ACI Research Paper #19-2023

# Facilitating Data Flows Across ASEAN: Challenges and Policy Directions

Jingting LIU

Ulrike SENGSTSCHMID

Yixuan GE

First Version: 21 August 2023
Current Version: 30 August 2023

Please cite this article as:

Liu, Jingting, Ulrike Sengstschmid, and Yixuan Ge, "Facilitating Data Flows Across ASEAN: Challenges and Policy Directions", Research Paper #19-2023, *Asia Competitiveness Institute Research Paper Series (August 2023)*

## Abstract

With the growing digital economy, personal data protection during data transfers has become a key concern. The study examines the landscape of cross-border data transfer regulations in the ASEAN region and the various compliance challenges faced by businesses. The analysis and discussion focus on the effectiveness and limitations of region-wide mechanisms like ASEAN model contractual clauses, the interoperability of laws, the specific challenges faced by small- and medium-sized enterprises (SMEs) and business implications of Vietnam's data protection decrees. It also evaluates external influences on ASEAN's data transfer regulations by examining the prevalence of provisions on free data flow and limiting data localisation in free trade agreements that ASEAN countries are party to. We find that Singapore is a major influencer within ASEAN, while Australia is a key external influencer in promoting free data flows and limiting data localization. However, harmonizing data regulations through trade agreements in ASEAN remains limited due to numerous exceptions to relevant clauses.

To facilitate smooth data transfers within the region, we outline a policy roadmap for both national governments and ASEAN as a regional organisation: In the near term, reducing ambiguity and raising awareness of personal data regulation compliance should be prioritized to mitigate the negative impact on business activities through formalizing rules and guidelines, SME-specific support, and closer government-industry collaboration. In the longer-term coherent cross-border data transfer mechanisms across the region and perhaps at an even larger scale should be goal, which can be supported by interim solutions of harmonizing existing national regulations and signing bilateral agreements.



**Acknowledgements:**

We thank representatives from the Singapore offices of Grab, Microsoft, and P2D Solutions, and the Asia office of Huawei for their discussions and sharing of business experiences surrounding cross-border data flows.

# Table of Contents

# I. Introduction

As the digital economy is rapidly growing in importance and integrating on a regional and global scale, personal data protection at home and during cross-border data transfers increasingly become a key concern for policy makers. Especially in Southeast Asia where the digital economy has nearly doubled in size between 2019 and 2022 and is predicted to continue growing at an annual rate of 20%, many countries have enacted new legal frameworks to better regulate data and data flows (Google et al., 2022). However, national data regulations are only the first step, as it is vital for making full use of digital technologies to also facilitate cross-border data flows both within Southeast Asia and between Southeast Asia and external countries. This calls for the need for Southeast Asian states to create a more developed data protection framework, amidst increasing interest of major powers in working with this region to facilitate data flows.

This paper aims to discuss the challenges of compliance with cross-border data transfer (CBDT) regulations within the ASEAN member states from a business perspective, including the usefulness of region-wide mechanisms such as the ASEAN model contractual clauses, the interoperability between the various laws, as well as the experience with Vietnam's decrees requiring data localization and *ex ante* impact assessments. Additionally, we assess to what degree external influence is affecting ASEAN's CBDT regimes. Finally, we lay out a policy roadmap highlighting the priorities that can be achieved in the near- and long- term with actionable items that will protect data and business growth without compromising on national interests.

To fulfil these aims a range of data sources will be used. The analysis of the current regulatory landscape is directly based on a qualitative analysis of the various laws and regulations in place in the ASEAN member states. These are complemented with interviews conducted with various types of businesses active in the data economy in Southeast Asia, including large multinationals like Microsoft, regionally active firms like Grab, as well as P2D Solutions, a specialist data protection consulting and advisory firm working with small- and medium-sized enterprises (SMEs). Additionally, using a quantitative coding of trade agreements, the main external and internal influences in this policy domain for the ASEAN region were identified. Based on the combination of these sources, we propose policy recommendations to make the data environment more conducive to business operations.

Whereas numerous policy papers and reports have previously aimed to assess the regulatory landscape regarding cross-border data flows in ASEAN or the Asia-Pacific region more generally, this paper expands on this work in multiple ways. Firstly, the large number of changes the data protection landscape in this region has seen in recent years, including, most recently, the publication and entry into force of Vietnam's Personal Data Protection Decree in April and July 2023 respectively, calls for an updated analysis. Second, this paper draws from a range of sources including trade agreements, national laws, as well as interviews with businesses, to allow a more comprehensive understanding of both the theoretical and practical situation and challenges. And third, specific policy recommendations are provided for ASEAN as a regional organization and for national governments both in the near- and long-term to further promote ASEAN's digital economy.

After a short literature review, this paper will classify the ASEAN member states' national cross-border data flow policies in section III, before outlining the key obstacles faced by businesses in the region in section IV. Next, Vietnam's newest personal data protection rules and their implications for businesses will be outlined in section V. Finally, future policy directions will be explored by first analysing internal and external key players and influencers in section VI.A, and then outlining a

policy roadmap in section VI.B to further improve the data-related business environment in the region.

# II. Literature Review

It is widely agreed that the cross-border data flows function quite differently to international trade in traditional goods and services. Reasons for this include that data can be exported and imported multiple times by different users, that cross-border data flows may not necessarily be affiliated with transactions, that the storage location of data is often both irrelevant and difficult to determine, and that the distinction between personal and non-personal data may be unclear and firms may be using or transferring both simultaneously (see for example Aaronson, 2019). This novelty may be one of the reasons why a wide range of regulatory mechanisms have emerged to both protect data subjects' privacy and to safeguard national interests while businesses transfer data. For example, Casalini et al. (2021) find that 79% of OECD member countries use some form of *ex ante* government approval, but these can differ widely including adequacy decisions and standard contractual clauses. Even within similar mechanisms, however, further national differences can exist, making the landscape even less uniform, as becomes clear in Girot's (2018) book-long analysis of the regulatory frameworks regarding cross-border data transfers of just selected Asian economies.

## A. Far-reaching Impacts of Cross-Border Data Flow Regulations

Legislation regulating cross-border data flows has far reaching impacts on various economic indicators by affecting trade patterns which in turn can impact GDP, investments, and welfare, as well as on businesses' costs and thus firm performance.

In terms of trade effects, González et al. (2023) find that a 0.1 point reduction in the OECD's domestic digital trade restrictiveness index (DSTRI, scale of 0-1) – which can be caused by a major reform of the national data regulatory framework – corresponds to an increase in overall exports by 145%. This figure is likely to be even higher for emerging economies. Additionally, when examining international agreements on cross-border data flows, Spiezia & Tscheke (2020) find that the EU- and Switzerland-US Safe Harbor agreements which facilitated trans-Atlantic personal data transfers resulted in an 8% increase in trade flows in goods between the two trading partners. Similarly, among APEC member countries, for each additional provision on digital trade, including provisions on cross-border data flows, that came into force between two trading partners, the digital service flows between the two increased by 2.3%, which has resulted in an aggregate increase of 2.9% or 40.1 billion USD in digital trade due to such provisions between 2000 and 2018 (APEC, 2023).

These increases in trade also translate into wider economic benefits. In one of the most cited papers on the issue, Bauer et al. (2014) study the economy-wide effects of data localization regulations and project the enacted legislations on the matter to have significant negative effects on GDP ranging between -0.1% and -1.7% in all seven studied countries. Similarly, they find that domestic investments also reduced by between 0.5% and 4.2% as a result of lost competitiveness due to data localization. Finally, the study finds welfare losses per worker in China due to data localization requirements to amount to 13% of the average monthly salary.

Besides these macroeconomic consequences, regulations on data flows also affect firms directly. Especially micro-, small- and medium-sized enterprises (MSMEs) are negatively affected due to the relatively higher compliance costs they face in comparison to large multinationals. While using digital tools in trade can reduce export costs of MSMEs in the Asia-Pacific by 40% and 82% for manufacturers and service providers, respectively, these benefits are not only reduced by data flow restrictions, but data localization requirements could additionally increase computing costs for these

firms by 30-60% (AMTC, 2018). Furthermore, it is not only overly restrictive policies that are associated with business costs, but Liu (2018) highlights that not having a clear and formalised personal data protection framework also costs firms due to higher degrees of business uncertainty.

