DECEMBER 2020

DISCUSSION PAPER SERIES NO. 2020-47

Cross-border Data Regulation for Digital Platforms: Data Privacy and Security

Aiken Larisa O. Serzo

The PIDS Discussion Paper Series constitutes studies that are preliminary and subject to further revisions. They are being circulated in a limited number of copies only for purposes of soliciting comments and suggestions for further refinements. The studies under the Series are unedited and unreviewed. The views and opinions expressed are those of the author(s) and do not necessarily reflect those of the Institute. Not for quotation without permission from the author(s) and the Institute.

CONTACT US:

RESEARCH INFORMATION DEPARTMENT
Philippine Institute for Development Studies

18th Floor, Three Cyberpod Centris - North Tower
EDSA corner Quezon Avenue, Quezon City, Philippines

publications@mail.pids.gov.ph
(+632) 8877-4000

https://www.pids.gov.ph

Cross-border Data Regulation for Digital Platforms: Data Privacy and Security

Aiken Larisa O. Serzo

PHILIPPINE INSTITUTE FOR DEVELOPMENT STUDIES

December 2020

Abstract

The rise of digital platforms necessarily entails the processing of personal data between platforms and their users. More than enabling the delivery of services by the platforms, data shared by users has increasingly become valuable as various businesses are able to leverage their access to data in order to create and upsell other services.

Data is increasingly becoming a valuable commodity for platforms. The increase in digital transactions and individuals with access to the internet require the implementation of privacy regulations in order to uphold the privacy rights of individuals while still allowing the flow of data across entities and jurisdictions.

However, the ability of platforms to engage in cross-border transactions or operations are affected by the stringent requirements of data protection laws, coupled with the divergent regulations among jurisdictions. Such divergence also serves to weaken the ability of regulations to curb undesirable data processing practices, as platforms may take advantage of jurisdictions with weaker data protection rules in place. The effectivity of data protection mechanisms, which are focused on a consent-based regime, may also have some intended consequences where regulations have allowed platforms to legally exploit data without actually providing greater control to the data subjects themselves.

With the Philippines as an example, this paper points out the salient points in existing data protection regulations and the impact of these principles on both platforms and data subjects.

Given that data fuels the operations of digital platforms and other technology companies, restrictions on how data may be used, shared, stored, or otherwise processed, will undoubtedly affect digital platforms economically and operationally.

This paper aims to demonstrate how data protection regulations impact the operation of regional digital platforms and data subjects. It will also suggest policy considerations for the continuous development of such regulations.

To illustrate and provide an analysis on data protection regulations vis a vis the digital platforms, Part II of this Paper will do a thorough analysis of the data protection regulations in the Philippines. Part III will provide an overview of the existing international frameworks and a snapshot of the regulations of certain Asia Pacific countries with regard to the transfer of data to offshore jurisdictions.

Part IV will be a discussion on the implications of data protection regulations on the operations and viability of digital platforms. It will include the effects of such data protection legislation and regulations on the data subjects, and on digital platforms. Part V will identify certain regulatory and policy actions that may be considered moving forward.

Keywords: data privacy, regulatory reform, digital platforms, data sharing

Table of Contents

LIST OF TABLES

Cross border data regulation for digital platforms: Data privacy and security[1]

Aiken Larisa O. Serzo[2]

Introduction

1.1. Digital Platforms and the Processing of Data; New technologies and the Data Economy

Globalized trade and increased cross-border transactions present interesting legal implications on the ability of states and data subjects to control and protect data. Digital platforms made it possible for transactions to be concluded beyond national borders. Most digital platforms use cloud service providers to store user and transaction data and as a diligent way of ensuring business continuity. These cloud service providers, such as Google Cloud and Amazon Web Services, have data centers all around the world and would therefore host data in various countries. The ease of conducting transactions via online platforms allows participants, both private and public, to expand their reach and offer more services at accessible rates.

Digital platforms process and share data through layered activities – platforms may process and share data to fulfill its primary obligations to the user, such as the delivery of goods or services as directed by the user. However, the sharing of data may also be done in order to further upsell other services which the user has not actively opted in to. Given the developments in the areas of the internet of things, big data, and data science analytics, a secondary market for data has also been created. Data may be monetized by processing the same beyond the initial purpose of fulfilling the instructions of a user. This would include the conduct of targeted advertising and marketing communications, and other data science and machine learning applications such as credit scoring and market research.

The novel coronavirus disease (COVID-19) and the subsequent mobility restrictions set in place by government authorities sped up the adoption of technology and digital platforms. The ongoing response related to the COVID-19 pandemic also exposed the ways that data may be exploited: The identities of suspected patients are leaked in social media; employers have amended their policies to require personnel to disclose travel and medical history; and local

---

[1] "The Asian Development Bank is the sole owner of the copyright in ADB Contribution developed or contributed for this Work, and has granted permission to PIDS to use said ADB-copyrighted Contribution for this Work (, and to make the Contribution available under an open access license.)"

The views expressed in this publication are those of the authors and do not necessarily reflect the views and policies of the Asian Development Bank (ADB) or its Board of Governors or the governments they represent. ADB does not guarantee the accuracy of the data included in this publication and accepts no responsibility for any consequence of their use.

By making any designation of or reference to a particular territory or geographic area, or by using the term "country" in this document, ADB does not intend to make any judgments as to the legal or other status of any territory or area.

[2] Consultant at the University of the Philippines Law Center Technology Law and Policy Program; Senior Associate and Head of the Fintech Practice in Disini Buted Disini Law Office.

government units have published the names and addresses of individuals that are entitled to receive financial assistance. Academic and policy debates also abound related to the implementation of GPS tracking technology to implement better contact tracing tools, and AI-enabled technologies that assist doctors identify COVID-infected patients in x-rays.

The number of total internet users in South East Asia has steadily been rising. A study[3] by Google, Temasek and Bain & Company on e-commerce in South East Asia, found that there is a total of 400 million internet users in the region, with 40 million users added in 2020 alone – an exponential increase in light of a finding that a total of 100 million users were added between 2015 and 2019. The same study showed that the pandemic served to accelerate digital consumption with users increasingly relying on digital services. The surge in digital platforms and online commerce are further fueled by foreign investments from Asia.[4]

Government entities are also driving the growth in innovation and digitization of data processing. Policies from different agencies have been geared towards supporting innovation and developing the technological capabilities of private and public entities.

