CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

ASEAN *Ideas in Progress* Series

4/2021

June 2021

"Bite the Bullet: The Future of Data Protection Law and Policy in ASEAN"

Jonathan Lim

Space Generation Advisory Council
Space & Cybersecurity Project Group

Bite the Bullet: The future of Data protection law and policy in ASEAN

Abstract

This paper examines and presents an updated perspective regarding the need for an overarching regional data protection and privacy regulation for ASEAN in driving the open, free, and cross-border flow of data. This is contextualized by ongoing regional initiatives, the state of data protection and privacy laws across ASEAN Member States, and the utility of a stable legal and policy framework in advancing digital transformation, economic integration, and development across Southeast Asia.

This centres upon an analysis of prior confidence building measures, high-level discussions on data privacy laws and regulations, and review of data protection laws across individual ASEAN jurisdictions. Policymakers may draw inspiration from the European Union's General Data Protection Regulation (GDPR), pursue the development and adoption of best practices for digital data governance, and adhere to a 3C cooperative framework in driving greater cooperation and coherence across ASEAN.

The findings of this paper will assist ASEAN policymakers and academics in highlighting existing barriers to the harmonization of laws and regulations, and advancing the creation of best practice guidelines on data protection and privacy. The paper is distinguished in its intent to provide an updated legal, regulatory, and policy perspective regarding the ongoing progression toward a formative ASEAN data protection and privacy regulation.

Keywords: Cybersecurity, Digital Transformation, ASEAN, Data Protection, Privacy,

==========

Introduction

The continuing fragmented approach of Southeast Asian jurisdictions in the face of digital transformation and the Fourth Industrial Revolution (4IR) presents a significant challenge toward the promotion of digital integration, and in closing the significant economic and social developmental gap between ASEAN Member States. Policymakers must expedite regional development through the creation of a comprehensive data protection and privacy regulation across ASEAN. The adoption and harmonization of legal, regulatory, and policy approaches to data protection and privacy must thus be recognized as a core policy concern within regional discussions concerning economic development. This will place ASEAN in an ideal position to develop, share and adopt best practices, while also and undertaking progressive policies that promote interoperable mechanisms for cross-border data flows, facilitate the growth of digital economies, and protect the personal data of their citizens.

The importance of laws and frameworks pertaining to data protection and privacy are centred upon the recognized need to govern, manage, and regulate the exchange, use, and storage of data by all sectors of society – encompassing the government, private sector, and individuals. This has emphasized the importance of Consumer Data Rights (CDR) in providing data subjects with greater control over their data, the proper handling of Personally Identifiable Information (PII), and the need for mandatory reporting in the event of data breaches.[1]

[1] Office of the Australian Information Commissioner, 'What is the Consumer Data Right?' on Australian Government (2021) <https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right/>.

These requirements are driven by the growing impact of the digital economy and disruptive technologies in driving economic development and digital transformation across ASEAN nations, combined with the ever-increasing volume of cybercrime. As of July 2019, 416 million out of the Southeast Asia's population of 662 million were identified as active Internet users, while the region registered 853 million mobile phone subscriptions. Indeed, Internet penetration in ASEAN is 63% while mobile penetration is 129%, though the latter is concentrated in urban areas.[2] The digital market has since come to represent 7% of the region's $2.8 trillion GDP.[3] Consequently, the average cost of a security breach in 2020 was estimated to have risen to $2.71 million per organization across ASEAN.[4]

Closing the development gap among ASEAN Member States has concentrated upon promoting deeper integration and development both between and among Cambodia, Lao PDR, Myanmar, and Vietnam (CLMV).[5] One of the most critical tasks facing the CLMV countries is that of effectively leveraging the opportunities and benefits offered by disruptive technologies, and in advancing toward sustainable development as part of the wider 4IR phenomenon. The potential for CLMV to strategize and pursue the potential of disruptive technologies in driving economic growth and social welfare is limited by their relative low regulatory and policy capabilities vis-à-vis data protection and privacy, requiring a novel and reflexive approach which accounts of the unique nature of disruptive technologies. This raises the possibility of an inclusive and multi-stakeholder regulatory model for data protection and privacy based upon a principle-based approach – ensuring that regulatory decisions are more open-ended and subject to new knowledge and input from stakeholders across the public and private sectors.[6]

The drive toward interstate concordance over a harmonized legal and regulatory digital data environment within ASEAN is premised upon its significant implications for the integration and utilisation of 4IR technologies and processes (Artificial Intelligence (AI), Big Data, Blockchain), capacity to elevate the region's economic capabilities and boost integration into the global economy, and relevance to good governance and reinforcing trust in government institutions. Free data flow across borders benefits both people and economies by facilitating trade opportunities, investment innovation, development and growth, and productivity. However, in the absence of clear policy directions and leadership, it is noted that greater connectivity and digital transformation can also expose ASEAN members to a greater risk of cyberattacks, cyber threats, and privacy breaches.[7] Consequently, increased knowledge about an organization/government's data, coupled hand-in-hand with advances in data governance and privacy, plays a key role in positioning ASEAN members for greater digital transformation.

[2] Ibid, 2.
[3] US Mission to ASEAN, 'Growing ASEAN's Digital Economy' on US Mission to ASEAN (August 2020) <https://asean.usmission.gov/wp-content/uploads/sites/77/IGNITE-Digital-Economy-fact-sheet-Aug2020.pdf>.
[4] James Henderson, 'Data breaches cost ASEAN businesses $2.71M' on Channel Asia (2 August 2020) <https://www.channelasia.tech/article/681831/data-breaches-cost-asean-businesses-minimum-2-71m/>.
[5] Ching-Fu Lin and Han-Wei Liu, *Disruptive Technologies and Sustainable Development: Implications for Southeast Asia* (ICTSD, 2018) iv.
[6] Ibid, 11.
[7] US Mission to ASEAN, above n3, 2.

Context

Background

There have been wider ongoing policy efforts by regional governments to promote regulatory reform promoting the digital economy. Firstly, the *ASEAN Economic Community Blueprint 2025,* which was adopted during the 27th ASEAN Summit in November 2015.[8] The Blueprint commits ASEAN members toward embracing and leveraging evolving digital technologies in enhancing trade and investments, providing an e-based business platform, promoting good governance, and facilitating the use of sustainable technologies. This is underlined by the need to develop measures to protect personal data, as conducive to a coherent and comprehensive framework for personal data protection, in the advancement of Information and Communications Technology (ICT) and e-commerce. Second, the *ASEAN Digital Integration Framework*, which was adopted during the 51st ASEAN Economic Ministers Meeting in September 2019. The Framework calls upon ASEAN members to adopt digital economy regulations consistent with global rules and standards, to develop open application interface standards with financial institutions, and develop national digital identification to enable real-time and secure user verification.

Alongside numerous international frameworks, which have influenced the development of national data privacy legislations across the region to date,[9] over the past decade a concerted effort emerged to develop a bespoke and overarching data protection and privacy framework for ASEAN. The progression and evolution of this regional effort can be explained across several core regional frameworks.

Firstly, the *2016 ASEAN Framework on Personal Data Protection* (PDP) established a set of guiding principles concerning the implementation of national and regional measures to promote personal data protection. Here, the ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) recognized that "a harmonized legal and regulatory digital data environment within ASEAN plays a vital role in generating business confidence and stimulating economic growth".[10] Policymakers also recognized that the creation of an ASEAN Data Protection Forum can "facilitate the sharing of knowledge and operational know how by policy makers and regulators, which will help ASEAN Member States that do not have a personal data protection authority in setting up their respective authorities".[11] The Framework is thus interpreted as assuming a vital role in helping ASEAN Member States implement appropriate domestic laws and regulations aligned with global standards, thereby promoting global trade and the flow of information.

Second, the *2018 ASEAN Framework on Digital Data Governance* (DDG) – a continuation of the 2016 PDP seeking to enhance data management, facilitates the harmonization of data regulations across ASEAN members, and promote the intra-ASEAN flows of data.[12] Senior officials across specific ASEAN Member States were tasked with the development and implantation of four recognized strategic priorities of digital data governance under the Framework, to enhance digital capability and cooperation among ASEAN Member States and support the ASEAN digital economy. These strategic priorities are:

I. Data Lifecycle and Ecosystem – Establishing principles on data integrity and trustworthiness, data use and access control, and data security. This would be achieved through an ASEAN Data Classification Framework.

[8] ASEAN, 'ASEAN Economic Community' on ASEAN (2021) <https://asean.org/asean-economic-community/>.
[9] OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data (1980, 2013); APEC Privacy Framework (2015).
[10] *2016 Framework on Personal Data Protection*, ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) (16 November 2016) [27].
[11] Ibid, [33].
[12] National Privacy Commission, 'PH leads ASEAN's move to protect privacy' on National Privacy Commission (22 August 2019) <https://www.privacy.gov.ph/2019/08/ph-leads-asean-move-to-protect-privacy/>.

II. Cross Border Data Flows – Promoting the enactment of principles on cross border data flows which maximises the free flow of data, fosters a vibrant data ecosystem, and mandate necessary protections. This would be achieved through an ASEAN Cross-Border Data Flows Mechanism.

III. Digitalization and Emerging Technologies – Promoting principles on capacity development which incorporate capacity building and the provision of necessary resources for stakeholders. This would be achieved through an ASEAN Digital Innovation Forum.