## B. Challenges for ASEAN Businesses Posed by Data Regulations

Both scholars and business representatives are in agreement that the main challenge facing Southeast Asia as a region in their development of the data economy is the fragmentation of personal data protection regulations between the various ASEAN member states constraining both data flows within the region and between ASEAN and external partners (EU-ASEAN Business Council, 2020; GSMA, 2018; Khumon, 2018; Suvannaphakdy, 2023; US-ASEAN Business Council, 2019). Not only the content and requirements of various regulatory frameworks differs, but also the stage of development with some countries like Cambodia or Laos having effectively no personal data protection framework (GSMA, 2018; Khumon, 2018). This is further complicated by the fact that different countries in the region have acceded to different international mechanisms to regulate cross-border data flows such as the APEC CBPR or the CPTPP, and that RCEP, as one of the only international treaties with data provisions to which all states in the region are party, has far-reaching exceptions (Khumon, 2018). Although the value of regional frameworks, especially ASEAN's Model Contractual Clauses (MCCs), to bridge these difficulties in cross-border data flows are recognized, various challenges remain: First, they only offer a relatively low standard of data protection, making them less useful when trading with partners with highly developed data protection regimes (Greenleaf, 2021). Second, their use does not automatically make a company compliant, as additionally requirements in national laws must be adhered to (BakerMcKenzie, 2021; Kennedy, 2021). And third, they are not yet interoperable with the European Union's Standard Contractual Clauses or other international data transfer mechanisms (Greenleaf, 2021).

To address these challenges and further facilitate data flows, the consensus generally is that an interoperable unified framework needs to be created that allows for both intra- and inter-regional safe and secure data transfers. In this process, it is important that the new mechanism is compatible with already existing mechanisms, especially the APEC CBPR and the EU's SCCs to minimize businesses' compliance costs (EU-ASEAN Business Council, 2020; GSMA, 2018; Khumon, 2018; E. Lim, 2020; US-ASEAN Business Council, 2019). Additionally, interoperability must be ensured through harmonizing national data protection regulations in terms of data classification and data handling requirements (EU-ASEAN Business Council, 2020; GSMA, 2018). Furthermore, skills and expertise in data regulations should be promoted among the private sector, and certification schemes or MCCs should not be made mandatory to avoid high costs to SMEs and decrease reliance on third-party certification agents (GSMA, 2018; US-ASEAN Business Council, 2019). Finally, successful deep collaboration on these matters also requires regular updates and reviews of regulatory frameworks as countries' national policies mature and technology advances (J. Lim, 2021), which may be best achieved through more comprehensive digital economy agreements (Suvannaphakdy, 2023).

## C. External Influences on Data Regulation

When writing new or revising existing personal data protection policies, as in other policy domains, countries often learn and borrow from existing successful policies. In the data protection space, perhaps the main model regulation is the European Union's General Data Protection Regulation (GDPR), which has inspired many similar regulations around the world (Ryngaert & Taylor, 2020). However, beyond this influence, trade agreements are another way to shape and harmonize policies across jurisdictions. Casalini et al. (2021) argues that the potential of trade agreements in the data

policy space is significant due to the high degree of commonalities among personal data protection acts both within and between OECD and emerging economies, with a 68% overlap of provisions.

While large-scale international alignment of data policies, for example by a revision of WTO rules may be most effective in facilitating trade and economic growth (Chin & Zhao, 2022; Mitchell & Mishra, 2019), this may not be feasible in the short- to medium-term. Instead, bilateral or regional initiatives are more likely, and especially the big global powers like the US, the EU, and China are active to influence policymaking in this domain to benefit from smoother trade flows. These pushes can be detected in publications from both policy think-tanks and academic work from the countries (see for example Goodman & Risberg (2021) for the US or Xu (2022) for China). In general, among these powers, the US advocates for the freest trade flows and has the most coherent approach in introducing novel and strict provisions that enable cross-border data flows and limit data localization, as the examples of the US-led TPP data provisions that were later signed into force in the CPTPP have shown ((Burri, 2022; H.-W. Liu, 2018). The EU is more cautious in its approach due to its significantly higher standards of personal data protection. As such it seeks to limit data localization, but free data flows are conditional on meeting GDPR requirements, which is why as of 2022 none of its data-related clauses in trade agreements were binding in nature (Burri, 2022). Southeast Asia as a region may be particularly susceptible to external policy influence due to its comparatively less developed legal frameworks (H.-W. Liu, 2018) and no binding regional standards (Burri, 2022), which we examine in greater detail in Section VI.

# III. Personal Data Protection in ASEAN

## A. The Open, Conditional, and Control Model of Data Governance

The rapid growth of the digital economy and the subsequent importance of data flows has led many governments around the world to introduce comprehensive data regulatory frameworks. While similarities in the how data is protected may exist, differences in fundamental motivations – ranging from facilitating business, to protecting human rights, to safeguarding national security – translate into the emergence of three different data regime models: the open model, the conditional model, and the limited model (Ferracane & van der Marel, 2021). While the specific names and some country classifications may differ between scholarly approaches, the classification of data regimes along the following dimensions is generally agreed upon between scholars and practitioners (see for example also Global Data Alliance, 2023, Lim et al., 2023)

The open model usually accords the most liberties to businesses in terms of data processing, as it typically operates on an *ex-post* basis. This means that businesses are responsible for data protection, and regulatory authorities will only intervene after a data breach has occurred. Regarding cross-border data transfers, this model imposes limited to no restrictions and may rely on trade agreements to support data flows. For the data subject, this means however, that they have only limited rights and protections of their personal data. The US is perhaps the most prominent example of this model.

On the other end of the spectrum is the control model, which generally prioritizes national security concerns over both individual data rights and business needs, resulting in the most stringent data protection framework. While such models may include comprehensive data subject right and processor responsibilities for ensuring data protection, significant exceptions are usually granted to state authorities, both in terms of data they process and in being able to intervene in other domestic processing activities. Cross-border data transfers under this model are typically contingent on *ex-ante* security assessments or government approval and may even be completely prohibited in certain sectors. Additionally, many countries following this regime type also require data localization to some degree. China's newest data protection laws have confirmed its adherence to this model (J. Liu et al., 2023).

Finally, the conditional model lies between the other two, emphasizing data subject rights. Besides comprehensive domestic personal data protection frameworks, it typically allows cross-border data transfers given various conditions are fulfilled. Data exports are permitted as long as the recipient country or organization can guarantee a similar standard of data protection as the origin country – either through government decisions, or contractual agreements – or the data subject gives informed consent to the transfer. As such, this model aims to uphold the data subject's personal data protection rights even outside its jurisdiction. The most well-known model of this type is the EU's General Data Protection Regulation (GDPR) which serves as a model for many other countries following a broadly similar approach.

## B. ASEAN's Diverse Regulatory Landscape

Governments across ASEAN have also realized the need for comprehensive data protection frameworks and with the exception of Brunei, Cambodia, Laos, and Myanmar all have or are in the process of implementing a regulatory regime for personal data. However, while similarities between the various national data protection regimes exist – in part because many took inspiration from the

EU's GDPR – differences remain, due to the fundamentally different motivations of governments. In fact, all three models discussed above are present within ASEAN member states:

- The Philippines is the only example of the open model in the region, allowing for data exports as long as the data subject gives consent, or the firm takes responsibility for ensuring no data misuse.
- Singapore, Thailand, and Malaysia follow the conditional model, allowing transfers only if the recipient country has an adequate level of data protection, if binding contracts are signed with the foreign data processor (including, depending on the country, standard contractual clauses, binding corporate rules, or contract certified by the data protection office), or if the data subject has given explicit and informed consent.
- Vietnam's new data protection laws, which have entered into force in 2022 and 2023, belong to the control model, requiring legally binding contracts, informing the Ministry of Public Security, as well as data localization in some cases.
- Indonesia's current data protection framework also falls under the control model, with similar requirements as Vietnam. However, a new law (Law No. 27 of 2022 regarding Personal Data Protection) has been enacted in October 2022 that will become binding after a two-year transition period in October 2024. This new law is a move towards the conditional model as it removes data localization clauses and instead allows cross-border data transfers as long as a similar level of data protection can be guaranteed by the recipient country or organization.