In the Philippines for example, the Philippine Identification System ("PhilSys"), the country's national ID system, is meant to establish a foundational identification system to provide a valid proof of identity for all citizens and resident aliens as a means of simplifying public and private transactions.[5] Under the law, an individual's record in the PhilSys is considered as an official and sufficient proof of identity,[6] which all entities are required to accept. This will expedite the onboarding process of users to certain digital platforms where identity is crucial in the delivery of services and prevention of fraud. The Bangko Sentral ng Pilipinas ("BSP"), as documented through its National Strategy for Financial Inclusion which was launched in 2015, is also pushing for greater digitization. The financial inclusion steering committee of the BSP has been committed to ensure more Filipinos are able to open and regularly use a transaction account so that they can participate in the gains of an inclusive digital finance ecosystem.

The enactment of the Philippine Data Privacy Act of 2012 (the "DPA"), together with the aggressive enforcement efforts of the National Privacy Commission (the "Commission") placed the topic of data privacy and protection at the forefront of issues that businesses in the Philippines, especially digital platforms, are concerned with. The attention given to the DPA may also be attributable to the characterization of the law as criminal acts and the unauthorized processing of personal data. Violators may therefore be subject to fines and imprisonment, in addition to possible administrative and civil liabilities.

There has yet to be an instance where the Commission meted out substantial fines or penalties, however, the Commission however has been actively sending audit notices to several companies. The Commission has also cracked down on industries and certain activities that it determined to pose substantial privacy risks for its data subjects. The Commission issued a Cease and Desist Order to a Grab Philippines' selfie verification, audio and video recording

---

[3] Google & Temasek / Bain. 2019. E-Conomy SEA 2020.

[4] United Nations Conference on Trade and Development. 2016. Global Investment Trend Monitor. Geneva, Switzerland: UNCTAD. https://unctad.org/system/files/official-document/webdiaeia2016d3_en.pdf (accessed on 10 May 2020).

[5] Rep. Act. No. 11055, § 3.

[6] *Id.* at § 6.

systems after it identified certain deficiencies in the company's processing systems.[7] An Order was also sent to lending companies, ordering the latter to stop engaging in certain activities that violate the DPA.[8] It may only be a matter of time before the Commission takes a more aggressive approach against data breaches and other violations of the DPA. The foregoing acts show how serious the Commission is in instilling a culture of privacy to platforms, whether located here or abroad, that process the personal data of Philippine citizens.

The push for innovation and the consequent growth in digital transactions will only also result in the increased collection, storage, and sharing of personal information.

1.2 Challenges of regulating data protection and processing.

1.2.1 Absence of Enforceable Intergovernmental Data Protection Policies

In the context of increasing globalized trade and considering the borderless nature of digital platform transactions, commercial transactions and internal operations of platforms will necessarily involve cross-border sharing and/or transfers of data. A transaction may therefore trigger the regulations of several jurisdictions. Except for the General Data Protection Regulation (GDPR) of the European Union and the members of its European Economic Area, there is currently no enforceable and legally binding international standard for data regulation. Countries in the Asia Pacific region are not subjected to any overarching, international data protection regulation. This is in spite of the existence of various intergovernmental initiatives meant to encourage alignment of data protection policies. The details of these frameworks are discussed in more detail in Part III. These frameworks recognize the importance of data protection and privacy laws, identifying gaps, and providing policy options for developing and implementing national laws on data protection.

1.2.2 Exponential Developments in Technologies

Even without considering the cross-border nature of data processing, the effective implementation of data protection measures is complicated by the continuous development of the models and operations of entities that process data. Technology is always in flux. Technologies allow operations and business models that were previously unanticipated by the regulators. As such, regulations may not be sufficient to consider novel structures and processes. Regulators may be tempted to immediately regulate a new business model. However, a preemptive action by the regulator may also hamper the growth of innovation and serve to discourage further experimentation and innovation. Further, regulators are also at most times at a disadvantaged position in terms of technical expertise. This therefore makes the regulator dependent on the market participants for information and knowledge.

---

[7] National Privacy Commission (NPC). 2020. NPC Suspends GRAB PH'S Selfie Verification, Audio, Video Recording Systems. Pasay City, Philippines: NPC. https://www.privacy.gov.ph/2020/02/npc-suspends-grab-phs-selfie-verification-audio-video-recording-systems/ (accessed on 15 July 2020).

[8] National Privacy Commission (NPC). 2019. Order: Violations of the Data Privacy Act by Several Companies Operating Online Lending Applications. Pasay City, Philippines: NPC. https://www.privacy.gov.ph/2019/10/order-violations-of-the-data-privacy-act-by-several-companies-operating-online-lending-applications/ (accessed on 15 July 2020).

1.2.3 Normative Challenges

Data protection is also normatively and culturally challenging to enforce. Data protection legislation necessitates the regulation of the behavior of different actors with regard to data. Unlike other prohibitive regulations, the benefits of restricting the processing of data may not be clearly apparent to the persons subject of the regulations.

Case Study - Philippine Data Privacy regulation

1.2. Philippine Data Protection Act

The processing of personal information, which includes the cross-border transfer of data, is generally governed by the Data Privacy Act of 2012 ("DPA") and the implementing rules and regulations of the Commission. Some specific types of personal data relating to banking and financial information, tax information, and employment information may be regulated by banking or tax laws and other regulations. However, the baseline regulation for the processing of all types of personal information will still be the DPA. As provided in the law's policy declaration, the objectives of the DPA are (i) to protect the fundamental right of privacy of data subjects, and (ii) to ensure the free flow of information necessary to promote innovation and growth.[9]

The key principles espoused by the law relates to the following: (i) the parameters for the legal processing of personal information; (ii) the provision of substantive rights of data subjects relating to their personal information; (iii) accountability of entities that process personal information; and (iv) enforcement of data privacy rights. In the Philippines, all types of personal information, regardless of category, is protected by the DPA. This is unlike other jurisdictions with sector-specific personal data protection regulation.

1.2.1. Scope of Application

The law has a broad scope of application. The DPA applies to all persons (individual or juridical), in both government and private sectors, which process personal information.[10] Unlike the data protection regulations of other jurisdictions, the DPA covers all types of persons and entities, provided they are processing personal information, regardless of the type, size, or income of the organization. It will therefore apply even to sole proprietors, including informal and unorganized businesses (such as sari-sari stores, and other unregistered enterprises), and individual professionals and contractors. As a general rule, the law will find application provided that the data processing activity is conducted in the Philippines, regardless of the citizenship of the data subjects whose personal information is being processed.

Furthermore, the DPA has extraterritorial application (i.e. it will apply to activities done offshore) when the data subject whose personal information is being processed is a Filipino

[9] Rep. Act No. 10173 § 2.
[10] *Id.* at §4.

citizen or a Philippine resident.[11] Entities located offshore may therefore be subject to the regulatory reach of the Commission.