IV. Legal Regulatory and Policy – Intended to promote principles on personal data protection and privacy regulation, accountability, and the development and adoption of best practices. These would be advanced under hosting of an ASEAN Data Protection and Privacy Forum.

Above all, ASEAN governments were encouraged to balance their need for data protection and privacy regulations against any potential adverse impacts upon cross border data flows. Member States should avoid adopting measures which impact data innovation and the fostering of a vibrant data ecosystem across ASEAN.

Third, the *2021 ASEAN Data Management Framework* (DMF), which was approved at the first ASEAN Digital Ministers' Meeting (ADGMIN). The DMF signals a continuing commitment among ASEAN Member States toward the development of legal, regulatory, and policy advancements supportive to data-related business operations in the region. The DMF seeks to supply businesses with key resources to utilise data-related business operations, encompassing guidance in the creation of a data management system, data governance structures and safeguards, and good data management practices.[13] The creation of a bespoke data management framework enables ASEAN businesses to better unlock the value of data while enhancing data safeguards, while also making cross border data transfers more efficient and secure.[14] It is envisioned that the DMF will gradually facilitate consensus on the legal and regulatory strategic priorities of the DDG through the promotion of harmonized legal and regulatory landscapes, and the development and adoption of best practices for private businesses, serving as a precursor to wider regional-level regulations and guidelines.

At the regional level, the adoption of these three frameworks symbolizes several important trends:

I. a solidification of ASEAN's commitment to strengthening personal data protection through multilateral cooperation;
II. a response to the rising threat of cybercrime and data breaches upon businesses and individuals;
III. growing opposition to the power held by international technology conglomerates, and the dangers posed by social media upon individual privacy and social stability[15];
IV. the accelerating pace of digital transformation and economic integration across the region;[16] and,
V. growing recognition over the free flow of data as one of the primary drivers of economic development and digital transformation in ASEAN.

Regardless of its scopes, intentions and content, these frameworks do not constitute an overarching or uniform regulatory framework for data protection and privacy. Under the lens of international law, these

[13] Rajah & Tann Asia, 'Data Management for Businesses: Launch of ASEAN Data Management Framework and Model Clauses on Data Transfer' on Lexology (2 February 2021) <https://www.lexology.com/library/detail.aspx?g=8d070e4b-5817-42de-bd54-c17159af8571>.
[14] PDPA, 'ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows' on PDPA (22 January 2021) <https://www.pdpc.gov.sg/Help-and-Resources/2021/01/ASEAN-Data-Management-Framework-and-Model-Contractual-Clauses-on-Cross-Border-Data-Flows>.
[15] Eileen Yu, 'Facebook 'deeply concerned' about Singapore directive to block access' on ZDNet (18 February 2020) <https://www.zdnet.com/article/facebook-deeply-concerned-about-singapore-directive-to-block-access/>.
[16] KEARNY, 'The ASEAN digital Revolution' on KEARNY (24 November 2015) <https://www.nl.kearney.com/digital-transformation/article/?/a/the-asean-digital-revolution>.

documents, as “frameworks”, are not considered legally binding international agreements and to not create rights or obligations for ASEAN Member States. Consequently, adherence to these frameworks is predicated upon voluntary participation by ASEAN governments based on consultation and consensus, with members encouraged to provide regular updates on their progress of implementing the framework at the working group level. Subsequent non-compliance by any participating member state does not result in any penalties or consequences as these documents lack the necessary enforcement required for their broad adoption and are not conducive to promoting a rules-based digital order in ASEAN.

Benefits of an overarching data privacy regulation

Within an increasingly data-driven world the benefits of an overarching regional comprehensive data protection are numerous.[17] This is due to the growing utility of data as the "new oil" – providing insights into people's behaviours, the development of new and beneficial products and services through data manipulation, enabling governments and companies to exert influence over individuals,[18] and driving wider economic development and digital transformation.

In advocating for a regional framework for data protection and privacy, policymakers must comprehend the typology of data privacy regulation types.[19] Firstly, data collection regulations outline how and when businesses can collect data about consumers, and in notifying users when their data is being collected. Second, data breach regulations hold businesses accountable to certain measures in the event of a data breach, including notifying customers and agencies, and enacting precautions to prevent a repeat of such incidents in the future. Third, data access regulations specify how internal access of information should be handled and providing consumers with appropriate levels of access. Fourth, data storage regulations govern how data must be stored, and the nature of security concerning data storage. Fifth, data privacy training regulations provide for a requisite level of competence among staff concerning matters of data privacy.

The consideration and consolidation of these regulations under an overarching general data protection and privacy regulation bears tangible benefits for small-to-medium enterprises in promoting the equitable, secure, and free flow of data across ASEAN. Firstly, improved consumer confidence in organizations as the custodians of data:[20] the adoption of an established overarching data protection and privacy regulation provides organizations with a robust data governance system and responsible practices, enabling the fair and consumer friendly commerce and the provision of services while facilitating smoother and more efficient operations. Second, improved data security aligns an organization's security practices and cyber resilience in accordance with best practice frameworks. Third, there will be reduced maintenance costs with the reduced need to hold and manage customer data contributes to lower compliance cost and infrastructure maintenance. Fourth, effective management of the growing demand for data, and the ability to offer customers augmented goods and services will promote better alignment with evolving and emergent technologies. Finally, it would mean for improved decision-making processes where the implementation of a right to obtain human intervention in managing an individual's data promotes transparency, accountability, and decreases room for arbitrary decisions.

For governments and civil society, the implementation of an overarching general data protection and privacy regulation gives rise to several noted benefits from a policy perspective. First, driving innovation and entrepreneurship within the economy. The establishing of rules that protect the intellectual property rights of those who develop innovative products and services increases the propensity to innovate and file patents.[21] Second, implementation contributes to the advancement of human rights in restricting the ability of governments to spy on people without due cause, limiting the ability of groups from using an individual's personal data for their own goals, and in protecting freedom

[17] Katrin Sarap, 'Three reasons why we need strict data protection regulations' on Njord Law (9 February 2018) <https://www.njordlaw.com/three-reasons-why-we-need-strict-data-protection-regulations>.

[18] Samuel Legen, 'How much is your data worth to tech companies? Lawmakers want to tell you, but it's not that easy to calculate' on The Conversation (11 July 2019) <https://theconversation.com/how-much-is-your-data-worth-to-tech-companies-lawmakers-want-to-tell-you-but-its-not-that-easy-to-calculate-119716>.

[19] Jingcong Zhao, 'Understanding Data Privacy and Why It Needs to Be a Priority for Your Business' on Hyperproof (5 February 2020) <https://hyperproof.io/resource/understanding-data-privacy/>.

[20] Open Access Government, 'The five key business benefits of GDPR' on Open Access Government (16 April 2018) <https://www.openaccessgovernment.org/the-five-key-business-benefits-of-gdpr/44554/>.

[21] Francesco Banterle, 'The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis' in M. Bakhoum (eds.) et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer, 2018) 411.

of speech and thought.[22] Third, it promotes data residency: where the storage or retention of personal data within ASEAN ensures that data is processes in accordance with the common laws, customs and expectations of ASEAN. This helps companies based in ASEAN satisfy their customers' privacy concerns, improves national security, and contributes to faster data processing times.[23]

[22] Human Rights Careers, '10 Reasons Why Privacy Rights are Important' on Human Rights Careers (2021) <https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/>.
[23] Peter Day, 'Data across borders: The importance of data residency' on VentureBeat (3 October 2019) <https://venturebeat.com/2019/10/03/data-across-borders-the-importance-of-data-residency/>.

Analysis - Jurisdictional Frameworks

To date, only four ASEAN countries have data protection laws and have established a data privacy authority regulator. Enduring economic disparity, combined with differing rates of digital adoption and the widening algorithmic divide, continues to hamper the capacity and will of many ASEAN countries to adopt data protection laws. Other ASEAN members such as Indonesia are in various stages of developing their own data protection and data privacy laws. Consequently, a cursory review of laws and regulations across the more advanced economies of Singapore, Malaysia, and the Philippines highlights key differences across ASEAN jurisdictions regarding data protection and privacy, and demonstrates ongoing challenges hindering the harmonization of data regulations across the region.

Singapore

The key legislation in Singapore is the *Personal Data Protection Act 2012* (PDPA), of which the regulator is the Personal Data Protection Commission (PDPC). The PDPA provides a baseline standard of protection for personal data in Singapore, comprising various requirements governing the collection, use, disclosure, and care or personal data.[24] The PDPC may initiate an investigation to determine compliance with the PDPA, during which they carry the authority to request the production of any specified document or information, enter an organization's premises without warrant and with advanced notice, and to review complaints in relation to access and correction requests.[25]

The PDPA's application extends extraterritorially to cover organizations involved in the collection, use or disclosing of personal data in Singapore, regardless of their geographical location or registration status in Singapore. Most notably, the data protection obligations do not apply to any public agency, to whom separate rules under the *Instruction Manual for Infocomm. Technology and Smart Systems Management* (IM8) and the *Public Sector (Governance) Act 2018* apply.

Concerning the cross-border transfer of data, an organization in Singapore which deals with personal data may transfer such data overseas if it complies with the PDPA's requirements while in a third party's possession, and where the recipient is bound to provide protections comparable to that afforded under the PDPA.