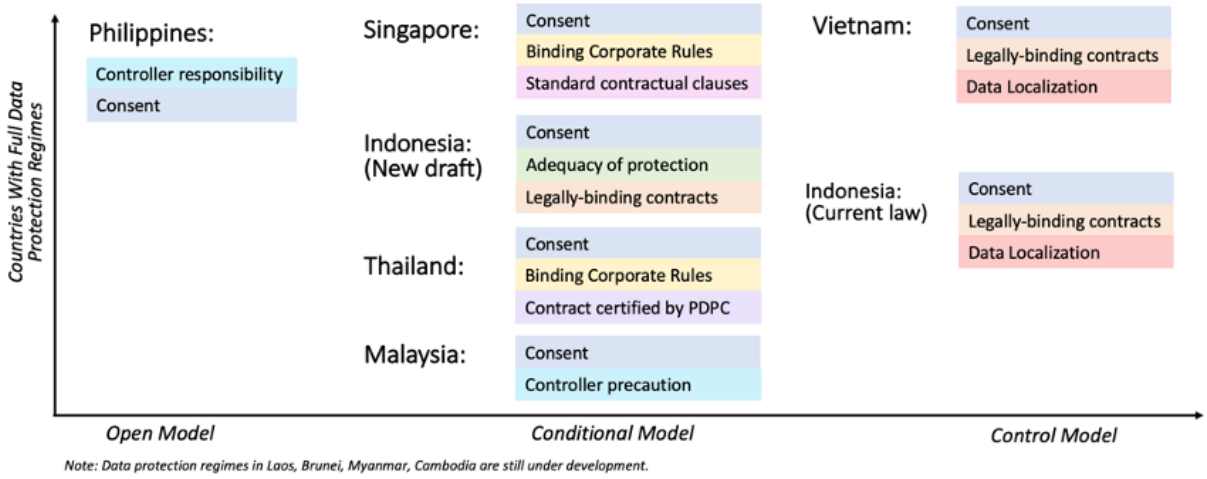


*Figure 1: National-level cross-border data transfer mechanisms within ASEAN*

However, even among the countries following the conditional model, data transfers are not seamless for businesses. As the exact details required in the legally binding contracts are not the same between countries, firms operating in multiple markets must sign and adhere to multiple contracts. This not only requires a high degree of legal knowledge, but also hampers business fluidity as each contract may have specific and potentially contradictory requirements regarding the details of data processing and transfer.

To overcome these challenges, several regional and international initiatives have been proposed for facilitating cross-border data transfers. One example of these is ASEAN's Model Contractual Clauses (MCCs) which have been in use since 2021. The MCCs are voluntary contractual terms that firms can

include in their binding legal agreements with foreign entities to which they transfer personal data. Compliance with the ASEAN MCCs guarantees a minimum level of personal data protection by the data processor which is sufficient for cross-border data transfers between all ASEAN member states. Thus, the ASEAN MCCs allow companies to reduce the legal complexity of cross-border data transfers by significantly reducing the number of contracts they need to sign.

Another example of an international mechanism to facilitate cross-border data transfers across jurisdictions with different legal requirements are the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (APEC CBPR) and its Privacy Recognition for Processors (PRP). Under these two schemes data controllers and data processors, respectively, can apply for certification from authorized bodies, which, if passed, indicates that the given organization's data operations are legally bound to meet a certain level of privacy protection. Thus, transferring data internationally between two certified organizations requires no further safeguards (PDPC Singapore, 2020). Although all 21 APEC countries have been involved in the development of this framework, only nine currently participate in the scheme (APEC, 2023). Singapore is the only country within ASEAN to participate,[1] thus limiting the CBPR and PRP's usefulness for data transfers within ASEAN. Nevertheless, in Singapore these certifications have proven quite popular, with 11 and 5 major companies, including UOB, Great Eastern Life Insurance, and Alibaba Cloud, certified under CBPR and PRP respectively (IMDA Singapore, 2023a, 2023b).

[1] The other economies participating in the ASEAN CBPR and PRP include Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Chinese Taipei, and the United States.

# IV. Remaining Obstacles for Businesses in Cross-Border Data Flows

Regional model contractual clauses and data protection certification mechanisms aim to overcome some of the barriers the different national data protection frameworks pose to cross-border data transfers. However, while significantly simplifying the process, a range of challenges remain, which must be addressed to smoothen data flows in Southeast Asia. Three key issues that remain will be addressed below, including (a) the modifications to the ASEAN MCCs required by national governments and the unclear legal status of the MCCs, (b) remaining problems in interoperability between national legislations that cannot be bridged using MCCs or certification schemes, and (c) the disproportionately large gap between SMEs and large corporations in data compliance.

## A. ASEAN Model Contractual Clauses: Modifications & Legal Status

Although the ASEAN MCCs significantly ease the compliance burden on companies, its effectiveness may currently be limited. Importantly, although the main MCCs are the same, different countries do require minor tweaks in the stipulated clauses to act as a legally valid mechanism for cross-border data transfers. So far, Singapore is the only ASEAN country that has issued official guidance on how to adapt the MCCs to comply with its own Personal Data Protection Act (PDPA). These include changes to the precise definition of "data subject" and the timeframe for notifications on data breaches (PDPC Singapore, 2021). Although these changes seem relatively minor, they are a complicating factor to business operations when data transfers are conducted across multiple ASEAN jurisdictions. Additionally, although other countries are likely to communicate guidance during workshops, the fact that they do not formally offer written guidance on such adaptations increases legal uncertainty (Khumon, 2023; Lee, Jeth (Microsoft), personal communication, 31 May 2023). Furthermore, except for Singapore, the other ASEAN member states do not legally endorse the MCCs – except in Singapore's PDPA advisory guidelines there is no express mention of MCCs in other ASEAN member states as a legal mechanism to transfer data across borders. The combination of these legal uncertainties may even inhibit some companies from using the MCCs, while recent initiatives including a joint guide to ASEAN MCCs and EU Standard Contractual Clauses between ASEAN and the European Commission are helpful in driving consensus (Lee, Jeth (Microsoft), personal communication, 31 May 2023).

## B. Interoperability Roadblocks: Incompatibility in National Legislations

Even if firms implement MCCs correctly and adapted to the relevant setting, the problem of interoperability between different legal frameworks may remain: Various provisions within data protection regulations such as the reasons for which data can be collected and processed, for which activities the data subject's consent is required, or how the data subject can revoke his consent are likely to be different between countries. Thus, even when the appropriate measures are taken for cross-border data transfer, firms handling data in multiple countries may still not be able to employ the same process across the jurisdictions, further complicating their operations.

For example, in different jurisdictions different legal bases for collecting and processing personal data exist (also see Table 1): while in Singapore and Thailand the legitimate interest of the data collector or public interest is sufficient, in Malaysia these exceptions are not given and even in these cases consent is required. Additionally, in Indonesia, for example, consent must be given in the Indonesian language and is not valid if only given in English. Furthermore, Thailand, Malaysia, and Vietnam have different requirements for processing sensitive personal data – but the definitions of what constitutes this also differ, with ethnicity and sexual orientation, for example, being sensitive in Thailand and Vietnam but not in Malaysia, and financial information and physical location being only

sensitive in Vietnam. As such, when collecting and processing a certain type of data, companies must ensure that either they meet the most stringent requirement in the region, or, if requirements are contradictory, they must adapt their data handling processes to the origin country of the data point.