The definition of personal information under the DPA is expansive as it includes any information, in whatever form, "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 the individual."[12] For digital platforms, the DPA will therefore apply even if the platform in question only provides services to business entities (i.e. B2B solutions) and does not have individual end users as customers. At a minimum, a B2B business will still be handling the personal information of its employees. There may also be solutions which require the platform to handle the personal data controlled by its business customers.

Relevantly, the term "processing" will include any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data,[13] whether through automated or manual means.[14]

There are certain instances when the DPA will not apply. For instance, the law does not apply to personal information processed for journalistic, artistic, literary or research purposes.[15] However, despite the explicit exclusion, the terms "journalistic", "literary" and "research" are not defined under the law or its implementing rules, thus providing a wide source of possible conflict. This is problematic, for example, for data science and AI-enabled technologies. Technically, merely training algorithms is an activity in furtherance of research. However, the procedure of training software and doing backtesting may have some implications in how the software will make decisions later on during production.

The DPA also explicitly exempts from its application personal information "originally collected from residents of foreign jurisdictions".[16] However, note that the law also states that the DPA will nonetheless apply should the personal information of Filipino citizens located overseas be involved. Hence to minimize potential liability, it will be prudent for entities covered by the law to simply comply with the DPA even if it only processes data from persons abroad.

In recognition of other existing regulations on credit information, bank information, and anti-money laundering, the law explicitly excludes from its scope personal information necessary for banks and other financial institutions regulated by the Philippine central bank to comply with anti-money laundering laws.[17] There are also exemptions[18] pertaining to the personal

---

[11] *Id.* at §6.
[12] *Id.* at §3(g).
[13] *Id.* at §3(j).
[14] Implementing Rules and Regulations of Rep. Act No. 10173, §3(o).
[15] Rep. Act No. 10173, §4(d).
[16] *Id.* at §4(g).
[17] *Id.* at §4(f)).
[18] *Id.* at §4 (a)(b)(c): This section lists down the exceptions: The DPA does not apply to "information about any individual who is or was an officer of a government institution that relates to the position or functions of the individual; information about an individual who is or was performing service under contract for a government institution that relates to the services performed, the terms of the contract, and the name of the individual given

information of government officials and government service providers. It should be noted that even for instances falling under the defined exceptions, the Commission requires that the entities involved in the processing of the data are legally obligated to comply with the requirements of implementing security measures for personal data protection.[19]

1.2.2. Accountability for Processing; The Principle of Accountability

The law provides a distinction between personal information controllers ("Controllers") and personal information processors ("Processors"). Essentially, an entity is deemed a Controller if it controls the collection, holding, processing or use of personal information,[20] and decides on what information is collected, or the purposes or extent of its processing.[21] On the other hand, a Processor refers to any natural or juridical person to whom a Controller may outsource the processing of personal data pertaining to a data subject.[22]

The legal obligations on data protection is primarily imposed on the Controllers.[23] Controllers must ensure that the processing activities undertaken pursuant to its purposes and instructions are compliant with the general data privacy principles of transparency, legitimate purpose, and proportionality, and other provisions of the DPA. Should the Controller outsource certain portions of its business to other entities whether local or offshore, the Controller will remain responsible for the acts of its contractors or processors to whom it outsources processing activities.[24] Processors may include cloud service providers, telecommunications providers, data management companies, logistics providers, and other subcontractors.

The gravity of the responsibility of the Controllers is magnified when one considers that the DPA is a criminal statute. The DPA penalizes any natural or juridical person who commits any of the offenses provided therein, including users and personal information controllers and personal information processors. As mentioned, the law provides that in cases of data breach by subcontractors, the subcontracting Controller will be held responsible.[25] Foreign persons committing the same statutory offenses are also penalized.[26] Corporations, partnerships, and

---

in the course of the performance of the services; and to information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit."

[19] Implementing rules and regulations of the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (2016).

[20] *Id.* at § 3(h).

[21] Implementing rules and regulations of the Data Privacy Act of 2012, Republic Act No. 10173, § 3 (m) (2016)

[22] Rep. Act No. 10173, § 3 (j).

[23] This is consistent with the principle of accountability provided under the DPA, to wit:

"SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request."

[24] *Id.* at §11.

[25] *Id.* at § 14.

[26] *Id.* at § 34.

any juridical persons, are still liable for monetary penalties ranging from five hundred thousand pesos (PhP 500,000) to four million pesos (PhP 4,000,000). For penalties of imprisonment, the penalty shall be imposed upon the responsible officers. Further, the court may suspend or revoke any of the offending party's rights under the law.[27] If the offender is a foreigner, he or she may be deported in addition to the penalties.[28]

1.2.3. Legal Parameters and Standards for Processing Personal Data

The law grants data subjects transparency and data autonomy rights over their personal information. The Controller is responsible for making sure that these rights are respected and that mechanisms are in place to ensure that these rights may be exercised. In particular, data subjects are accorded with the right to be informed whether personal information pertaining to him or her is being processed. The data subject should be furnished by the Controller with information containing (i) the description of the personal information being entered into a system; the purposes for which the data is being or to be processed; (iii) the scope and method of the processing; (iv) the recipients or classes of recipients to whom they are or may be disclosed; (v) the methods utilized for automated access; (vi) the identity and contact details of the personal information controller; (vii) the period for which the information will be stored; and (viii) the existence of the data subject's rights (such as the rights to access, correction, and the right to lodge a complaint before the Commission).

The foregoing rights are relevant in relation to the lawful processing of personal information. The presence of the information described in the immediately preceding paragraph is required in order to establish that the Controller procured the consent of the data subject.

Consent is only one legal criterion for processing, but is not the only legal basis in order for a Controller to validly process data. The Controller may process data without the consent of the data subject if (i) the processing is necessary and is related to the fulfillment of a contract with the data subject; (ii) the processing is necessary for compliance with a legal obligation; (iii) the processing is necessary to protect vitally important interests of the data subject, including life and health; (iv) the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or (v) the processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed.[29]

However, for data categories that are considered as "sensitive personal information,"[30] processing by digital platforms for commercial purposes will generally be prohibited except if the data subject gave his or her consent, specific to the purpose of the processing.

---

[27] *Ibid.*

[28] *Ibid.*

[29] Rep. Act No. 10173, §12 (f) provides that this processing of personal information on the basis of legitimate interest will not be valid if "such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution."

