-commission-firms-up-collaboration-with-uk-counterpart-in-sharing-best-privacy-practices/

National Privacy Commission. (2021b, June 25). A Stronger Data Privacy Law Sought in Proposed Amendments. https://www.privacy.gov.ph/2021/06/a-stronger-data-privacy-law-sought-in-proposed-amendments/

National Privacy Commission. (2021c, October 15). Privacy Commission launches open call for accountability agent applicants for APEC cross-border privacy rules system. https://www.privacy.gov.ph/2021/10/privacy-commission-launches-open-call-for-accountability-agent-applicants-for-apec-cross-border-privacy-rules-system/

National Privacy Commission. (2021d, November 11). NPC launches Ph Privacy Trust Mark to add value to business, boost trust in cross-border data transfers. https://www.privacy.gov.ph/2021/11/npc-launches-ph-privacy-trust-mark-to-add-value-to-business-boost-trust-in-cross-border-data-transfers/

National Privacy Commission. (2021e, November 25). Online safety of children takes center stage in NPC's Kabataang Digital. https://www.privacy.gov.ph/2021/11/online-safety-of-children-takes-center-stage-in-npcs-kabataang-digital/

Office of the President. (2017, April). National Security Policy for Change and Well-being of the Filipino People: 2017-2022.
.
Organisation for Economic Co-operation and Development. (2013). Privacy Framework.

Pasadilla, G. (2020). Next generation non-tariff measures: Emerging data policies and barriers to digital trade. Asia-Pacific Research and Training Network on Trade. Working Paper No. 187.

Ponemon Institute. (2017). The True Cost of Compliance with Data Protection.

Ramos, C., Sheppard, L., & Yayboke, E. (2021). The Real National Security Concerns over Data Localization. CSIS Briefs.

Startup Genome. (2021). The Global Startup Ecosystem Report 2021.

Storage Networking Industry Association. (n.d). What is Data Protection? https://www.snia.org/education/what-is-data-protection

United Nations. (1948). Universal Declaration of Human Rights.

United Nations (General Assembly). (1966). International Covenant on Civil and Political Rights. Treaty Series, 999, 171.

United Nations Conference on Trade and Development. (2016). Data Protection Regulations and International Data Flows: Implications for Trade and Development. New York: United Nations.

White, L. (2008). Antitrust Policy and Industrial Policy: A View from the U.S. New York University Law and Economics Working Papers. Paper 118.

World Economic Forum. (2018). Data Policy in the Fourth Industrial Revolution: Insights on personal data.