Furthermore, it is mandatory for eligible organizations under the PDPA to appoint a Data Privacy Officer (DPO) as responsible for ensuring their compliance with the Act. The failure to appoint a PDO can result in an investigation by the PDPC and may result in financial penalties of up to SGD$100,000 for an organization.

Recent changes to the PDPA include the adoption of an Amendment Bill in November 2020, coming into effect in February 2021.[26] The Bill strengthens organizational accountability and consumer protections through the introduction of a new mandatory breach notification regime, expands the scope of deemed concept, and provides for a new right of data portability for individual data subjects.[27]

Malaysia

The core legislation on personal data protection in Malaysia is the *Personal Data Protection Act 2010* (MPDP),[28] to which the regulator is the Personal Data Protection Commissioner. The MPDP was

[24] PDPC, 'PDPA Overview' on PDPC (2021) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>.
[25] Drew & Napier LLC, 'Q&A: the data protection legal framework in Singapore' on Lexology (28 August 2020) <https://www.lexology.com/library/detail.aspx?g=63abc7b6-1b8f-4809-9d5c-8e261475dd3a>.
[26] Ashurst, 'Amendments to Singapore's Personal Data Protection Act' on Ashurst (12 November 2020) <https://www.ashurst.com/en/news-and-insights/legal-updates/amendments-to-singapore-s-personal-data-protection-act/>.
[27] PDPC, 'Amendments to the Personal Data Protection Act (PDPA) Take Effect From 1 February 2021' on PDPC (29 January 2021) <https://www.pdpc.gov.sg/news-and-events/announcements/2021/01/amendments-to-the-personal-data-protection-act-take-effect-from-1-february-2021>.
[28] Nadarashnaraj Sargunaraj, *Personal Data Protection in ASEAN* (ZICO Law, 2020).

introduced to strengthen consumer confidence in business transactions and e-commerce. The Commissioner carries the power to investigate, inspect data users' personal data system, access computerized data, and search and seize data both with and without a warrant.[29]

The MPDP applies to any person who processes and has control over the processing of any personal data in respect of commercial transactions. The MPDP also applies to data users using equipment in Malaysia for the processing of personal data, otherwise than for the purposes of transit through Malaysia. Additionally, the MPDP requires several classes of data users to register for an annual certificate authorizing the processing of personal data under the MPDP, including those involved in communications, banking and financial institutions, insurance, health, tourism and hospitalities, transportation, education, direct selling, services, real estate, utilities, pawnbrokers, and moneylenders.[30]

Concerning the cross-border transfer of data, a data user cannot transfer personal data to a location outside of Malaysia without the data subject's explicit consent, unless that organization is on a whitelist specified by the Minister, or where exceptions apply under the MPDP. Such exceptions include that the transfer is necessary for the performance of a contract with the data subject, that the data user has undertaken due diligence to ensure processing in line with the MPDP, and where the transfer is necessary to protect the data subject's interest.

Consequently, registrable organizations are not required to appoint a DPO, and there is no requirement under the MPDP for data users to notify authorities regarding data breaches in Malaysia. However, ongoing review of the MPDP under the *Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020)* of February 2020 is considering the introduction of an obligation to appoint a DPO, and is also reviewing the introduction of requirements to report data breaches.

Philippines

The *Data Privacy Act 2012* (PDA)[31] represents the governing law on data privacy matters in the Philippines. The PDA represents a comprehensive legislative instrument designed to protect the fundamental human right of privacy, while ensuring the free flow of information to promote innovation. This is reinforced by the *Implementing Rules and Regulations of the DPA* (IRR) adding specificity to the PDA, which came into force in September 2016.

The PDA is enforced by the National Privacy Commission (NPC), which possesses the authority to perform all necessary acts to enforce its orders, including issuing compliance orders, awarding indemnities on matters affecting the personal data or rights of data subjects, issue cease and desist orders, referring cases to the Department of Justice for prosecution, compel entities to abide by its directions on data privacy matters, and impose administrative fines.[32]

The PDA applies to the processing of personal data by any natural and juridical person in the government or private sector, and may also apply extraterritorially if certain links exist to the Philippines. The PDA applies to businesses with offices in the Philippines, when an entity utilises equipment based in the Philippines is used for processing, and to entities involved in the processing of the personal information of Philippines citizens regardless of where they reside.[33]

[29] Robert Healey, 'The Malaysia Personal Data Protection Act 2010 – All you need to know (Part 1)' on FORMITI (6 January 2021) <https://formiti.com/the-malaysia-personal-data-protection-act-2010-all-you-need-to-know-part-1/>.

[30] DLA Piper, 'Data Protection Laws of the World - Malaysia' DLA Piper (2021) <https://www.dlapiperdataprotection.com/index.html?c=MY&t=law#>.

[31] *Data Privacy Act 2012* (Republic Act No. 10173).

[32] DFDL, 'Data Protected – Philippines' on Lexology (4 May 2020) <https://www.lexology.com/library/detail.aspx?g=0f0ece6e-9fc3-41be-bb21-570b5df0a9b3>.

[33] Alex Wall, 'Summary: Philippines Data Privacy Act and implementing regulations' on iapp (27 April 2017) <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/>.

Concerning the cross-border transfer of personal data, the PDA does not restrict such actions. However, the personal information controller remains responsible for the personal information under its control, and where such information is transferred to a domestic/international third party.[34]

Finally, the PDA requires the appointment of a DPO by personal information controllers and personal information processors.[35] The DPO is accountable for the organization's compliance with the PDA, and their identity must be disclosed to data subjects upon request. There are no legislated penalties relating to the incorrect appointment of a DPO, and no restrictions on the citizenship and residency of the DPO.

[34] DLA Piper, 'Data Protection Laws of the World – Philippines' on DLA Piper (29 December 2020) <https://www.dlapiperdataprotection.com/index.html?c=PH&t=law#>.
[35] National Privacy Commission, 'Appointing a Data Protection Officer' on National Privacy Commission (2021) <https://www.privacy.gov.ph/appointing-a-data-protection-officer/>.

External influences Upon A Data Protection and Privacy Framework

In assessing the viability of an overarching framework, policymakers must consider how ongoing international and regional developments have impacted the region's data protection and privacy frameworks, and the current prospect of an overarching ASEAN data protection regulation. This follows the unprecedented effects of the COVID-19 pandemic upon the rate of digital transformation in ASEAN, the prospect of closer trade and economic integration across Indo-Pacific nation within recent regional trade agreements, and the growing influence of China over the region.

COVID-19

The COVID-19 pandemic has accelerated the rate of digital transformation and adoption, while highlighting issues of public trust surrounding the nature of data protection and privacy regarding emerging technologies. During the pandemic, an increasing number of governments around the world have sought to employ technology-based solutions to combat the spread of COVID-19, leveraging Big Data in the use of contact tracing applications as a means of bolstering epidemiology efforts.[36]

The pandemic has also resulted in a dramatic update of digital technologies across ASEAN Member States. The *e-Conomy SEA 2020 Report*[37] highlighted that 40 million people across Southeast Asia came online for the first time in 2020, boosting the number of Internet users from 250 million to 400 million between 2015 to 2020, and equating of 70% of the region's population being online. Further, the region's Internet economy exceeded $100 billion in 2020, and is expected to reach $300 billion by 2025. The underlying explanation for this phenomenon can be traced to the surging use of e-commerce platforms, food delivery apps, online media, and digital financial services accelerating the pace of digital transformation and adopted which was originally predicted to take several years.[38] Consequently, 33% of those surveyed by the report indicated that they began using a new online service, with 94% intending to continue the use of such services beyond the pandemic.

The impact of the pandemic has been more pronounced among the youth population. A survey conducted by the World Economic Forum highlighted that 9 out of 10 young people between the ages of 16 and 35 across ASEAN have increased their use of at least one digital tool during the pandemic, while 45% declared that they had picked up at least one new digital tool. From this, approximately 50% said that their experience of the pandemic had educated them to be more resilient in the future, while 38% said they had learned to think more creatively.[39]

Within this new vibrant digital landscape, the question persists whether existing data protection and privacy safeguards under the ASEAN frameworks are sufficient to protect the privacy and interests of data subjects within the COVID-19 paradigm, while also enabling the free flow of data and innovation throughout ASEAN. While the increasing amount of data required from the public improves the accuracy and effectiveness of such technology, this has given rise to serious concerns over the privacy of data subjects and the importance of trust between the government and data subjects. This was

[36] Benjamin Chiang, 'How can data governance drive economic advantage for Southeast Asia?' on EY (11 June 2020) <https://www.ey.com/en_sg/government-public-sector/how-can-data-governance-drive-economic-advantage-for-southeast-asia>.

[37] Google and TEMASEK, Bain & Company, 'Google e-Conomy SEA 2020' on Google (2020) <https://economysea.withgoogle.com/>.

[38] Sebastian Strangio, 'In Southeast Asia, COVID-19 Speeds Transition to Digital Technologies' on The Diplomat (11 November 2020) <https://thediplomat.com/2020/11/in-southeast-asia-covid-19-speeds-transition-to-digital-technologies/>.