[30] Rep. Act No. 10173, § 3 (k). Sensitive personal is defined under the DPA as: "personal information: (i) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (ii) 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

Digital platforms may oftentimes collect a slew of personal information which are usually associated with registration information such as name, address, and contact details. The platform may also process device information, transaction information, and other data related to the use of the data subject of the platforms. At times, it may also include sensitive personal information, such as birthdays, health information (for health tech apps), or government IDs, as part of its operations. The collection of sensitive personal information is usual during the onboarding process or during the facilitation of payments or logistics services. To prevent fraudulent transactions, platforms will sometimes require the submission of copies of the government identification cards of users. To allow said platforms to process all of these data categories, the platform must therefore get the explicit consent of its users, specific to the purposes for the processing.

Getting the consent of the data subject is not a straightforward matter. There are standards which must be met in order for consent to be deemed valid and legal. Consent must be freely given, specific, informed indication of will, where the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Implied consent, therefore, is not valid under the law. Since the law requires that consent be specific, the consent form published by platforms must describe in granular detail the following information: the data categories processed, the manner by which it will be processed, and the purposes as to why it is being processed.

The Commission advises that acceptance or rejection in bulk, or "bundled" consent "will generally not suffice as the data subject is not empowered to make a true choice."[31]

1.3. Limitations on Cross-Border Transfer of Data

Subject to the possible application of other regulations for financial and government data, the DPA does not prohibit the transfer of personal information to foreign jurisdictions. Note that the DPA enables cross-border enforcement of data privacy protection,[32] and the DPA provides for extraterritorial application in cases where the processing of personal information is about a Philippine citizen or resident, the processing entity has a link with the Philippines and/or has a branch, agency, office, or subsidiary in the country.[33] The DPA does not have specific rules on data localization. However, due the accountability principle where the Controller is held responsible for data that is processes, the Controller must ensure that the rights provided by the DPA to data subjects and the obligations imposed on Processors are observed.

Parenthetically, various government agencies are given auditing, visitorial, and examining powers under the law. This includes the Bangko Sentral ng Pilipinas, the Secretary of the Department of Labor and Employment, and the Bureau of Internal revenue.***[34]*** By these grants of auditing powers, it can be inferred that the data, systems, and records of entities falling under the jurisdiction of these Government offices, must be made accessible to the said authorities.

---

of any court in such proceedings; (iii) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (iv) Specifically established by an executive order or an act of Congress to be kept classified."

[31] National Privacy Commission Advisory Opinion No. 2018-013.

[32] Rep. Act No. 10173, § 7(q).

[33] *Id.* at § 6.

[34] National Internal Revenue Code, as amended by R.A. No. 10963, § 270.

The Controller must therefore ensure that its offshore subcontractors will allow the relevant government agencies to conduct an audit when so requested.

1.3.1. Sector-Specific Regulations on Cross-Border Data Transfers

Some types of personal data will be governed by sector-specific regulations, in addition to the DPA.

Government-held data. Data processed by government entities is governed by the Cloud First Policy of the Department of Information and Communication Technology. Under this issuance, the "benefits of [cloud storage] are best realized when there [are] no data residency restrictions placed on data."[35] However, the same policy classifies data stored into three (3) tiers, each entailing storage in an accredited public cloud or private cloud deployment, and security and encryption requirements.[36]

Financial Data. The BSP also regulates data processed by banks and other BSP-supervised financial institutions (BSFIs). The BSP prohibits the outsourcing of inherent or core banking functions and prevents banks, therefore, from transferring data related to certain functions to offshore locations. The term "core banking functions" would include the taking of deposits from the public, granting of loans and other credit exposures, managing of risk exposures, and the general management of Central Bank-supervised entities. Relative to this, entities supervised by the Central Bank are required to conduct audits of its service providers offshore. It also mandates that in case offshore outsourcing is permitted, this extends only to service providers operating in jurisdictions which uphold confidentiality.[37]

BSFIs, such as banks, must also comply with the regulations on using cloud computing.[38] In addition, the BSP requires BSFIs to exercise a certain level of diligence when engaging cloud service providers or other outsourced services providers.

Overview of Rules on Data Localization in Selected Countries in the ASEAN

1.4. Regional Data Protection Structures

There are a number of international and regional frameworks for data protection. However, not all countries have data protections legislation or regulations in place. According to data from the United Nations Conference on Trade and Development (UNCTAD),[39] out of sixty (60) countries that UNCTAD considered in Asia and the Pacific, thirty-four (34) countries or fifty-seven percent (57%) have some form of data protection legislation, six (6) countries or ten percent (10%) have draft legislations, sixteen (16) countries have no data protection legislation, and four (4) countries have no data. 3 of the 6 countries with no data protection legislation are

[35] Department of Information and Communications Technology Circular No. 2017-002.
[36] *Ibid.*
[37] Bangko Sentral ng Pilipinas Circular No. 899, s.2016.
[38] BSP Manual of Regulations on Banks, Appendix 78.
[39] United Nations Conference on Trade and Development. N.d. Data Protection and Privacy Legislation Worldwide, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed on 2 July 2020).

members of the ASEAN: Cambodia, Brunei Darussalam and Timor-Leste. Myanmar has a draft data protection legislation that has yet to be enacted.

The foregoing statistic is interesting when juxtaposed with the number of existing international frameworks that countries in Asia are parties to.

The United Nations Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights recognize the right to privacy. In 2013, the United Nations General Assembly adopted a resolution[40] on privacy rights in the digital age.

The Organization for Economic Cooperation and Development ("OECD") issued its Privacy Guidelines[41] as early as 1980. The OECD Privacy Guidelines was updated in 2013 and upholds certain principles with regard to data protection: (i) there should limits to the collection of personal data; (ii) personal data should be relevant to the purposes for which they are to be processed; (iii) the purposes for which personal data are collected should be specified; (iv) personal data should not be processed for purposes that are not authorized; (v) personal data should be protected with reasonable safeguards; (vi) there should be a general policy of openness about developments, practices and policies with respect to personal data; (vii) individuals should be given certain rights over their personal data; and (viii) the data controller is accountable for ensuring the data protection principles are complied with.

With regard to cross border transfers, the OECD Privacy Guidelines recommends the adoption of certain measures to foster international cooperation among regulators. The OECD Privacy Guidelines provide that the measures should enable each member country to enforce data protection laws, enable individuals who are harmed by data protection legislation to have redress in all jurisdictions relevant to the specific violation, and regularly interface to consider adjustments to each of their domestic frameworks to further cross-border cooperation. The OECD also launched the Global Privacy Enforcement Network (GPEN), an informal network of public law enforcement authorities responsible for enforcing data protection laws and regulations. The GPEN is intended to provide a space for law enforcement entities to regularly interface and share information on issues, trends, cooperate and participate in various training activities.