*Table 1: Selected examples of different provisions and requirements in national personal data protection regimes in ASEAN (Compiled using information from: (BakerMcKenzie, n.d.; Government of Vietnam, 2023)).*

| Topic Area | | Thailand | Singapore | Philippines | Malaysia | Indonesia | Vietnam |
|---|---|---|---|---|---|---|---|
| **Legal bases to process non-sensitive personal data:** | appropriate notice to data subject | No | Yes | No | No | Yes | No |
| | data subject's consent | Yes | Yes | Yes | Yes | Yes, but must be in writing and in the Indonesia language | Yes |
| | necessary to perform a contract with data subject | Yes | Yes | Yes | Yes | Yes | Yes |
| | necessary to comply with a legal obligation | Yes | Yes | Yes | Yes | Yes | No |
| | necessary to protect a person's vital interests | Yes | Yes | Yes | Yes | Yes | Yes |
| | In the public interest | Yes | Yes | Yes | No | Yes | Yes |
| | legitimate interest | Yes | Yes | Yes | No | Yes | No |
| | preparation of historical documents or public archives | Yes | No | No | No | No | No |
| | Necessary for the administration of justice | No | No | No | Yes | No | No |
| **Sensitive/special personal data includes:** | racial or ethnic origin | Yes | No sensitive data regime in the PDPA. This is left to sector-specific laws. | Yes | No | While there is no categorization of sensitive personal data, the PDP law refers to "specific personal data", for which however there are no additional requirements. | Yes |
| | political opinions | Yes | | Yes | Yes | | Yes |
| | religious or philosophical belief | Yes | | Yes | Yes | | Yes |
| | trade / professional union or association membership | Yes | | No | No | | No |
| | genetic data | Yes | | Yes | Yes | | Yes |
| | biometric data | Yes | | No | Yes | | Yes |
| | health/medical information | Yes | | Yes | Yes | | Yes |
| | person's sex life or sexual orientation | Yes | | Yes | No | | Yes |
| | criminal record | Yes | | Yes | Yes | | Yes |
| | passwords | No | | No | No | | No |
| | disability status | Yes | | No | No | | No |
| | financial information | No | | No | No | | Yes |
| | individual's location | No | | No | No | | Yes |
| | Government identity card information | No | | Yes | No | | No |
| **Legal bases to process sensitive personal data:** | data subject's consent | Yes | No sensitive data regime in the PDPA. This is left to sector-specific laws. | Yes | Yes | While there is no categorization of sensitive personal data, the PDP law refers to "specific personal data", for which however there are no additional requirements. | Data subjects must be informed that the data is sensitive. No additional restrictions. |
| | necessary to perform obligations in field of employment and social security | No | | No | Yes | | |
| | necessary to protect a person's vital interests | Yes | | Yes | Yes | | |
| | Legitimate activities by not-for-profit | Yes | | Yes | No | | |
| | On data explicitly made public by data subject | Yes | | No | Yes | | |
| | Necessary for establishment, exercise, or defence of legal claims | Yes | | Yes | Yes | | |
| | In public interest | No | | No | No | | |
| | For health or social care | No | | Yes | Yes | | |
| | In interest of public health | No | | No | No | | |
| **Requirements for collecting or processing personal data from minors:** | Age below which an individual is considered a minor | 20 | 21 | 18 | 18 | No age in the PDP law. | No age in PDP decree. |
| | Special requirements for data processing of minors | Below age of 10 parents must consent. Between 10-20, minor can consent on some issues and parents must consent on others. | Below age of 13 parents must consent. Between 13-21, minor can consent on some issues and parents must consent on others. | Consent must be given/ authorized by parent. Parents must be notified of data breach. | Consent must be given/ authorized by parent. | Consent must be given/ authorized by parent. | Below age of 7 parents must consent. Above 7, both the child and a parent must consent. |
| **Notifications about personal data security breaches** | Authorities must be notified: | Office of the Personal Data Protection Committee within 72 hours. | PDPC within 72 hours. | NPC within 72 hours. | No requirement. | Within 72 hours (to which authority is unclear). | Ministry of Public Security within 72 hours. |
| | Data subject must be notified: | If data breach is likely to result in a high risk to the rights of the person, without undue delay. | At the same time or as soon as practicable after PDPC notification. | Within 72 hours. | No requirement. | Within 72 hours. | No requirement. |

## C. Data Compliance Disparity: Unique Challenges for SMEs

All of the above-mentioned issues are faced by companies of all sizes as the vast majority of data protection compliance in Southeast Asia is independent of the size of the company or the volume of data processed. Nevertheless, the costs of compliance do not scale linearly with company size, as implementing an adequate data protection regime within a firm's operations comes with significant upfront fixed costs and investments. As compliance does not directly generate revenue, even seemingly small investments in this domain can be unpopular for SMEs at best, and difficult to stem at worst. Especially in today's economic climate where many SMEs are still recovering from the effects of the Covid-19 pandemic and its associated business disruptions, and where additionally, the data protection frameworks in many Southeast Asian countries are in flux as they are being newly implemented and updated to suit new technological developments, the costs of even just understanding the data protection regulations and their requirements may act as a significant deterrence to SME compliance. As Desmond Chow, Director of P2D Solutions, a consultancy working with SMEs in Singapore on data protection compliance, points out, "For SMEs, the compliance is a lot tougher because they currently really do not have enough resources– not just for handling overseas transfer compliance, but from a general PDPA compliance standpoint".

However, besides the associated costs, unfamiliarity with the data protection regulations and their requirements and obligations may be a similarly large issue (Chow, Desmond (P2D Solutions), personal communication, 19 June 2023). Most SMEs do not have the resources to engage a designated data protection officer (DPO) to oversee their data handling processes, meaning that managers of other departments or units must often double- or triple-hat to also fulfil the role of the DPO. Oftentimes, they are not sufficiently trained for this. At an even more fundamental level, many SMEs and their employees may not even be aware of the existence of data protection regulations or if and how these regulations apply to them. Since these concerns already apply to national level regulations, and if national level regulations cannot be complied with, then compliance with cross-border transfer rules will be next to impossible. However, Mr. Chow, Director of P2D Solutions, notes two positive trends: Firstly, awareness levels in SMEs about Singapore's Personal Data Protection Act have significantly increased in recent years due to a combination of government promotion and media attention. Secondly, and closely related, the vast majority of those SMEs that are aware of and becoming compliant with national level data protection regulations are also similarly aware of the cross-border data transfer restrictions and requirements, meaning that increasing compliance with national and international data protection regimes for SMEs will likely go hand-in-hand.

### Key Issues Faced by SMEs

- Lack of awareness
  - Many SMEs are not familiar with the data protection regulations and their requirements and obligations
- High costs in a difficult economic environment
  - Compliance costs for SMEs are disproportionately high, and as compliance generates no direct revenue, other business needs may be more important when many firms are still recovering from Covid-19.
- Lack of manpower
  - DPOs often wear multiple hats, reducing focus on data protection. Staff tasked with data handling may not have the relevant training or experience.

## V. Vietnam's New Personal Data Protection Decree

Most recently, in April 2023, Vietnam published its Decree on Personal Data Protection (PDPD), which will enter into force on July 1st, 2023 (Government of Vietnam, 2023).[2] In conjunction with Decree 53 on data localization which came into force in October 2022, it harmonizes and clarifies the country's legal framework on personal data which was previously governed by 19 separate laws and regulations.

The new PDPD clarifies the rights of data subjects, the obligations of data handlers, as well as the legal basis for data processing. However, significant ambiguities remain. Perhaps the most pressing unclarity surrounds the nature of the required impact assessments. Under the new decree, firms must conduct an impact assessment within 60 days from the commencement of processing any personal data of Vietnamese citizens, and an additional one for transferring such data overseas for processing. These must be submitted to the Ministry of Public Security. Such impact assessments must be conducted in addition to a company's use of ASEAN MCCs to transfer data abroad, reducing the benefit companies can draw from such regional agreements.

Furthermore, what exactly must be included in such an assessment has not been specified. Additionally, companies wonder whether this is a de facto approval process, and what would happen to data that has already been transferred by the time the relevant officials raise an objection. Moreover, it remains to be seen to what extent the Ministry of Public Security and its Department of Cybersecurity and Hi-tech Crimes Prevention (commonly referred to as "A05") – officially designated to oversee personal data protection – will interact with other bodies such as the Ministry of Information and Communications, and how that will affect the interpretation and implementation of the new decrees. Resultingly, as Microsoft's ASEAN Head of Legal and Regulatory Affairs Jeth Lee explains "most companies may wait to transfer data overseas until they get an indication of no-objection from the Ministry of Public Security", even if this involves negative business consequences.

Besides the negative business impacts stemming from the ambiguity inherent in these new laws and regulations, the specific provisions of the Vietnamese decrees, especially surrounding data localization raise operating costs for businesses. Decree 53 states that all local companies and foreign businesses in 10 industries upon request from the Ministry of Public Security must store personal data within Vietnam. This directly impacts business operations in the country as those subject to data localization can no longer use data centres abroad to store and process their users' data. Instead, they may need to set up a new data centre in Vietnam, which not only requires infrastructure investments but also trained human capital. Maintaining such a new data centre in Vietnam may cost firms around 0.5 million USD annually.