[39] Douglas Broom, 'Young people in ASEAN have emerged from lockdowns more resilient and digitally switched on. Here's how' on World Economic Forum (8 October 2020) <https://www.weforum.org/agenda/2020/10/young-people-asean-digital-adoption-covid-19/>.

highlighted in Singapore by the lack of clarity by the government over the purpose and use of personal data acquired by the government's contract tracing initiatives – TraceTogether and SafeEntry.[40]

While this period of rapid digital adoption and transformation has sparked interest within the ASEAN Economic Community to accelerate the region's digital integration in order to boost regional recovery in the post-COVID19 period, it is recognized that the harmonization of regulation among ASEAN Member States presents a significant roadblock to further progress.[41] Additionally, the growth in distance education and remote working has highlighted the need for organizations to elevate their data security and privacy posture, in precluding the borderless and evolving nature of cybercrimes.[42] Finally, ASEAN governments must resolve to build public trust in safeguarding the data and privacy of their citizens by acting with transparency and accountability.

The Regional Comprehensive Economic Partnership

The adoption of the *2020 Regional Comprehensive Economic Partnership* (RCEP)[43] highlights the commitment of signatories to improve international trade and commerce, with a noted focus on telecommunications, e-commerce, cybersecurity, and the free flow of data across borders. The agreement was signed between all ten members of ASEAN and China, Japan, South Korea, Australian and New Zealand—with the intent to eliminate a range of tariffs on imports over the next two decades.[44]

The document references free data flows under Chapter 12 on Electronic Commerce,[45] resolving that "the parties shall consider current and emerging issues such as the treatment of digital products, source code, and cross-border data flow and the location of computing facilities in financial services." Accordingly, the agreement focuses on the enhancement of the digitalization of trade by increasing the level of trust and confidence of e-commerce users through several data protection and privacy measures:[46] firstly, the enactment of regulations on the protection of personal data and protection of e-commerce users from fraud and misleading practices; second, maintaining the current practice of not imposing customs duties for electronic transmissions between Member States; third, prohibiting the requirement to use or locate a computing facility in a certain territory to conduct business in that territory; and fourth, prohibiting the prevention of cross-border transfer of information, unless otherwise provided to achieve public policy objectives and protect security interests.[47]

The multilateral nature of the RECP presents a compelling framework for continuing ASEAN regional cooperation in promoting the free flow of data and innovation through international trade and commerce. However, it must be emphasized that the character of the RCEP represents a blueprint for a reduction in tariffs in Asia, rather than an architectural framework for the development of an overarching data

[40] Kristen Han, 'Broken promises: How Singapore lost trust on contact tracing privacy' on MIT Technology Review (11 January 2021) <https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/>.
[41] Huawei, 'ASEAN to Accelerate Digital Integration for Post-COVID Economic Recovery' on Huawei (10 December 2020) <https://www.huawei.com/en/news/2020/12/asean-digital-connectivity-digital-transformation-covid19-pandemic>.
[42] EXECASSIST, 'Data protection is a key in a COVID-19 environment: IBM Security' on ASEAN Tech & Sec (2 September 2020) <https://aseantechsec.com/data-protection-a-key-in-a-covid-19-environment-ibm-security/>.
[43] Department of Foreign Affairs and Trade, 'RCEP text and associated documents' on Australian Government (15 November 2020) <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/rcep/rcep-text-and-associated-documents>.
[44] Tim McDonald, 'What is the Regional Comprehensive Economic Partnership (RCEP)?' on BBC (16 November 2020) <https://www.bbc.com/news/business-54899254>.
[45] Article 12.16: Dialogue on Electronic Commerce.
[46] Chian Voen Wong et al., 'Asia-Pacific Signals Strong Commitment to Economic Integration and Cooperation with RCEP Signing' on K&L Gates (9 December 2020) <https://www.klgates.com/Asia-Pacific-Signals-Strong-Commitment-to-Economic-Integration-and-Cooperation-with-RCEP-Signing-12-9-2020>.
[47] Ivy Tan and Wu Di, 'Understanding the Regional Comprehensive
Economic Partnership Agreement (RCEP)' on Baker McKenzie (2 December 2020) <bakermckenzie.com/-/media/files/insight/publications/2020/12/bakermckenzie_understandingrcep_dec2020.pdf?la=en>.

protection and privacy regulation.[48] The primary objective of such trade agreements is the reduction of tariffs and regulations, rather than the imposition of legal duties and obligations upon data administrators, the inclusion of which is necessary for an effective and enforceable data protection and privacy framework in ASEAN.

China's Influence

The steady rise in digital trade and commerce between ASEAN members states and China draws attention to the potential influence and guidance which Beijing may provide in the creation of an overarching ASEAN data protection and privacy regulation. Between January to October 2020, China-ASEAN bilateral trade volume amounted to $571.64 billion. This surge in conventional trade has contributed to deepened cooperation in the digital economy, including online cross-border shopping, online education, and telemedicine.[49]

As one of the leading nations driving the development of digital infrastructure and the digital economy in the region, China has become an important partner to ASEAN. This was highlighted during the November 2020 ASEAN-China Digital Economy Cooperation Conference in Chengdu, involving the publicizing of policies and exchanging of opinions concerning new growth points across the fields of digital and industrial cooperation including smart cities, AI, and Big Data. The conference saw Chinese officials herald 2020 as the ASEAN-China Year of Digital Economy Cooperation, focusing upon economic revitalization, social development, increased employment, the improvement of people's livelihood, and the development of the Belt and Road Initiative cooperation under the Digital Silk Road (DSR). [50]

Further cooperation in digital and cybersecurity affairs with China was demonstrated during the first ASEAN-China Cyber Dialogue in December 2020.[51] The dialogue referenced the Initiative on Building ASEAN-China Partnership on Digital Economy—following the 23rd ASEAN-China Summit[52]—concerning the significance of the digital economy to regional development, and the enduring commitment of both sides to an open, secure, stable, accessible and peaceful ICT environment. Consequently, both sides resolved upon the continuing importance of data security to national security and expressed the desire to collaborate in strengthening the region's data security ecosystem.

Consequently, recent developments within China's domestic legislation may bear some relevance. This concerns the October 2020 *Draft Personal Information Protection Law* (PIPL),[53] representing the country's first comprehensive law on the protection of personal data. The law was created following the growing need to protect the personal information of Chinese citizens, given its importance for economic development. The draft PIPL's main features include extraterritorial application, data residency, requirements for consent of a data subject, and individual rights and control over the processing of personal information.

[48] Riad Ajami, 'The Regional Comprehensive Economic Partnership: Asia Trade Connectedness' (2020) *Journal of Asia-Pacific Business* 1-3.

[49] Xinhua, 'Economic Watch: China, ASEAN forge deeper digital economy cooperation' on Xinhuanet (13 November 2020) <http://www.xinhuanet.com/english/2020-11/13/c_139514351.htm>.

[50] ASEAN-China Centre, 'The 2020 ASEAN-China Digital Economy Cooperation Conference Successfully Held in Chengdu' on ASEAN-China Centre (9 November 2020) <http://www.asean-china-center.org/english/2020-11/5474.html>.

[51] Ministry of Foreign Affairs of the PRC, 'Co-Chairs' Statement on the 1st ASEAN-China Cyber Dialogue' on Ministry of Foreign Affairs of the PRC (16 December 2020) <https://www.fmprc.gov.cn/mfa_eng/wjbxw/t1840666.shtml>.

[52] ChinaDaily, 'Speech by Chinese Premier at the 23rd China-ASEAN Summit' on ChinaDaily (13 November 2020) <https://www.chinadaily.com.cn/a/202011/13/WS5fad6e7ca31024ad0ba93c17.html>.

[53] Taft Stettinius & Hollister LLP, 'China's Personal Information Protection Law (PIPL) - Data Privacy in the Land of Big Data' on Lexology (13 January 2021) <https://www.lexology.com/library/detail.aspx?g=db4592e2-53c1-4cb6-91a9-94da1ee14b26>.

An assessment of China's potential influence upon ASEAN's digital future requires reference to China's Cyber Diplomacy and vision of cyber sovereignty. China is a strong advocate for control over cyberspace and the Internet within its own borders, and expresses the desire to build a coalition of like-minded nations favourable to state-centric models of international cyber governance.[54] Further, from a geopolitical perspective, the potential for China to spur disagreements between ASEAN Members States and disrupt the established data privacy frameworks benefits its wider ambitions to extend and strengthen its influence over the region.[55] Bolstered by its digital diplomacy and DSR initiatives, Beijing will likely seek to promote an integrated view of cyber sovereignty vis-à-vis data protection and privacy through its engagements with ASEAN, seeking to prioritize its laws and regulations as the ideal model for promoting the free flow and data and innovation. Alternatively, Beijing may seek to contribute its ideas and contentions on the formation of a formative data protection and privacy regulation applicable to ASEAN members, but to which Beijing is not subject. Finally, Beijing may promote the balkanized development of data protection and privacy laws across individual ASEAN Member States while opposing the development of an overarching regional regulation, pursuing a strategy of divide and conquer mirroring its wider "salami-slicing" strategic actions in the South China Sea.

[54] Nokolay Bozhkov, 'China's Cyber Diplomacy: A Primer' on EU Cyber Direct (9 March 2020) <https://eucyberdirect.eu/content_research/chinas-cyber-diplomacy-a-primer/>.