In the Asia Pacific, the APEC Privacy Framework encourages the improvement of the interoperability of privacy frameworks to facilitate information flows. With regard to cross-border transfers, the Framework provides general policy directives that instructs members to formulate rules that allow the recognition of cross-border rules across jurisdictions. The rules adopted by members should also encourage responsible transfers of data across jurisdictions with minimal regulatory burden.[42]

The APEC Cross Border Privacy Rules system (the "CBPR system") was then endorsed by APEC leaders in order to implement the Privacy Framework. The CBPR system is "a voluntary accountability-based scheme to facilitate privacy-respecting data flows among APEC

---

[40] United Nations. 2014. General Assembly Resolution 68/167, *The right to privacy in the digital age,* A/RES/68/167. https://undocs.org/pdf?symbol=en/a/res/68/167 (accessed on 5 July 2020).

[41] Organisation of Economic Cooperation and Development. 2013. The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris, France: OECD.

[42] Asia-Pacific Economic Cooperation. 2015. Privacy Framework. Singapore, Singapore: APEC.

economies.".[43] The CBPR has four main components: (i) set criteria for bodies to become recognized as CBPR system accountability agents; (ii) a process for information controllers to be certified as APEC CBPR system compliant; (iii) assessment criteria for use by recognized accountability agents when reviewing whether a controller is compliant with CBPR requirements; (iv) arrangements for enforcing CBPR system requirements through complaints processes provided by accountability agents.[44] Nonetheless, only a handful of countries[45] agreed to join the APEC CBPR System. The CBPR System provides a certification mechanism that may serve as a seal of privacy compliance. Note that among ASEAN countries, only the Philippines and Singapore joined the CBPR.

Through the World Trade Organization ("WTO"), an international framework that could function to limit the ability of states to implement arbitrary and unreasonable data protection policies that hinders data transfers and data sharing. The WTO General Agreement on Trade and Services (GATS) recognized that countries may implement measures to uphold the privacy rights of individuals when it comes to the processing of personal information of the latter. However, the GATS also provides that such measures must not result in regulations that have the effect of enabling arbitrage or discrimination between member countries. Such measures should also not have the effect of becoming trade barriers.[46]

1.5. Divergent Data Protection Policies

Despite the international agreements and frameworks described in the foregoing section, national legislation on data protection still diverge. There is a recognition that each country approaches the subject of data protection differently. A legal report[47] made the observation that data protection policies of each country are driven by different motivations: some treat data as a data sovereignty, national security, big-data driven economy issue (the "Chinese Model"); some recognize privacy as a fundamental human right (the "European Model"); and some treat data protection regulation through liberal and market-driven approach (the "American Model"). The three models may be concurrently applied in one region, thus making it difficult to achieve a supranational method of regulating data.

1.6. Cross-Border Data Transfers

All jurisdictions with data protection legislation, in principle, allow cross-border transfers of data provided that certain conditions are met (consent, adequacy, etc.). However, the legal standards for data transfers vary among jurisdictions. Some jurisdictions, for example require consent before the data of a data subject is exported to another jurisdiction; while some jurisdictions require that the receiving country is part of a whitelist drafted up by the regulator before data may be exported. The standards as to what constitutes as valid consent also vary from state to state.

---

[43] Asia-Pacific Economic Cooperation. 2015. Privacy Framework. Singapore, Singapore: APEC.
[44] *Ibid.*
[45] As of 9 March 2020: the Philippines, the United States, Mexico, Canada, Japan, Republic of Korea, Singapore, Taipei,China, and Australia.
[46] World Trade Organization. 1994. General Agreement on Trade in Services. Geneva, Switzerland: WTO.
[47] Asian Business Law Institute. 2018. Regulation of Cross-Border Transfers of Personal Data in Asia. Singapore, Singapore: ABLI. https://abli.asia/UploadPDF/DP_Compendium_May_2018.pdf (accessed on 5 July 2020).

A study involving selected countries,[48] documented in a Working Document[49] published by the Asia Business Law Institute ("ABLI") in May 2020, compiled the standards required under the regulations of certain countries for data transfers to other jurisdictions. An abridged version quoting portions of the comparative table and findings of the ABLI and its researchers are compiled below. The table demonstrates how standards for data transfer are implemented differently in each country.

Table 1: Legal Standards for Data Transfers (selected countries)[50]

Jurisdiction and Data Protection Regulation	**Consent**	**White Lists, Adequacy Findings**
Australia Privacy Act (1988), Australian Privacy Principle 8.1 Accountability Principle. Before an entity discloses personal information to an overseas recipient, the entity must 'take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information.' S16C: If an entity discloses personal information about an individual to an overseas recipient and APP 8.1 applies to the disclosure of the information, the entity is accountable for any acts or practices of the overseas	Yes (optional) The accountability principle in APP 8.1 does not apply where the individual consents to the cross-border disclosure after the entity informs the individual that APP 8.1 will no longer apply (APP Guidelines at para. 8.27 ff.). Consent means 'express consent or implied consent' (Privacy Act s 6(1)).	No.

[48] The study considered the regulations in Australia, People's Republic of China, Hong Kong, China, India, Indonesia, Japan, Macau SAR, Malaysia, New Zealand, Philippines, Singapore, Republic of Korea, Thailand, and Viet Nam.

[49] Asian Business Law Institute. 2020. Comparative Table of Laws and Regulations on Cross-Border Personal Data Flows in Asia. Singapore, Singapore: ABLI. https://cdn2.hubspot.net/hubfs/5955262/Comparative%20Table%20of%20Laws%20and%20Regulations%20on%20Cross-Border%20Personal%20Data%20Flows%20in%20Asia_.pdf?utm_campaign=ABLI%20ebook&utm_medium=email&_hsmi=88671899&_hsenc=p2ANqtz--jcyH3PXxd4aZDWUWBWeuum5gy8c4lAnFcCYH_l0uIemV8FFupw9t5isRycNHTPzwKTfbZjh0qOj8j32TCEJOIo6R7OQ&utm_content=88671899&utm_source=hs_automation (accessed on 3 July 2020).

[50] Ibid., p. 6-15.