Additionally, if data cannot be processed abroad it also means that Vietnamese citizens and businesses may have challenges accessing services that require employees or servers abroad, save where specific conditions are adhered to. Consequently, Vietnamese firms may be less able to extract the full value from their data and may need to work with products with lower technical capabilities such as less robust data recovery.

[2] Available here in Vietnamese: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx.

### Key Short-Term Business Impacts of Vietnam's PDP Decree

- Additional administrative efforts
    - Impact assessments that must be conducted additionally to other legal requirements like MCCs are an additional hurdle to smooth data flows.
- Remaining legal ambiguities
    - Ambiguities remaining in how requirements, especially around impact assessments, will be interpreted and their consequences can act as a deterrent to business operations.
- Data localization increases business costs
    - If companies are required to store data in Vietnam, this directly increases costs and may also decrease the range of services offered to Vietnamese customers.

# VI. Future Policy Directions

The landscape of policies governing cross-border data transfers is in a constant state of evolution and refinement. In this section, we first discuss how future data governance in ASEAN will be shaped by influence from leading economies that actively participate in rule-setting through trade agreements. We then outline a feasible policy roadmap that protects business interests without sacrificing national priorities.

## A. Growing External Influence

Highlights

- Within the ASEAN region, Singapore is the major influencer and a forerunner in promoting free data flows and limiting data localisation.
- Outside the region, Australia has the highest number of agreements with provisions on free data flows and limiting data localisation.
- Overall, there are more agreements with provisions on free cross-border data flows than limiting data localisation, probably because the former is easier to be agreed upon.
- However, the effectiveness of external influence on harmonising data regulations across ASEAN is limited. Trade agreements containing provisions on free data flows are often riddled with exceptions.

ASEAN, being a dynamic region with robust economic and trade connections to the global stage, faces not only needs regarding cross-border data transfers within its boundaries but also seeks a unified framework for data transfers with external partners, notably key trading partners such as China, the United States, and the European Union. Balancing internal and external challenges and needs will be an issue for ASEAN in the future.

There is active discussion, especially among law academics and practitioners, on how growing influence from the EU and the US may foster a cooperative and coherent digital data governance framework across ASEAN (J. Lim, 2021). Recent high-level events that demonstrate the growing external influence on the region include the US-led Indo-Pacific Economic Framework for Prosperity (IPEF), which just held its negotiating round in Singapore in May. Notably, cross-border data flow is a key topical issue raised during its stakeholder listening session. The Global Cross-Border Privacy Rules (CPBR) Forum, again US-led, to which Singapore and several other economies are invited as founding members, is another avenue of interaction among policymakers of different countries. The EU, on the other hand, has had initial policy influence, by various ASEAN countries, most notably Thailand, drawing heavily from the GDPR when writing their own data protection regulation (International Trade Administration, 2022). In addition, it continues to cooperate closely with ASEAN, with the two regional organizations having released the ASEAN-EU Joint Guide to the regions' respective model contractual clauses, and working on an implementation guide to further facilitate interregional business operations (ASEAN Secretariat & European Commission, 2023).

We therefore assess to what extent external influence will harmonise data regulations across ASEAN countries and promote free data flows by taking stock of how prevalent provisions of free flow of data and limiting data localisation are in trade agreements signed by ASEAN countries individually and as a whole. In doing so, we identify key influencers both within ASEAN and outside the region for free flow of data. We also evaluate the effectiveness of such agreements by checking the

presence of exclusions. To this end, we use the TAPED (Trade Agreements Provisions on Electronic-commerce and Data) dataset, which codifies provisions in trade agreements and classifies the provisions based on whether they are hard or soft (Burri et al., 2022).

During the years between 2000 and 2022, ASEAN member states have signed 66 trade agreements (PTAs) that are currently in force– including both those that ASEAN as a region has signed and those that at least one member state has signed with an external country. Of these, the 23 PTAs that include at least one clause on either promoting the free movement of data or on limiting data localization have been listed in Table 1Table 2. The TAPED dataset codes relevant provisions either as "2" for "hard" provisions and "1" for "soft" provisions, with the former being enforceable by another party, for example through appropriate dispute settlement mechanisms. Similarly, it also encodes whether various exclusions to such provisions are present in the agreement – these will be addressed in more detail later. While the dataset distinguishes between whether a relevant clause is found inside the dedicated chapter on e-commerce or not, this will not be relevant for the following analysis and only the highest score for each type of provision will be used.

Figure 2 and Figure 3 below visualize this information on maps. In Figure 2, the left column shows the number of agreements each ASEAN country has signed with at least one provision on either free data movement (top row) or limiting data localization (bottom row). The right column similarly visualizes the total sum of all scores for each type of clause by country. Figure 3 mirrors this, visualizing the count and sum of scores for all non-ASEAN partner countries. It can be seen that within ASEAN, Singapore is by far the leading actor in both domains, while Vietnam and Malaysia, which generally rank second and third, only have 25% or less of the count or sum of scores of Singapore. In terms of partner countries, Australia clearly takes a leading position with just over double the counts and scores of New Zealand and South Korea that rank second and third. Interestingly, the EU seems to outperform both the US and China in terms of free data movement but has 0 agreements with ASEAN countries that touch upon data localization.

To gauge the overtime developments in the data governance in trade agreements within the ASEAN region, Figure 4 plots the number of agreements with provisions on the free flow of data in red and on limiting data localization in blue. It can clearly be seen that agreements with provisions on free data flows are signed more often and these clauses have also been included in PTAs earlier than those on limiting data localization. The first trade agreement that included a provision on the free flow of data was signed in the year 2000, whereas the first PTA including provisions on limiting data localization was only signed in 2016. This trend may be due to the fact that countries requiring data localization often do so for national security reasons or other high-level national interests. Thus, negotiations on these provisions are likely to be significantly more difficult, resulting in fewer and later clauses on this issue in international agreements.

As Singapore has been previously identified as a leading actor in terms of the number of agreements with relevant clauses signed (also see Table 3 below), Figure 5 disaggregates ASEAN's overtime trend into those agreements signed by Singapore (red) and those signed by the rest of ASEAN (blue), showing both provisions on free flow of data (left panel) and limiting data localization (right panel). It is clearly visible that in both cases, Singapore signs agreements earlier in time than the rest of ASEAN, with Singapore being a signatory to a PTA with a provision on free data flows in 2000 and to a PTA limiting data localization in 2016, while the first agreements without Singapore were only signed in 2009 and 2018, respectively. This further highlights the influential role in regional policymaking Singapore has taken up in this domain.

*Table 2: ASEAN PTAs with at least one clause on either free data movement or limiting data localization*

| Short Title | Year | Free Data Movement | Limiting Data Localization | Free Data Movement (outside chapter) | Limiting Data Localization (outside chapter) | Exclusion related to E-commerce/ Digital Trade | Exclusion of internal taxes | Exclusion of digital financial instruments | Exclusion of data held/processed by government |
|---|---|---|---|---|---|---|---|---|---|
| Korea-Singapore DEA | 2022 | 2 | 2 | N/A | N/A | 1 | 1 | 0 | 1 |
| Singapore-UK DEA | 2022 | 2 | 2 | N/A | N/A | 0 | 2 | 0 | 1 |
| Australia Singapore Digital Economy Agreement (ASDEA) | 2020 | 1 | 2 | 0 | 0 | 0 | 2 | 0 | 2 |
| Chile - New Zealand Singapore Digital Economy Partnership Agreement (DEPA) | 2020 | 1 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| RCEP | 2020 | 1 | 2 | 2 | 2 | 2 | 2 | 0 | 0 |
| Singapore - UK FTA | 2020 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 |
| Australia-Indonesia CEPA | 2019 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 2 |
| EU Vietnam FTA | 2019 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 |
| CPTPP | 2018 | 2 | 2 | 2 | 2 | 2 | 0 | 2 | 2 |
| EU Singapore FTA | 2018 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 |
| Singapore Sri Lanka FTA | 2018 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 2 |
| Australia Singapore FTA | 2016 | 2 | 2 | 0 | 2 | 2 | 2 | 0 | 2 |
| Korea Vietnam FTA | 2015 | 1 | 0 | 2 | 0 | 0 | 2 | 0 | 0 |
| Singapore Turkey FTA | 2015 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| Chile Thailand FTA | 2013 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| Singapore Taipei (Taiwan) FTA | 2013 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| Australia Malaysia FTA | 2012 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 |
| ASEAN-Australia-New Zealand FTA (AANZFTA) | 2009 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| Panama Singapore FTA | 2006 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| India Singapore ECA | 2005 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| Korea Singapore FTA | 2005 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| Japan Singapore FTA | 2002 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 0 |
| New Zealand Singapore CEPA | 2000 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |

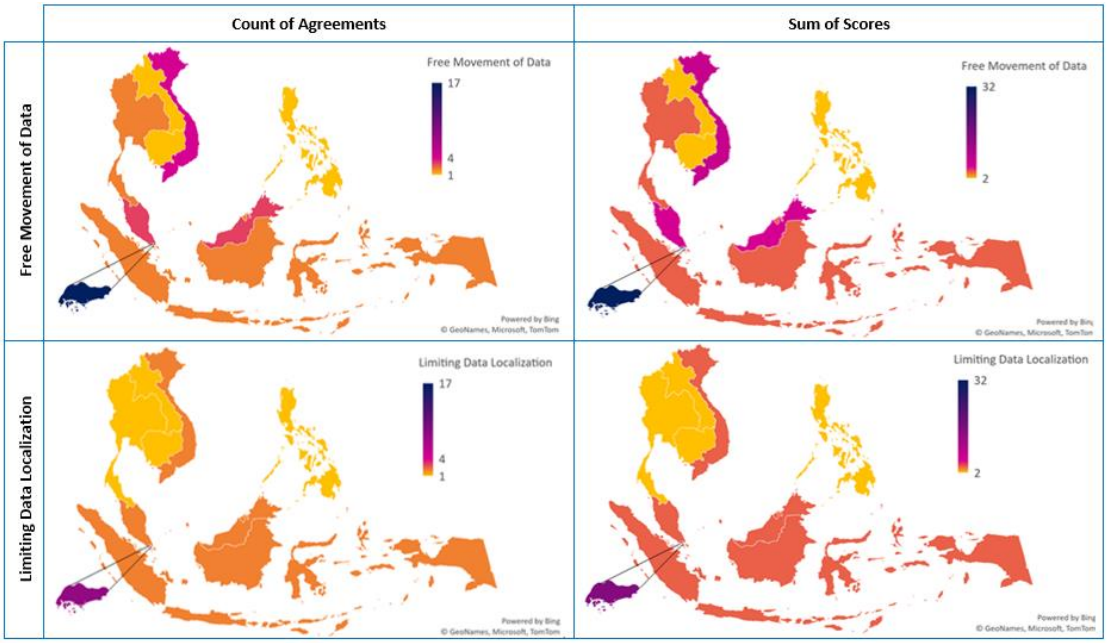


*Figure 2: ASEAN countries' counts and scores of relevant PTAs*

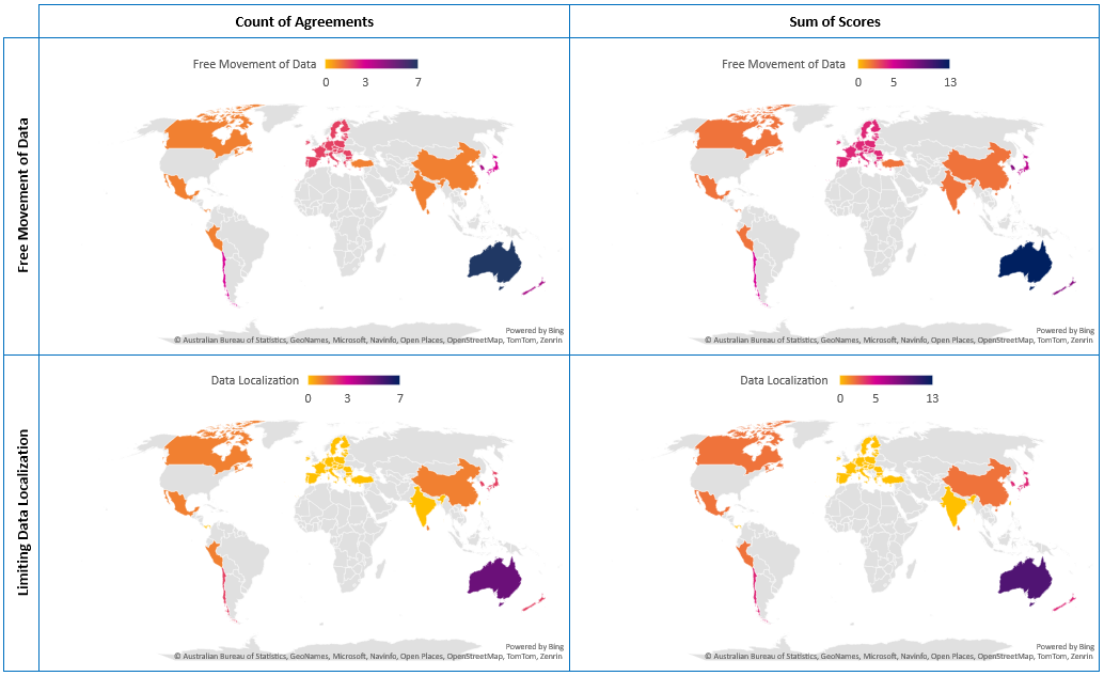


*Figure 3: Partner countries' counts and scores of relevant PTAs*

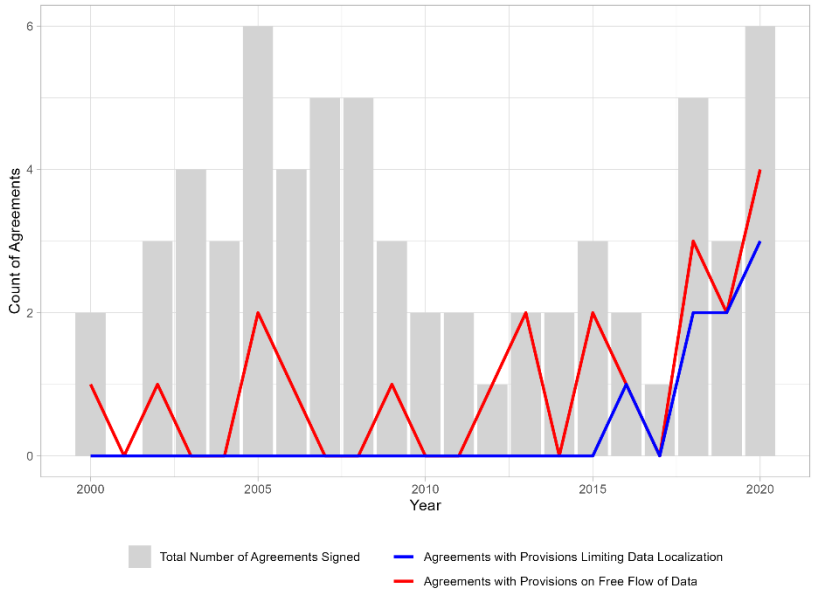


*Figure 4: Relevant Agreements in ASEAN over time, 2000-2020*

*Table 3: Comparison of number of trade agreements signed by any ASEAN country vs those signed by Singapore*

| | Signed by any country in ASEAN | Signed by Singapore |
|---|---|---|
| **Total Number of Trade Agreements** | 66 | 38 |
| **Total Number of Trade Agreements with Provisions on Free Data Flows** | 23 | 18 |
| **Total Number of Trade Agreements with Provisions on Limiting Data Localisation** | 9 | 8 |