[55] Cissy Zhou and Finbarr Bermingham, 'China's Asean influence sets stage for new superpower battleground with US, as the ball shifts to Biden's court' on SCMP (13 December 2020) <https://www.scmp.com/economy/china-economy/article/3113620/chinas-asean-influence-sets-stage-new-superpower-battleground>.

Key Policy Challenges

Harmonizing Legal and Regulatory Landscapes

Firstly, the differing status of data protection and privacy laws and regulations across individual ASEAN jurisdictions presents significant barriers to the formation of an overarching ASEAN regulation. An analysis of the legislative and administrative approaches adopted by Singapore, Malaysia and the Philippines reveals key differences across the privacy enforcement bodies and the scope of their authority, the application and reach of privacy laws across governments and private entities, the cross-border transfer of data, and penalties for non-compliance.

Among the most significant differences is that of the powers afforded to the administrative body tasked with enforcing the legislation. In Singapore, the PDPC carries a wide range of coercive powers which enable it to enter upon a premise without a warrant, while in the Philippines the NPC is limited to legal and administrative options for non-compliance. Further, in Singapore the PDPA has only recently enacted a mandator data breach notification regime, while Malaysia and the Philippines have yet to implement such requirements.

The varying enforcement capabilities, cultural attitudes, and legal/governance systems of each ASEAN government has therefore resulted in the organic development of such differences. There thus exist significant regulatory challenges to the creation of an interoperable and overarching data protection and privacy framework across ASEAN. Additionally, the high cost of regulatory conformity and the continuing lack of capacity by ASEAN Member States present significant hurdles to harmonisation.[56] In such a diverse region, the state of digital transformation within each ASEAN Member State varies significantly, which is further highlighted by the significant difference in GDP per capita between its most advanced and least developed Member States.

The enforcement of a uniform and comprehensive 'one-size-fits-all' framework of laws and regulations will prove unaffordable, unfeasible, and impractical for many CLMV states to comply and enforce upon their domestic markets. This is given the anticipated high cost of implementation, and the skills and expertise required to manage the process. Where the CLMV countries have not yet established independent data privacy enforcement authorities, this has not detracted from their interest in further training and assistance to better understand regional data privacy frameworks such as the Asia-Pacific Economic Cooperation (APEC).

It is noted that the ASEAN PDP and the DDG Frameworks have promoted capacity building efforts, including workshops and seminars, to impart ASEAN Member States with the knowledge and skills necessary to develop personal data protection policies. Organisations such as the Asia Business Law Institute (ABLI) have consolidated support from governments and non-governmental stakeholders to conduct in-depth research and produce knowledge products around the regulation of international data transfers, privacy, and data protection across the region.[57] Consequently, ASEAN governments are conducting more consultations with stakeholders that serve as critical mechanisms to share information. Over time, as data privacy becomes an increasingly important realm of policy, it will be accorded additional priority and resources.

[56] GSMA, *Regional Privacy Frameworks and Cross-Border Data Flows - How ASEAN and APEC can Protect Data and Drive Innovation* (GSMA, 2018)

[57] Asian Business Law Institute, 'Convergence of data privacy laws and frameworks for cross-border transfers of personal data in Asia' on Asian Business Law Institute (2021) <https://abli.asia/Projects/Data-Privacy-Project>.

Cybersecurity Maturity

The formation of an overarching data protection and privacy framework in ASEAN is contingent upon the cybersecurity maturity level, and overall cyber resilience, of individual ASEAN Member States. Cybersecurity has a direct bearing upon both the government and local institutions' abilities to implement effective information security safeguards and ICT governance frameworks, conducive to meeting minimum standards of data protection and privacy. Consequently, ASEAN has emphasized the importance of a secure and connected regional information infrastructure within the ASEAN Economic Community 2025 Blueprint. [58]

During the COVID-19 pandemic, the rapid rise of cybersecurity threats targeting governments and organizations underscored the importance of an overarching framework on data protection and privacy. The Cyber Security Agency of Singapore (CSA) indicated that between 2018 and 2019, the number of cybercrime cases increased by 51.7% from 6,215 to 9,340 cases.[59] These developments highlighted two persisting issues in ASEAN's cybersecurity efforts: 1) the lack of sufficient spending on cybersecurity and cyber resilience measures;[60] and 2) the continuing lack of reporting surrounding cybersecurity incidents.[61]

In meeting these shortfalls, ASEAN governments must elevate their cyber capabilities through the following four-point agenda, as part of the ideal regional cybersecurity defense playbook.[62] Firstly, elevate cybersecurity on the regional policy agenda: there must be concerted effort and coordination in driving the implementation of a rapid action cybersecurity framework, and cybersecurity must be elevated to the top of the agenda in economic dialogue by the ASEAN Economic Community. Second, secure a sustained commitment to cybersecurity: ASEAN ministers must pursue a commitment to addressing the regional cybersecurity spending gap between Member States, while also defining and tracking cybersecurity metrics through a publicly accessible cyber-hygiene dashboard. Third, fortify the cyber ecosystem: policymakers must foster a risk-centric mindset in the corporate sector, promote a culture of sharing threat intelligence concerning cyber threats, extend cyber resilience across the supply chain, and implement regional public-private partnerships. Fourth, build-up the next wave of cybersecurity capabilities: policymakers must commit to funding education and developing the next generation of information security professionals. This requires a strengthening of their individual domestic cybersecurity industries through collaboration with global players, driving research and development, and emphasise transforming ASEAN into an anchor for world-class cyber expertise and capabilities.

[58] CCDCOE, 'Association of Southeast Asian Nations' on CCDCOE (2021) <https://ccdcoe.org/organisations/asean/>.

[59] Davina Tham, 'Cybercrime jumps more than 50% in 2019, new threats emerge from COVID-19 pandemic' on CNA (26 June 2020) <https://www.channelnewsasia.com/news/singapore/cybercrime-jumps-more-than-50-2019-new-threats-covid-19-csa-12872818>.

[60] John J. Brandon, 'Why ASEAN Needs to Invest More in Cybersecurity' on The Asia Foundation (9 May 2018) <https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/>.

[61] Leo Lin, 'COVID-19's Impact on Cybersecurity in ASEAN' on Atlas Institute of International Affairs (26 August 2020) <https://www.internationalaffairshouse.org/covid-19s-impact-on-cybersecurity-in-asean/>.

[62] KEARNY, 'Cybersecurity in ASEAN: An Urgent Call to Action' on KEARNY (23 January 2018) <https://www.southeast-asia.kearney.com/web/southeast-asia/article?/a/cybersecurity-in-asean-an-urgent-call-to-action>.

ASEAN Governance Shortfalls

The most significant persistent shortfall in governance and cooperation between ASEAN Member States is tied to the defining style and nature of ASEAN regional cooperation.[63] First, while steady engagement and confidence building has served to reduce conflict among members, this contributes to a lengthened decision-making process. Second, while the emphasis on the principle of non-interference in the internal affairs of member countries has fostered mutual trust and respect between members, it also hinders the possibility of meaning institutional change and the advancement of human rights. Third, while economic cooperation represents a major focus of ASEAN, this must be pursued in a manner which avoids the emergence of serious disharmony between its Member States. Such a circumstance may constrain the undertaking of radical developmental initiatives and hinder trade, commerce, and innovation.

Most evident is the enduring impact of the "ASEAN Way" upon economic integration.[64] The "ASEAN Way" refers to several principles which collectively prevent organizational change, which can be reduced to two essential components: first, an emphasis upon decision making through informal consultation among diplomats, thereby facilitating group consensus at official meetings; and second, a series of six behavioural principles set forth in the *1976 Treaty of Amity and Cooperation*:[65] 1) respect for state sovereignty; 2) freedom from external interference; 3) non-interference in internal affairs; 4) peaceful dispute settlement; 5) renunciation of the use of force; and 6) cooperation. The combination of these principles has given rise to the notion of non-interference between ASEAN Member States in each other's internal affairs. It is this emphasis on the cooperative mechanisms of reciprocal consultation, unanimous consensus on decisions, and non-interference which forces the organization to adopt only those policies which satisfy the "lowest common denominator."[66] The consequences of the ASEAN Way are evident within the whole-of-ASEAN community response to the COVID-19 pandemic, resulting in insufficient and belated measures which failed to contain the spread of the virus.[67]

Consequently, the fate of regional economic integration and digital transformation in ASEAN has been fundamentally shaped by socio-political contestation over the distribution of economic power and resources.[68] At its core, the assumption of a technocratic response has resulted in an insufficient capacity to make and enforce regulations, deficiencies in institutional design, and inadequate political will. This entrenched resistance evident within ASEAN's cooperative mechanism can often only be overcome through very prolonged struggles, or when the severe socio-economic dislocation changes the balance of power between social forces. The potential for an overarching ASEAN data protection and privacy regulation therefore does not depend on institutional reforms, normative change or national leaders' political will. Rather, this is contingent upon struggles over the structural adjustments involved in each sector, and how historically contingent relations between dominant economic interests and ruling coalitions can shape what reforms are politically feasible.

[63] Frank Frost, 'ASEAN at 30: Enlargement, Consolidation and the Problems of Cambodia' on Australian Parliament (25 August 1997) <aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/CIB/CIB9798/98cib02>.

[64] Lee Leviter, 'The ASEAN Charter – ASEAN Failure of Member Failure?' (2009/10) 43(1) *International Law and Politics* 177.