Jurisdiction and Data Protection Regulation	Consent	White Lists, Adequacy Findings
recipient that would breach the APPs in relation to the information.		
Indonesia Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), Art 26 Regulation No.20 of 2016 of the Ministry of Communication and Information (MCI 20/2016), Arts 21 and 22 Principle: Electronic System Providers ('ESPs') may transfer data only with the individual's consent; and following 'coordination with the Ministry' (in the current case the Ministry of Communication and Information, or 'Kominfo'). The coordination requirement seems closer to a notification requirement than to a prior authorisation but sometimes regulatory scrutiny is applied.[51]	Yes (required) The written consent of the 'data owner' is required unless specific regulations apply (MCI 20/2016, Art 21(1)). Express opt-in is not explicitly required by Art 21(1) but is derived from MCI 20/2016, Art 1(4).	Uncertain It is not known if the Ministry would assess the level of protection in certain countries (e.g. countries with data protection laws) in the context of the coordination provided in MCI 20/2016 Art 22.
Malaysia Personal Data Protection Act 2010 Data transfers outside Malaysia may in principle take place only to places specified by the Minister where there is in force any law which is substantially similar to, or that serves the same purposes as the PDPA or which ensures an adequate level of protection which is at least equivalent to	Yes (optional) Consent may operate as an exception to the requirement that transfers may take place only to places specified by the Minister (s 129(2)(a)).	Yes The Minister, upon the recommendation of the Commissioner, may specify any place outside Malaysia to where data may freely flow

[51] Ibid., citing Danny Kobrata, 'Jurisdictional Report: Indonesia', in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), p. 151.

Jurisdiction and Data Protection Regulation	Consent	White Lists, Adequacy Findings
the level of protection afforded by PDPA.		
New Zealand Privacy Act 1993 International transfers are permitted, as long as the legal requirements in the privacy principles and appropriate conditions for privacy protection are observed. However, in exceptional circumstances the Privacy Commissioner may prohibit a transfer to another State when: - The personal information has been received from another State and will be transferred to a third State where it will not be subject to a law providing comparable safeguards to the Privacy Act; and - The transfer would be likely to breach the basic principles of national application set out in the OECD Guidelines.	No Consent is neither optional nor required, and would not currently appear to waive the requirements of existing privacy safeguards in the country of destination.	No. The Privacy Act does not provide for the possibility to adopt 'white lists'. However, the Commissioner may prohibit a transfer 'if the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to this Act' and the transfer would be likely to lead to a contravention of the basic principles of national application.
Philippines Data Privacy Act of 2012 and its Implementing Rules and Regulations	Yes (Optional) Data may only be processed (includes transfer) if there is lawful criteria for doing so. Consent is one lawful criterion. The IRR provides that data sharing shall be allowed in the private sector if the data subject consents to the data sharing.	No The DPA does not recognize or consider the data protection regulations in the country of destination.
Singapore Personal Data Protection Act (PDPA), 2012	Yes (optional) The requirements of s 26 may be satisfied if the transferring organisation obtains the individual's consent to the	Conceivable The exporting organization must have taken "appropriate steps to ascertain whether, and to ensure that, the

Jurisdiction and Data Protection Regulation	Consent	White Lists, Adequacy Findings
s. 26: An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under PDPA	effect of transferring the data (Reg 9(3)(a)). Consent cannot be used to waive the requirement of existing privacy safeguards in the country of destination	recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act"
Thailand Personal Data Protection Act 2019 s. 28: Data transfers may freely take place to a foreign country or international organisation that have adequate data protection standards, and in accordance with the data protection rules prescribed by the Data Protection Committee. -- Exceptions to the 'adequacy' requirement apply in four series of circumstances: - the data subject's consent has been obtained; - specific statutory exemptions apply; - the receiving organisation provides suitable protection measures which enable the enforcement of the data subject's rights; or - the receiving organisation has put in place a 'Personal Data Protection Policy' app	Yes (optional) obtaining the data subject's consent will be one of the circumstances in which the data controller may derogate to the rule that transfers may take place only to a destination country or international organisation that has adequate data protection standards under PDPA. Where consent is obtained, data subject must be informed of the inadequate data protection standards of the destination country or international organisation. The conditions for obtaining valid consent are defined in the PDPA.	Conceivable When PDPA Chapter 3 enters into force, in the event that the data controller sends or transfers the personal data to a foreign country, unless an exemption applies, the destination country or international organisation that receives such personal data must have an 'adequate data protection standard', and the transfer must be carried out in accordance with the rules for the protection of personal data as prescribed by the Committee (s 28).

Gaps and Challenges in Existing Regulation

The structure of data protection regulatory frameworks, on a national and regional level, impacts digital platforms that have or may potentially have cross-border operations. Such regulations will also impact the privacy rights of data subjects.

1.7. Effect on Digital Platforms

1.7.1. Uncertainty and Divergence in Regulations as a Business Concern

Part III illustrates that there is no binding international framework which provides a single standard for legal data transfers among different jurisdictions in the region. Personal information will be regulated by each state individually.

Representatives from businesses across Asia mentioned compliance and adapting to new regulations as the biggest challenge facing Asian businesses in 2018.[52] An UNCTAD publication[53] cited certain concerns from businesses: "(i) too stringent protection regimes will unduly restrict, increase administrative burdens, and stifle innovation; (ii) a lack of clarity and computability between regimes add uncertainty, with negative effects on investments; and (iii) given the nexus between cross-border e-commerce and data protection, divergent regimes will inhibit the adoption and proliferation of emerging technological development, reducing potential accompanying societal benefits."

The variance in regulation is another layer of difficulty for digital platforms, especially small to medium enterprises that seek to enable cross-border transactions. The compliance process would be a multijurisdictional process that a platform has to go through. Compliance-driven platforms may therefore have to deploy resources to implement compliance processes, assess risk, and operate regionally.

The divergent, dynamic, and stringent compliance requirements in each jurisdiction require digital platforms to invest in compliance procedures to ensure that their activities are compliant with all applicable data protection legislation and regulations. The regulations in each country are still developing hence the compliance teams of digital platforms should be agile when considering changes in the rules vis a vis its operations. In jurisdictions that employ a consent-based regime and/or implement an accountability mechanism, significant resources must further be spent in order to conduct data processing audits and privacy impact assessments. A platform must understand and map out the extent of processing it conducts, the types of data it collects, and the purposes for which it processes data.

The digital platform should further ensure that its mechanism for procuring consent will be recognized and will be enforceable in all jurisdictions that require prior to data transfers. To illustrate, in the Philippines consent must be an affirmative indication of will and the data subject must be made to actively opt in. For a platform, implementing opt-ins may add a kink in the user experience by adding another step before the user may be onboarded or before the

---

[52] Baker McKenzie's Asia Pacific Business Complexities Survey 2017, "Simplifying Business in a Complex World: Business Challenges and Legal Solutions in Asia Pacific", as cited in Asia Business Law Institute, "Regulation of Cross-Border Transfers of Personal Data in Asia", (2018).