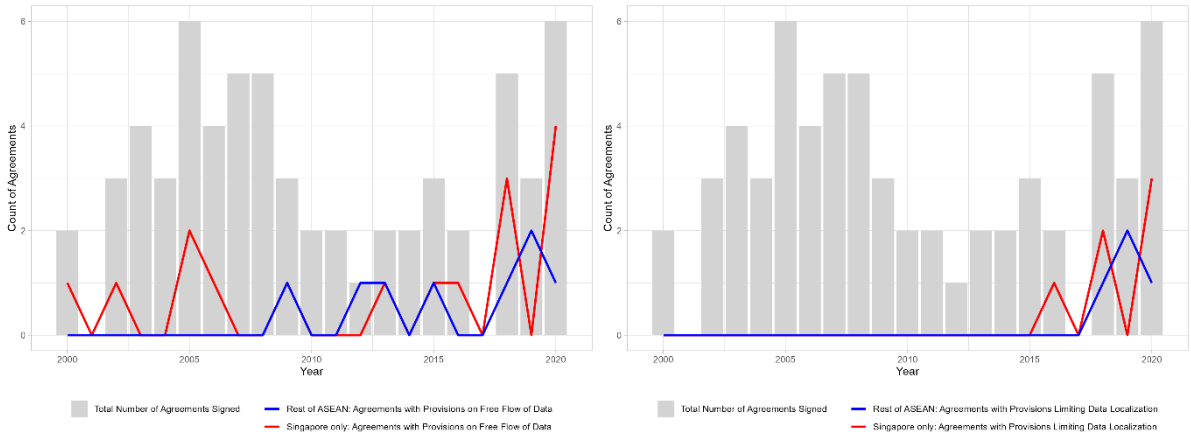


*Figure 5: Singapore (red) vs the rest of ASEAN (blue) for provisions on the free flow of data (left) and limiting data localization (right), 2000-2020*

Finally, to gauge the true impact of external influences through trade agreements on the domestic regulatory frameworks surrounding data governance, it is important to look at the exceptions that undermine the stringency of relevant clauses. While the employed dataset codes exceptions, these are coded at a very general level and cannot be traced back to which clause or which country they apply to. Therefore, a short qualitative review of relevant exceptions has been conducted and summarized in Table 4 below. The four relevant trade agreements that Vietnam is party and their key clauses both on free data flows and limiting data localization can be used as an example. RCEP and CPTPP include very similar clauses on both issues, however the exclusions are very different. While both exclude measures that are required to achieve legitimate public policy objectives, what constitutes these can be formally disputed under the CPTPP, whereas this is up to the implementing

party and cannot be disputed in RCEP. Additionally, whereas a country like Vietnam has obtained a two-year exclusion period under the CPTPP, it has obtained a five-year exclusion period under RCEP. The combination of these exclusions indicates that RCEP will, effectively, be much less strict on these matters than CPTPP. When including Vietnam's bilateral FTAs – the EU-Vietnam FTA and the Korea-Vietnam FTA – further differences between the relevant clauses emerge. For example, in the EU-Vietnam FTA no direct provision on free flow of data could be found, only that such data flows cannot be limited by imposing customs duties on electronic transmissions. While the Korea-Vietnam FTA does have a clearer provision on free data flows, this is limited to the financial service sector. Thus, while all of these agreements generally tackle the issues as coded, for a more fine-grained analysis a more detailed coding of the inclusions and exclusions would be necessary.

Besides trade agreements, ASEAN and the EU have recently launched an additional effort at facilitating cross-border data flows at the regional level. In May 2023, the first part of the "Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses" – the "Reference Guide" – was released, which aims to provide a comparison between the ASEAN MCCs and the EU SCCs (ASEAN Secretariat & European Commission, 2023). This will be followed up by an "Implementation Guide" that outlines best practices from businesses that have aligned their data handling practices complying with both regions' requirements. Although the joint guide does not provide any new legally binding provisions, the detailed comparison between the two regional mechanisms allows businesses that already have experiences with one of the two to easily understand what adaptations are needed to also become compliant with the other. Similarly, the planned implementation guide further aims to facilitate transfers by providing real-life business examples. Thus, while not influencing policy directly, such cross-regional initiatives may nevertheless play an important role in facilitating cross-border data transfers for businesses and may act as a first step towards deeper regulatory harmonization.

Overall, the findings in this section indicate increasing efforts in harmonizing data handling and transfer mechanisms between ASEAN member states and their trade partners. This is evident from the increasing number of trade agreements that include provisions on free data flows and limitations on data localization, which ASEAN countries have actively participated in. Singapore stands out as the leading member country, having signed the highest number of such agreements at an earlier stage. In terms of external partners, Australia emerges as a key country, having signed the most agreements of this nature.

However, the pace of harmonization is not entirely satisfactory, and the effectiveness of provisions for free cross-border data flows within these agreements is undermined by broad exceptions, with no trade agreement to which all ASEAN members are party having clear hard provisions, as Burri (2022) also confirms. External influence has proven insufficient to achieve comprehensive harmonization of cross-border data transfers. To address this challenge, in the next section, we propose a policy roadmap with specific actionable steps for national governments and ASEAN as a whole. This roadmap aims to facilitate data flows within the region and overcome existing obstacles.

*Table 4: Selected exceptions from treaties Vietnam is party to*

| *Trade Agreement* | Article | Exclusion |
|---|---|---|
| *CPTPP* | **Article 14.11: Cross-Border Transfer of Information by Electronic Means:** Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person. | **Measures to achieve legitimate public policy objectives.** Can be disputed using **dispute settlement mechanism** (Article 14.18): Malaysia and Vietnam excluded from dispute settlement for first 2 years. |
| | **Article 14.13: Location of Computing Facilities:** No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. | **Measures to achieve legitimate public policy objectives.** Can be disputed using **dispute settlement mechanism** (Article 14.18): Vietnam excluded from dispute settlement for first 2 years. |
| *RCEP* | **Article 14.11: Cross-Border Transfer of Information by Electronic Means:** Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person. | **Measures to achieve legitimate public policy objectives.** What constitutes a legitimate public policy objective is decided by the implementing party and **cannot be disputed**. Cambodia, Laos, and Myanmar are excluded for 5 years with an additional 3 years if necessary. Vietnam is excluded for 5 years |
| | **Article 14.13: Location of Computing Facilities:** No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. | **Measures to achieve legitimate public policy objectives.** What constitutes a legitimate public policy objective is decided by the implementing party and **cannot be disputed**. Cambodia, Laos, and Myanmar are excluded for 5 years with an additional 3 years if necessary. Vietnam is excluded for 5 years |
| *EU-Vietnam FTA* | **Article 8.51: Customs Duties:** The Parties shall not impose customs duties on electronic transmissions. | General exceptions relating to provisions on electronic commerce, including measures necessary to protect public security, human health, etc. |
| *Korea-Vietnam FTA* | **Article 10.2: Customs Duties:** A Party may not impose customs duties on electronic transmissions in compliance with any agreement relating to electronic commerce under the WTO, to which both Parties are party. | |
| | **Annex 8-A, Article 6: Data Processing:** Each Party shall permit a financial service supplier of the other Party to transfer information in electronic form, into and out of its territory, for data processing where such processing is required in the ordinary course of business. | Measures to **protect personal data, personal privacy**, and to require a financial service supplier to **obtain prior authorization from the relevant regulator** to transfer such information, based on prudential considerations |

## B. Policy Roadmap

In this section, we propose a policy roadmap with clear call-to-action items for both the ASEAN and the individual member states, which seeks to enhance cooperation and coordination among stakeholders, enabling more seamless data transfers and fostering an environment conducive to the region's data-driven growth.