[65] *Treaty of Amity and Cooperation in Southeast Asia Indonesia* (entered into force 24 February 1976) <https://asean.org/treaty-amity-cooperation-southeast-asia-indonesia-24-february-1976/>.

[66] Leviter, above n64, 161.

[67] Haridas Ramasamy and Wendy He, 'Coping with COVID-19 the ASEAN way' on East Asia Forum (10 July 2020) <https://www.eastasiaforum.org/2020/07/10/coping-with-covid-19-the-asean-way/>.

[68] Lee Jones, 'Explaining the failure of the ASEAN economic community: the primacy of domestic political economy' (2016) 29(5) *The Pacific Review* 647-670

Recommendations

The achievement of a regional overarching data protection and privacy regulation is predicated upon the capacity of ASEAN governments to and draw upon established international privacy frameworks, collectively improve data governance, and engage in cybersecurity capacity building. The question arises as to what elements of an anticipated data governance and privacy regulation are considered as critical or essential to a functioning and effective framework, and how policymakers can drive consensus and spark action between ASEAN Member States.

Insights from the European Union's (EU) GDPR

The contents and extraterritorial reach of the GDPR has predicated an accelerated effort among ASEAN countries to review or institute their own domestic data protection laws. The GDPR was adopted in 2016 and came into force in May 2018, replacing the Data Protection Directive. The regulation administers the usage of data of its citizens by companies in terms of data, privacy, security, and transparency, both domestically and extraterritorially. Where a directive allows for each EU member to adopt and customize the law to suit the needs of its citizens, a regulation requires the full adoption and application of the law as a binding legislative act across the EU.[69]

The GDPR outlines six data protection principles which involve a risk-based approach to data protection. This includes: 1) lawfulness, fairness and transparency; 2) purpose limitation; 3) data minimisation; 4) accuracy; 5) storage limitation; and 6) integrity and confidentiality. Compliance with these principles ensure that appropriate policies and procedures are in place to deal with the transparency, accountability, and individuals' rights provisions, and building a workplace culture of data privacy and security.[70] Following the GDPR's implementation, it was found that the regulation had boosted public awareness among EU citizens concerning data protection rules and their rights as data subjects. Businesses have similarly adapted and developed a compliance culture and were developing privacy as a competitive advantage, and there was also an upward convergence towards high data protection standards and safe data flows at international level.[71] Consequently, ASEAN policymakers may find benefit and common ground in drawing upon these six established data protection principles.

Additionally, the GDPR's unique approach to data localization requirements bears some relevance to the formation of an overarching ASEAN data protection and privacy regulation.[72] Firstly, policymakers must acknowledge that data localization requirements constitute barriers to trade in services. It is thus imperative to adopt measures encouraging ASEAN members states to abide by their existing services liberalization commitments. This is achievable by removing or moderating data localization requirements inconsistent with those commitments, and by avoiding the enactment of unnecessary localization requirements. Second, policymakers must clarify what legitimate public policy reasons justify derogations from the free flow of data. While this view is understandable vis-à-vis personal data, where cross-border transfers of personal data are subject to adequacy restrictions based on the need to protect individual privacy, the question of non-personal data must also be addressed. Third, ASEAN must establish strict standards on the justification of data localization requirements. Any data localization requirements imposed should be targeted so as not to excessively inhibit trade in services, innovation, and the free flow of data. This must be with the adoption of viable less-restrictive alternatives to data localization where possible.

[69] European Union, 'Regulations, Directives and other acts' on European Union (2021) <https://europa.eu/european-union/law/legal-acts_en#decisions>.

[70] Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' (2017) 59(6) *International Journal of Market Research* 703-705.

[71] Nathalie Vandystadt, 'General Data Protection Regulation shows results, but work needs to continue' on European Commission (24 July 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449>.

[72] Benjamin Wong, 'Data Localization and ASEAN Economic Community' (2019) 10 *Asian Journal of International Law* 178.

Adopting Good Digital Data Governance Practices

ASEAN must promote consensus and consultation upon the legal and regulatory strategic priorities of existing data protection and privacy frameworks, concentrated upon the development and adoption of good governance practices in the public sector. This impetus is supported by the contents of the DMF, wherein the need for governance and oversight represents one of the document's six foundational components covering the entire data life cycle. This requires the setting out of roles and responsibilities across an organization, designating who is responsible for implementing and executing good governance practices by ensuring adoption, operation, and compliance.[73] Reference to the Organisation for Economic Co-operation and Development (OECD) highlights an emphasis on promoting leadership and vision, developing a capacity for coherent implementation, and established regulations.

First is the strategic need to promote leadership and vision in data governance. Where data strategies are considered as an element of good data governance, they enable accountability and can help define leadership, expectations, roles and goals. The formulation of data policies and strategies can benefit from open and participatory processes, integrating and directing the inputs of actors and stakeholders from the public and private sectors toward greater policy ownership. This may incorporate elements for data openness and sharing by governmental Chief Data Officers (CDO), and within data policy, highlight milestones and timeframes within a data strategy while promoting the use of policy levers.

Second is the tactical need to develop capacities for coherent policy implementation. This involves the talking of development challenges in a holistic manner, developing mutually reinforcing policies across all sectors to achieve a shared objective.[74] This references the need for governments and private companies to find common business definitions across departments for critical data elements to avoid discrepancies.[75] Here, a thoughtfully designed data governance framework identifies these data elements, assigning them with common definitions and to appropriate stakeholders, improving accountability and reducing the occurrence of conflicts.

Third is the tactical need for the harmonising of legal and regulatory frameworks across ASEAN Member States. This calls for a concentrated and accelerated effort among CLMV countries to adopt data protection and privacy legislation. Data-related legislation and regulations help countries define, drive and ensure compliance with the rules and policies guiding data management, including data openness, protection and sharing From a domestic level, this will improve the capacity of the public sectors in CLMV countries to extract value from data assets, and highlighting the value of institutional networks and communities of practice as levers of public sector maturity and collective knowledge. From a regional level, this will feed into ASEAN's capacity to define, drive, and ensure compliance with existing data protection and privacy frameworks guiding data management (PDP, DDG, DMF), opening the way for further consensus on an overarching regulation.

[73] Gabriela Kennedy and Karen H.F. Lee, 'Finding Harmony – ASEAN Model Contractual Clauses and Data Management Framework Launched' on Mayer Brown (8 February 2021) <https://www.mayerbrown.com/en/perspectives-events/publications/2021/02/finding-harmony-asean-model-contractual-clauses-and-data-management-framework-launched>.

[74] OECD, 'Policy coherence for sustainable development' on OECD (2021) <http://www.oecd.org/gov/pcsd/>.

[75] Chiang, above n36.

3C Cooperative Framework

At the regional level, the 3C cooperative framework represents a specific condition beneficial to managing governance and driving cooperation among ASEAN Member States. There is a clear convergence among ASEAN Member States to embrace the free and cross-border flow of data. The realization of a concrete outcome requires adoption of an overarching 3C framework based upon cross-sectoral consortium, capacity building measures, and communication.[76]

Concerning cross-sectoral consortium, the common participation of organizations across the public and private sectors in data protection and privacy-focused endeavours can contribute to the harmonization of laws and regulations across jurisdictions.[77] First is the safeguarding intra-ASEAN and international transfers of data. Interoperability should be a key factor when assessing data governance in ASEAN, which encompasses transfers within ASEAN and vis-à-vis other jurisdictions (i.e. US, EU). Bridging mechanisms, including APEC's Cross Border Privacy Rules (CBPR) and binding corporate rules, should be considered. Second, policymakers must encourage industry self-regulation; where such flexibility can reinforce accountability, empower companies to take charge in the upkeep of data privacy protection, and motivate them to keep pace with ongoing digitalization. This will ensure there are proper safeguards in place without stifling innovation and takes account of firms working across borders, while also serving as a precursor to overarching regulations.

Concerning capacity-building measures, policymakers must coordinate between privacy regulatory bodies within individual ASEAN Member States. ICT ministries must proactively work with their counterparts in other ministries and agencies, including finance and trade, to formulate and implement new trade policies surround e-commerce, technology, and data flows. This may incorporate elements of organizational and systemic capacity building, including forging partnerships between agencies, investing in new shared ICT capacity, and raising awareness across government bodies. Policy consistency is crucial in nurturing an enabling and open environment for digital trade, which will in turn promote the growth of e-commerce and foster data-driven innovation across the region.

Concerning communication, policymakers must promote communication and information exchanges between ASEAN Member States. This involves the sharing of best practices, regulatory guidelines, and intelligence. The sharing of best practices draws upon non-governmental privacy experts in the private sector, civil society, and academia. Further, the sharing of regulatory guidelines enables greater inclusivity which respects the ASEAN Member States' inherent legal frameworks and digital capabilities.[78] Finally, the sharing of intelligence encourages consistent and collaborative interactions with the private sector in anticipating cyber-related events and threats. ASEAN must continue to consult stakeholders to leverage upon established and leading technical expertise and experiences. The facilitating of communication thus empowers cooperation across borders and sectors in the development of ASEAN's data ecosystem.

[76] East-West Center, 'US, Japan, and Southeast Asia Cooperation on Building a Data Governance Blueprint' on East-West Center (30 April 2020) <https://www.eastwestcenter.org/events/us-japan-and-southeast-asia-cooperation-building-data-governance-blueprint>.