[53] United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development (2016).

user is allowed to make a transaction. This speedbump will entail additional costs to the platform as additional step may lead to a loss in transactions.

Actively monitoring the organization's compliance in multiple jurisdictions, or even in a single jurisdiction, will require platforms to invest in hiring a data protection officer and, in some cases, an entire data protection team.

1.7.2. Incentivizes Blanket Consent Forms

The divergence in data protection legislation may also lead to overbroad compliance measures from the digital platforms such as comprehensive consent forms.

Taking the Philippines as an example, note that the DPA requires controllers to be transparent to data subjects about all the details of its processing activities. Given the monetary and operational cost of having to revise the consent forms for each time that the Platform introduces a functionality or a purpose for the processing, the Controller may try to minimize cost by simply trying to cover all the potential processing activities that it will conduct. This encourages Controllers to cast a wide net of possible data categories that they may collect in the future, and purposes for the processing of said data. This leads to consent forms and privacy policies that are lengthy and oftentimes, legalese. This has a detrimental effect on the accessibility and readability of an organization's consent forms and privacy policies to the data subject.

4.1.3. Regulatory Arbitrage: Privacy Compliance vis a vis Regional Competitiveness

Data protection legislation and regulations may act as non-tariff trade barriers. As shown in Part III, countries have varying regulations despite the existence of overlapping international frameworks. The regulatory hurdles and operational limitations that a platform may be subjected to by a particular jurisdiction may persuade the said entity to shop for a business address in jurisdictions with less stringent data protection regulations.

For example, due to the cost of compliance and the amount of risk that platforms face when processing data in the Philippines, digital platforms may choose to either opt not to provide services to Philippine citizens and locate elsewhere. However, some platforms may simply try to avoid being subject to the DPA but still target the Philippine market and Philippine data subjects. In South East Asia, the Philippine market is appealing to platforms engaged in e-commerce and financial services due to the number of potential users that have access to the internet and mobile phones. Some platforms may still therefore choose to provide services to Filipinos and process the personal information of Filipinos even if such platforms are offshore. Despite the extraterritorial provisions of the DPA, the applicability and actual enforceability of the law are two different matters. It will be difficult for Philippine law enforcement agencies to subject offshore entities to their regulatory reach, without the cooperation of the affected jurisdictions.

1.8. Effect of the DPA on Data Subjects right to Privacy

*1.8.1. Empowering Individuals by **Providing a Broad Protection** for Personal Information*

Most of the data protection regulations of the countries cited in part III provides a blanket coverage for all personal information and for all persons processing personal information. The Philippine DPA, for example, generally does not provide exemptions on the basis of organizational structure, size, or income. This regime may provide greater privacy protection as it will be difficult for entities to try and circumvent the law in order to escape coverage. In contrast the data protection regime in the United States is governed through different sector-specific regulations (generally limited to health data regulations and consumer protection regulations).

For data subjects and the general public, the explicit grant of certain rights under data protection legislation gives data subjects more control over how their personal information is being processed. The greater transparency and autonomy operationalizes the constitutional protection to one's privacy. At the same time, this may also lead to greater trust for businesses that are compliant with such regulations.

The breadth of the scope of the law forces digital platforms to rationalize how they handle data and actually conduct privacy impact assessments with the objective of mapping out their data processing activities. The transparency requirements of the law require platforms to disclose, in very granular detail, the types of data collected, how these are being processed, the purposes for such processing, details on retention and deletion, and details on how the same is shared. The difficulty of making and managing such disclosures will force digital platforms to only process data as may be necessary for its operations.

Compliance requirements and the possibility of legal liability and enforcement action will lead Controllers to review and draft internal data processing policies more carefully. The accountability provisions in some jurisdictions and heavy penalties are also disincentives against unscrupulous collection and handling of data.

1.8.2. Effectiveness of Self-Management of Privacy rights; Legal Exploitation of Data

Legal scholars[54] have discussed the shortcomings of regulations that are designed based on the expectation that the data subjects can sufficiently and rationally manage their own privacy rights.

As forwarded by Professor Daniel Solove, privacy self-management assumes that the data subject is in a position to fully understand the extent of the processing activities conducted regarding his or her personal information, and is thus able to properly consent to the same. He argues that from a cognitive standpoint, it would be unreasonable to assume that a normal person has the capacity to effectively manage his or her privacy rights, given the language in which policies are written, the context in which he or she is making the decision of whether or

---

[54] See Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review 1880–1893 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018&download=yes (last visited Apr 29, 2020) where he argues that although privacy self-management is certainly a necessary component of any regulatory regime, it is being asked to do work beyond its capabilities.

not to consent. From a structural standpoint, there is also the problem that any single individual will be using and accessing numerous online services (websites, applications, and other services) and will thus be subject to voluminous privacy policies. To compound the problem, a data subject is also expected to make the decision early on, upon the initial collection of the data. At this point the data subject may not be in a position to fully understand the extent of processing activities that may happen to his personal data.[55] The difficulty of effectively being informed about how personal is processed is magnified by the method by which individuals usually access privacy policies or consent forms which is done through mobile devices.

It should further be noted that consents forms for platform services are generally given on a take-it-or-leave it basis, leaving consumers with no real opportunity to negotiate the details of how his or her data should be processed.

In the context of the Philippines, compliance with the Philippine DPA may lead to a digital platform publishing privacy policies and consent forms that are lengthy and legalese. The requirements of the DPA necessitate the enumeration of all types of data points processed, all the types of processing activities that will be done to the data and the purposes behind the processing of each data category. It also requires the personal information controller to disclose how the data will be stored, how it will be deleted or destroyed. Should the data be shared, the personal information controller must explain what data categories will be shared, what the purpose of the sharing is, and to what entities it will be shared. The law also requires the controller to inform the data subject about the latter's privacy rights and how said data subject may exercise it against the controller. Complying with all of these will require a lawyer, working with the controller operations and tech team, to draft a very detailed document. This trend has led one legal scholar[56] to refer to privacy policies as "surveillance policies."

One study estimated it would cost $781 billion in lost productivity if a person were to read every privacy policy at websites he or she visited in a one-year period.[57] In his book Code Version 2.0, Larry Lessig explains, "Cluttering the web with incomprehensible words will not empower consumers to make useful choices as they surf the Web. If anything, it drives consumers away from even attempting to understand what rights they give away as they move from site to site." The weakness therefore of a consent-based regime is that it may actually enable the legal exploitation of personal data.