[77] US-ASEAN Business Council, *Digital Data Governance in ASEAN – Key Elements for a Data-Driven Economy* (US-ASEAN Business Council, 2019) 27.

[78] Mark Manantan, 'U.S., Japan, and Southeast Asia Cooperation: Building a Data Governance Blueprint' on East-West Center (30 April 2020) <https://www.eastwestcenter.org/publications/us-japan-and-southeast-asia-cooperation-building-data-governance-blueprint>.

Conclusion

Continuing efforts toward an overarching ASEAN data governance and privacy regulation bears relevance in promoting responsible data stewardship and data management, in protecting and benefiting ASEAN citizens, and in boosting the region's competitiveness and capabilities across through the free flow of data.

As referenced, ASEAN governments have expressed support for a multilateral approach to privacy and data protection in creating a framework that is responsive to the regulatory and legislative differences in the region and considers the states' level of maturity of laws, as well as cultural and socio-political nuances across jurisdictions. This was highlighted by the adoption of the 2016 PDP, 2018 DDG, and 2021 DMF, symbolizing the emergent consensus over the need to adopt overarching guidelines and standards to drive wider economic development and digital transformation across ASEAN.

Consequently, this trend has accelerated significantly over the past several years in response to COVID-19, growing regional economic integration, and the rising influence of China. The impact of the pandemic has irrevocably accelerated the pace of digital transformation across the region, with the majority of the region's population currently engaged in distance education, remote work, and e-commerce activities. Additionally, strides taken towards greater economic integration have increasingly incorporated measures conducive to the free flow of goods, services, and data. These highlights growing recognition at the ministerial level as to the importance and links between data protection and privacy vis-à-vis trade and commerce. Finally, China's growing influence, digital capabilities, and imminent adoption of data privacy legislation draws attention to its capacity to influence and draw from the formation of an overarching data protection and privacy regulation for ASEAN.

The need for an overarching, multilateral approach to data protection in ASEAN is therefore predicated upon several key realities: first, that corporate co- and self-regulation has proven ineffective at protecting consumer data rights vis-à-vis transnational corporations;[79] second, the need to anticipate and adapt to technological disruptions and developments; third, the need to drive progress through persuasion within ASEAN's informal political process; and finally, the need to mitigate the propensity of Southeast Asian states to embrace a restrictive approach towards the open flow of data beyond their borders.

Greater integration and harmonization between ASEAN's privacy frameworks must therefore recognise the level of maturity and readiness of each member state to adopt new features. A joint regional approach should be an evolving instrument that is updated and reviewed as specific countries adapt to regional changes, and progress toward the eventual enacting of an overarching data protection and privacy regulation for ASEAN.

[79] Estelle Masse, 'Data protection: why it matters and how to protect it' on Access Now (25 January 2018) <https://www.accessnow.org/data-protection-matters-protect/>.

Bibliography

Books/Articles/Reports

Ajami, Riad, 'The Regional Comprehensive Economic Partnership: Asia Trade Connectedness' (2020) *Journal of Asia-Pacific Business* 1-3

ASEAN, *ASEAN Digital Masterplan 2025* (ASEAN, 2021)

ASEAN Digital Senior Officials' Meeting, *ASEAN Data Management Framework - Data governance and protection throughout the data lifecycle* (ASEAN, 2021)

Bakhoum, M. (eds.) et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer, 2018)

Bozhkov, Nokolay, 'China's Cyber Diplomacy: A Primer' on EU Cyber Direct (9 March 2020) <https://eucyberdirect.eu/content_research/chinas-cyber-diplomacy-a-primer/>

Broom, Douglas, 'Young people in ASEAN have emerged from lockdowns more resilient and digitally switched on. Here's how' on World Economic Forum (8 October 2020) <https://www.weforum.org/agenda/2020/10/young-people-asean-digital-adoption-covid-19/>

Chiang, Benjamin, 'How can data governance drive economic advantage for Southeast Asia?' on EY (11 June 2020) <https://www.ey.com/en_sg/government-public-sector/how-can-data-governance-drive-economic-advantage-for-southeast-asia>

Day, Peter, 'Data across borders: The importance of data residency' on VentureBeat (3 October 2019) <https://venturebeat.com/2019/10/03/data-across-borders-the-importance-of-data-residency/>

Deloitte, *Data and privacy protection in ASEAN - What does it mean for businesses in the region?* (Deloitte, 2018)

Frost, Frank, 'ASEAN at 30: Enlargement, Consolidation and the Problems of Cambodia' on Australian Parliament (25 August 1997) <aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/CIB/CIB9798/98cib02>

Goddard, Michelle, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' (2017) 59(6) *International Journal of Market Research* 703-705

GSMA, *Regional Privacy Frameworks and Cross-Border Data Flows - How ASEAN and APEC can Protect Data and Drive Innovation* (GSMA, 2018)

H. Heinl, Caitriona, 'Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime' (2014) 18 *Asia Policy* 131-159

Han, Kristen, 'Broken promises: How Singapore lost trust on contact tracing privacy' on MIT Technology Review (11 January 2021) <https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/>

Healey, Robert, 'The Malaysia Personal Data Protection Act 2010 – All you need to know (Part 1)' on FORMITI (6 January 2021) <https://formiti.com/the-malaysia-personal-data-protection-act-2010-all-you-need-to-know-part-1/>

Henderson, James, 'Data breaches cost ASEAN businesses $2.71M' on Channel Asia (2 August 2020) <https://www.channelasia.tech/article/681831/data-breaches-cost-asean-businesses-minimum-2-71m/>

J. Brandon, John, 'Why ASEAN Needs to Invest More in Cybersecurity' on The Asia Foundation (9 May 2018) <https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/>

Jones, Lee, 'Explaining the failure of the ASEAN economic community: the primacy of domestic political economy' (2016) 29(5) *The Pacific Review* 647-670

Kennedy, Gabriela and Karen H.F. Lee, 'Finding Harmony – ASEAN Model Contractual Clauses and Data Management Framework Launched' on Mayer Brown (8 February 2021) <https://www.mayerbrown.com/en/perspectives-events/publications/2021/02/finding-harmony-asean-model-contractual-clauses-and-data-management-framework-launched>

Legen, Samuel, 'How much is your data worth to tech companies? Lawmakers want to tell you, but it's not that easy to calculate' on The Conversation (11 July 2019) <https://theconversation.com/how-much-is-your-data-worth-to-tech-companies-lawmakers-want-to-tell-you-but-its-not-that-easy-to-calculate-119716>

Leviter, Lee, 'The ASEAN Charter – ASEAN Failure of Member Failure?' (2009/10) 43(1) *International Law and Politics* 159-210

Lin, Ching-Fu and Liu, Han-Wei, *Disruptive Technologies and Sustainable Development: Implications for SoutheastAsia* (ICTSD, 2018)

Lin, Leo, 'COVID-19's Impact on Cybersecurity in ASEAN' on Atlas Institute of International Affairs (26 August 2020) <https://www.internationalaffairshouse.org/covid-19s-impact-on-cybersecurity-in-asean/>

Manantan, Mark, 'U.S., Japan, and Southeast Asia Cooperation: Building a Data Governance Blueprint' on East-West Center (30 April 2020) <https://www.eastwestcenter.org/publications/us-japan-and-southeast-asia-cooperation-building-data-governance-blueprint>

Masse, Estelle, 'Data protection: why it matters and how to protect it' on Access Now (25 January 2018) <https://www.accessnow.org/data-protection-matters-protect/>

McDonald, Tim, 'What is the Regional Comprehensive Economic Partnership (RCEP)?' on BBC (16 November 2020) <https://www.bbc.com/news/business-54899254>

Ramasamy, Haridas and Wendy He, 'Coping with COVID-19 the ASEAN way' on East Asia Forum (10 July 2020) <https://www.eastasiaforum.org/2020/07/10/coping-with-covid-19-the-asean-way/>

Rueppel, Patrick, 'The Geopolitics of Digital Trade and Sustainable Development' (2020) 11 *Yusof Ishak Institute – Perspective* 1-10

Sarap, Katrin, 'Three reasons why we need strict data protection regulations' on Njord Law (9 February 2018) <https://www.njordlaw.com/three-reasons-why-we-need-strict-data-protection-regulations>

Sargunaraj, Nadarashnaraj, *Personal Data Protection in ASEAN* (ZICO Law, 2020)

Strangio, Sebastian, 'In Southeast Asia, COVID-19 Speeds Transition to Digital Technologies' on The Diplomat (11 November 2020) <https://thediplomat.com/2020/11/in-southeast-asia-covid-19-speeds-transition-to-digital-technologies/>

Tan, Ivy and Di, Wu, 'Understanding the Regional Comprehensive Economic Partnership Agreement (RCEP)' on Baker McKenzie (2 December 2020) <https://www.bakermckenzie.com/-/media/files/insight/publications/2020/12/bakermckenzie_understandingrcep_dec2020.pdf?la=en>

Tham, Davina, 'Cybercrime jumps more than 50% in 2019, new threats emerge from COVID-19 pandemic' on CNA (26 June 2020) <https://www.channelnewsasia.com/news/singapore/cybercrime-jumps-more-than-50-2019-new-threats-covid-19-csa-12872818>

Thomas, Jason, 'ASEAN's data governance challenge' on The ASEAN Post (20 June 2019) <https://theaseanpost.com/article/aseans-data-governance-challenge>.

US-ASEAN Business Council, *Digital Data Governance in ASEAN – Key Elements for a Data-Driven Economy* (US-ASEAN Business Council, 2019)

Vandystadt, Nathalie, 'General Data Protection Regulation shows results, but work needs to continue' on European Commission (24 July 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449>

Voen Wong, Chian et al., 'Asia-Pacific Signals Strong Commitment to Economic Integration and Cooperation with RCEP Signing' on K&L Gates (9 December 2020) <https://www.klgates.com/Asia-Pacific-Signals-Strong-Commitment-to-Economic-Integration-and-Cooperation-with-RCEP-Signing-12-9-2020>

Wall, Alex, 'Summary: Philippines Data Privacy Act and implementing regulations' on iapp (27 April 2017) <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/>

Wong, Benjamin, 'Data Localization and ASEAN Economic Community' (2019) 10 *Asian Journal of International Law* 158-180

Yu, Eileen, 'Facebook 'deeply concerned' about Singapore directive to block access' on ZDNet (18 February 2020) <https://www.zdnet.com/article/facebook-deeply-concerned-about-singapore-directive-to-block-access/>

Zhao, Jingcong, 'Understanding Data Privacy and Why It Needs to Be a Priority for Your Business' on Hyperproof (5 February 2020) <https://hyperproof.io/resource/understanding-data-privacy/>

Zhou, Cissy and Finbarr Bermingham, 'China's Asean influence sets stage for new superpower battleground with US, as the ball shifts to Biden's court' on SCMP (13 December 2020) <https://www.scmp.com/economy/china-economy/article/3113620/chinas-asean-influence-sets-stage-new-superpower-battleground>

ZICO Law, 'ASEAN Insiders Series 2019 – Personal Data Protection' on ZICO Law (19 July 2019) <https://asialawportal.com/2019/07/19/asean-insiders-series-2019-personal-data-protection/>

Instruments

2016 Framework on Personal Data Protection, ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) (16 November 2016)

2018 Framework on Digital Data Governance, ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) (6 December 2018)

2020 Implementing Guidelines for ASEAN Data Management Framework and ASEAN Cross Border Data Flows Mechanism, 1st ASEAN Digital Ministers' Meeting (ADGMIN) (January 2021)

2020 Regional Comprehensive Economic Partnership

Data Privacy Act 2012 (Republic Act No. 10173) - Philippines

Personal Data Protection Act 2010 of Act 709 - Malaysia

Personal Data Protection Act 2012 (Act 26 of 2012) - Singapore

Public Sector (Governance) Act 2018 (Act 5 of 2018) - Singapore

Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020) - Malaysia

Treaty of Amity and Cooperation in Southeast Asia Indonesia (entered into force 24 February 1976) <https://asean.org/treaty-amity-cooperation-southeast-asia-indonesia-24-february-1976/>

Other

ASEAN-China Centre, 'The 2020 ASEAN-China Digital Economy Cooperation Conference Successfully Held in Chengdu' on ASEAN-China Centre (9 November 2020) <http://www.asean-china-center.org/english/2020-11/5474.html>

ASEAN, 'ASEAN Economic Community' on ASEAN (2021) <https://asean.org/asean-economic-community/>

ASEAN, 'The 18th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings – Joint Media Statement' on ASEAN (6 December 2018) <https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf>

Ashurst, 'Amendments to Singapore's Personal Data Protection Act' on Ashurst (12 November 2020) <https://www.ashurst.com/en/news-and-insights/legal-updates/amendments-to-singapore-s-personal-data-protection-act/>

Asian Business Law Institute, 'Convergence of data privacy laws and frameworks for cross-border transfers of personal data in Asia' on Asian Business Law Institute (2021) <https://abli.asia/Projects/Data-Privacy-Project>

CCDCOE, 'Association of Southeast Asian Nations' on CCDCOE (2021) <https://ccdcoe.org/organisations/asean/>

ChinaDaily, 'Speech by Chinese Premier at the 23rd China-ASEAN Summit' on ChinaDaily (13 November 2020) <chinadaily.com.cn/a/202011/13/WS5fad6e7ca31024ad0ba93c17.html>

Department of Foreign Affairs and Trade, 'RCEP text and associated documents' on Australian Government (15 November 2020) <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/rcep/rcep-text-and-associated-documents>

DFDL, 'Data Protected – Philippines' on Lexology (4 May 2020) <https://www.lexology.com/library/detail.aspx?g=0f0ece6e-9fc3-41be-bb21-570b5df0a9b3>

DLA Piper, 'Data Protection Laws of the World - Malaysia' DLA Piper (2021) <https://www.dlapiperdataprotection.com/index.html?c=MY&t=law#>

DLA Piper, 'Data Protection Laws of the World – Philippines' on DLA Piper (29 December 2020) <https://www.dlapiperdataprotection.com/index.html?c=PH&t=law#>

Drew & Napier LLC, 'Q&A: the data protection legal framework in Singapore' on Lexology (28 August 2020) <https://www.lexology.com/library/detail.aspx?g=63abc7b6-1b8f-4809-9d5c-8e261475dd3a>

East-West Center, 'US, Japan, and Southeast Asia Cooperation on Building a Data Governance Blueprint' on East-West Center (30 April 2020) <https://www.eastwestcenter.org/events/us-japan-and-southeast-asia-cooperation-building-data-governance-blueprint>

European Union, 'Regulations, Directives and other acts' on European Union (2021) <https://europa.eu/european-union/law/legal-acts_en#decisions>

EXECASSIST, 'Data protection is a key in a COVID-19 environment: IBM Security' on ASEAN Tech & Sec (2 September 2020) <https://aseantechsec.com/data-protection-a-key-in-a-covid-19-environment-ibm-security/>

Google and TEMASEK, Bain & Company, 'Google e-Conomy SEA 2020' on Google (2020) <https://economysea.withgoogle.com/>

Huawei, 'ASEAN to Accelerate Digital Integration for Post-COVID Economic Recovery' on Huawei (10 December 2020) <https://www.huawei.com/en/news/2020/12/asean-digital-connectivity-digital-transformation-covid19-pandemic>

Human Rights Careers, '10 Reasons Why Privacy Rights are Important' on Human Rights Careers (2021) <https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/>

KEARNY, 'Cybersecurity in ASEAN: An Urgent Call to Action' on KEARNY (23 January 2018) <https://www.southeast-asia.kearney.com/web/southeast-asia/article?/a/cybersecurity-in-asean-an-urgent-call-to-action>

KEARNY, 'The ASEAN digital Revolution' on KEARNY (24 November 2015) <https://www.nl.kearney.com/digital-transformation/article/?/a/the-asean-digital-revolution>

National Privacy Commission, 'Appointing a Data Protection Officer' on National Privacy Commission (2021) <https://www.privacy.gov.ph/appointing-a-data-protection-officer/>

National Privacy Commission, 'PH leads ASEAN's move to protect privacy' on National Privacy Commission (22 August 2019) <https://www.privacy.gov.ph/2019/08/ph-leads-asean-move-to-protect-privacy/>

OECD, 'Policy coherence for sustainable development' on OECD (2021) <http://www.oecd.org/gov/pcsd/>

Office of the Australian Information Commissioner, 'What is the Consumer Data Right?' on Australian Government (2021) <https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right/>

PDPA, 'ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows' on PDPA (22 January 2021) <https://www.pdpc.gov.sg/Help-and-Resources/2021/01/ASEAN-Data-Management-Framework-and-Model-Contractual-Clauses-on-Cross-Border-Data-Flows>

PDPC, 'Amendments to the Personal Data Protection Act (PDPA) Take Effect From 1 February 2021' on PDPC (29 January 2021) <https://www.pdpc.gov.sg/news-and-events/announcements/2021/01/amendments-to-the-personal-data-protection-act-take-effect-from-1-february-2021>

PDPC, 'PDPA Overview' on PDPC (2021) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

Rajah & Tann Asia, 'Data Management for Businesses: Launch of ASEAN Data Management Framework and Model Clauses on Data Transfer' on Lexology (2 February 2021) <https://www.lexology.com/library/detail.aspx?g=8d070e4b-5817-42de-bd54-c17159af8571>

Taft Stettinius & Hollister LLP, 'China's Personal Information Protection Law (PIPL) - Data Privacy in the Land of Big Data' on Lexology (13 January 2021) <https://www.lexology.com/library/detail.aspx?g=db4592e2-53c1-4cb6-91a9-94da1ee14b26>

US Mission to ASEAN, 'Growing ASEAN's Digital Economy' on US Mission to ASEAN (August 2020) <https://asean.usmission.gov/wp-content/uploads/sites/77/IGNITE-Digital-Economy-fact-sheet-Aug2020.pdf>

Vanessa Tanopo Jimenez, Arianne, 'Towards A Data Protection Soft Law Framework for the ASEAN Region' on Berkeley University (2016) <https://digitalassets.lib.berkeley.edu/etd/ucb/text/Jimenez_berkeley_0028E_16147.pdf>

Xinhua, 'Economic Watch: China, ASEAN forge deeper digital economy cooperation' on Xinhuanet (13 November 2020) <http://www.xinhuanet.com/english/2020-11/13/c_139514351.htm>