To address this issue, regulators may explore forwarding additional guidelines and best-practices as to how consent forms should be presented, taking into account its effect on user experience and balancing it with the interest of the data subject in actually understanding what he or she is assenting to.

---

[55] *Id.,* at 1883-1893.

[56] Zuboff, S. 2020. *The Age of Surveillance Capitalism: The Fight For A Human Future at the New Frontier of Power.* New York: Public Affairs.

[57] McDonald, A.M., Cranor, L.F. 2008. The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society.*

Moving Forward

1.9. Macro Policy Considerations

There is a need to push for stronger intergovernmental and regional data protection frameworks. It may not be feasible to propose uniform data protection legislation among the countries in the region due to the difference in policy considerations and policy rationale surrounding the value of data and the purpose data protection.

A more viable approach in the short to medium term may be to focus on intergovernmental mechanisms that will facilitate the cross-border transfer of data, instead of lobbying for a general and comprehensive international data protection regime. This may include promoting cooperation among each country's enforcement authorities responsible for data protection; instituting mechanisms that will allow data subjects to enforce data protection rights in all relevant jurisdictions where an injury or data breach occurs; and pushing for uniform certification standards for controllers, similar to the existing mechanism provided under the APEC CBPR, to make data transfer standards more objective and predictable.

Efforts should also be made in eliminating data transfer restrictions for data categories that are necessary to facilitate digital platform transactions, with due consideration to each particular country's national security considerations. This may be read together with the policy statements of the WTO in the GATS which respects the rights of countries to implement certain restrictions on data provided that the forms of such restrictions do not result in discrimination among countries or in trade barriers.

5.2. Towards a More Malleable Regulatory Regime

Regulators and international bodies should also consider how each country's data protection legislation and regulation may affect digital platforms and other emerging technologies. Regulating technologies that are continuously developing is difficult. The regulator must balance the need to protect the public and the need to ensure that legislation and regulation do not have a chilling effect on innovation. The details of data protection rules need not be determined by legislation and may instead be ironed out in other instruments.

To carefully navigate this, the regulators may consider implementing light-touch regulatory approaches for specific types of technologies that involve the processing of data, alongside more general data protection legislation. This may be done through the use of various regulatory tools that provide oversight such as best practices guidelines, warnings and advisories, official speeches, interpretations, and meetings with regulated parties. This allows the government to supervise developments in certain industries while observing how the tech will develop and affect consumers. Intergovernmental organizations may also consider issuing uniform guidelines and best practices suggestions. Regular interface among data protection regulators will help in this regard.

The regulators may also consider adopting and issuing rules for regulatory sandboxes. Regulatory sandboxes are limited frameworks set up by regulators in order to allow certain, pre-qualified entities to soft-launch their products in controlled environments. This may be particularly helpful for AI and Internet of Things technologies with regard to how these systems process data and affect the data subjects. This will allow the regulator to understand the industry sought to be regulated without preempting developments in the same.

Bibliography

Asian Business Law Institute. 2020. Comparative Table of Laws and Regulations on Cross-Border Personal Data Flows in Asia. Singapore, Singapore: ABLI. https://cdn2.hubspot.net/hubfs/5955262/Comparative%20Table%20of%20Laws%20and%20Regulations%20on%20Cross-Border%20Personal%20Data%20Flows%20in%20Asia_.pdf?utm_campaign=ABLI%20ebook&utm_medium=email&_hsmi=88671899&_hsenc=p2ANqtz--jcyH3PXxd4aZDWUWBWeuum5gy8c4lAnFcCYH_l0uIemV8FFupw9t5isRycNHTPzwKTfbZjh0qOj8j32TCEJOIo6R7OQ&utm_content=88671899&utm_source=hs_automation (accessed on 3 July 2020).

Asian Business Law Institute. 2018. Regulation of Cross-Border Transfers of Personal Data in Asia. Singapore, Singapore: ABLI. https://abli.asia/UploadPDF/DP_Compendium_May_2018.pdf (accessed on 5 July 2020).

Asia-Pacific Economic Cooperation. 2015. Privacy Framework. Singapore, Singapore: APEC.

Bangko Sentral ng Pilipinas Circular No. 899, s.2016.

Department of Information and Communications Technology Circular No. 2017-002.

Google & Temasek / Bain. 2019. E-Conomy SEA 2020.

Implementing Rules and Regulations of Rep. Act No. 10173.

McDonald, A.M., Cranor, L.F. 2008. The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society.*

National Internal Revenue Code, as amended.

National Privacy Commission Advisory Opinion No. 2018-013.

National Privacy Commission (NPC). 2020. NPC Suspends GRAB PH'S Selfie Verification, Audio, Video Recording Systems. Pasay City, Philippines: NPC. https://www.privacy.gov.ph/2020/02/npc-suspends-grab-phs-selfie-verification-audio-video-recording-systems/ (accessed on 15 July 2020).

National Privacy Commission (NPC). 2019. Order: Violations of the Data Privacy Act by Several Companies Operating Online Lending Applications. Pasay City, Philippines: NPC. https://www.privacy.gov.ph/2019/10/order-violations-of-the-data-privacy-act-by-several-companies-operating-online-lending-applications/ (accessed on 15 July 2020).

Organisation of Economic Cooperation and Development. 2013. The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris, France: OECD.

Republic Act No. 10173. Data Privacy Act of 2012.

Republic Act No. 11055. Philippine Identification System Act.

Solove, D. 2013. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126: 1880-1893.

United Nations. 2014. General Assembly Resolution 68/167, *The right to privacy in the digital age*, A/RES/68/167. https://undocs.org/pdf?symbol=en/a/res/68/167 (accessed on 5 July 2020).

United Nations Conference on Trade and Development. 2016. Data Protection Regulations and International Data Flows: Implications for Trade and Development. Geneva, Switzerland: UNCTAD. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed on 2 July 2020).

United Nations Conference on Trade and Development. N.d. Data Protection and Privacy Legislation Worldwide, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed on 2 July 2020).

United Nations Conference on Trade and Development. 2016. Global Investment Trend Monitor. Geneva, Switzerland: UNCTAD. https://unctad.org/system/files/official-document/webdiaeia2016d3_en.pdf (accessed on 10 May 2020).

World Trade Organization. 1994. General Agreement on Trade in Services. Geneva, Switzerland: WTO.

Zuboff, S. 2020. *The Age of Surveillance Capitalism: The Fight For A Human Future at the New Frontier of Power.* New York: Public Affairs.