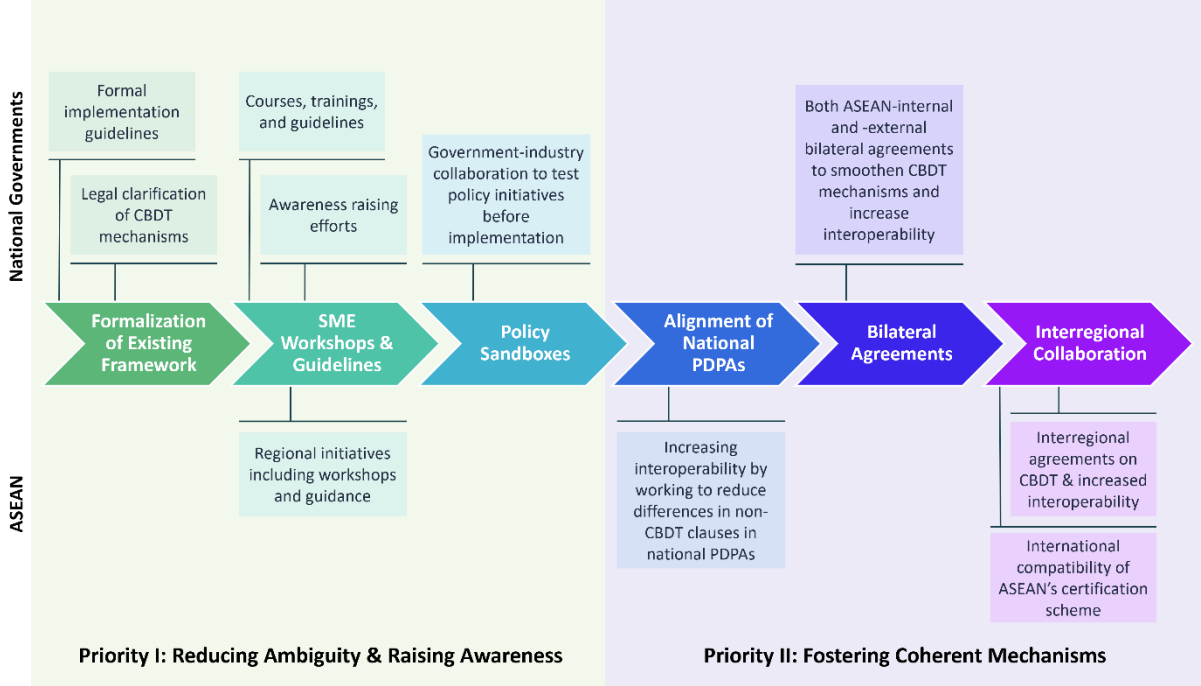


*Figure 6: Policy Roadmap*

### 1. ASEAN

The ASEAN MCCs have been an important first step in facilitating free data flows in the region. However, as discussed previously, two key issues that remain are the modifications required by national governments and the legal uncertainty surrounding their use in some ASEAN member states. While the first issue is more difficult to address as national interests and priorities in data protection may be different among ASEAN member states, the second should be a priority for governments. As all ASEAN member states have signed the MCCs, it is just a matter of formality to more clearly include them in their respective national personal data protection acts as well.

In addition to this, key problems remain for businesses in terms of interoperability. Besides just focusing on the MCCs and the direct cross-border data transfers, there is a role for regional organizations like ASEAN to also work on harmonizing some of the procedural and definition-related clauses within national level regulations. While, of course, issues of what constitutes sensitive data may be more challenging to reach agreements due to various national priorities, other clauses on how consent is given, when authorities must be notified, or what constitutes a data breach may be important first steps in simplifying the compliance burden for firms operating in multiple ASEAN jurisdictions. Moreover, addressing interoperability issues with key trading partners will further ease interregional data transfers. Here, the the recently published EU-ASEAN Joint Guide on MCCs and SCCs can be seen as a first step to ease the compliance burden on business, which can be deepened and/or expanded to include additional countries in the future.

Furthermore, ASEAN is currently working on its own certification mechanism that can be used by firms to transfer data between certified data handlers without further legal burdens. As the APEC CBPR have shown, this is a promising strategy. However, it again does not address interoperability issues between national regulations as discussed above. And equally importantly, it raises the question of how many different certifications are required before they too become a burden on firms rather than a helpful tool. If the ASEAN certification requirements are not significantly different from the CBPR demands, it may be more useful to firms if more ASEAN countries join the CBPR, or if the new ASEAN certification scheme is made compatible with existing certifications, to ensure that firms do not need to undergo multiple certification procedures to transfer data within its markets. Additionally, this would not just boost free data flows and its subsequent economic benefits within the ASEAN region but would also help to integrate the region better into the global data economy.

Besides harmonizing legislative frameworks at a regional level, ASEAN may also have a role to play at supporting SMEs in their pursuit to become compliant with national as well as regional data protection laws and agreements. On a regional level, MSMEs constitute between 97-99% of enterprises and 45% of GDP (Dunne et al., 2022). While MSMEs are more likely than large firms to be data non-users or passive users, in Europe between 40-57% of MSMEs are regular or advanced data users, while around 60% of large firms fall in that category (ASEAN, n.d.). Although comparable data is not available at the ASEAN level it is likely that similar trends would be observed with smaller firms handling data less than large firms but the share still being significant. Region-wide initiatives that specifically aim to support MSMEs in cross-border data transfers, such as training courses, clear guidelines, or workshops may be useful in boosting regional compliance with cross-border data transfer regulations and thus boosting data protection and privacy on a regional scale.

## 2. National Governments

To achieve the aims of promoting a more secure data economy, it is imperative that national governments do not see passing a national personal data protection act as the end of the road, but instead, work together with the private sector at all stages of the process to ensure its successful implementation and limit any negative side-effects on other parts of the economy. Additionally, although regional and large-scale international agreements and certification mechanisms may ultimately be the most effective in supporting the data economy, governments may use bilateral agreements on personal data protection standards and mechanisms as interim solutions.

Reducing policy uncertainty and compliance ambiguity is key to ensuring smooth business operations for firms active in the data economy. In the process of formulating new policies or regulations, sandboxes may provide a valuable avenue for both government and private sector stakeholders to collaboratively test and experiment with new policies for cross-border data transfers. This allows businesses to get acquainted with the regulations and how to adapt their operations to be compliant before the regulations enter into force, which ultimately protects data subjects' rights as well as any other national priorities that may be harmed by data leaks. As Shivi Anand, Grab's Regional Public Policy Manager highlights: "Policy sandboxes help companies understand the new legislative context and adapt internal practices accordingly. Legal precedents come too late for that". At the same time, policymakers can obtain deeper understanding of the challenges and concerns faced by private sector actors, leading to more informed and balanced policy decisions, and potentially reducing unintended negative side-effects of data protection regulations.

Once new policies have entered into force, national governments can reduce the uncertainty faced by firms regarding how they must be implemented and how they will be enforced. In many countries in ASEAN today, implementation and enforcement guidelines are communicated verbally in informal settings. Replacing such verbally communicated regulations during workshops with written guidance documents on implementation, accompanied by reasonable grace periods, can significantly enhance company compliance. This shift towards textual guidance offers greater clarity and specificity, ensuring that all businesses have access to clear instructions and requirements. Additionally, providing ample time for adjustment through grace periods gives companies time to reconfigure their data handling process, facilitating a smoother compliance process for companies, and greater societal benefits as the approach taken is less likely to be haphazard and incomplete.

These efforts must be complemented by compliance support especially for SMEs, including courses and workshops to raise awareness as well as formal guidelines and support structures during the implementation process to ensure that SMEs do not only receive a first push but are supported throughout the whole compliance process. In the region, the Singaporean government's and personal data protection commission's efforts may be a good example for other actors in the region, as they have provided a vast array of free and paid resources for local businesses to become aware of and receive basic training in PDPA compliance.

Furthermore, national governments can help tackle issues arising for firms in cross-border data transfers. Ideally, coherent policy and regulatory frameworks to manage international data flows could be set up internationally between as many countries as possible. However, even at a regional level this process can be slow and tedious, and therefore governments can engage in bilateral discussions and agreements as interim solutions. Besides aligned cross-border data transfers rules as well as the interoperability of national personal data protection regimes to be truly effective. If aspects like the legal basis of data processing – when data can be collected from an individual and used for certain purposes – are not aligned internationally, multinational business continue to face operational complexity as they must configure their data processing activities differently in each country. Bilateral coordination of such requirements to create a more uniform system would facilitate businesses to make use of data from across the region until an ASEAN-level or other international agreement can be reached.

# VII. Conclusion

The combination of an assessment of the current situation of personal data protection regulations, and especially policies on cross-border data flows, and interviews with data-driven businesses have shown that fundamental challenges within ASEAN's data-policy landscape remain: (1) Whereas initiatives like the ASEAN Model Contractual Clauses have been a useful first step towards simplifying international data transfers, these will only be fully effective if national adaptations are not needed and if all member states formally include them in their respective national legal frameworks. (2) Besides direct cross-border mechanisms the lack of uniformity in the underlying personal data protection acts still severely hinders smooth cross-border business operations. And (3) especially SMEs face severe cost- and knowledge-barriers to compliance and may thus either put user or nationally important data at risk or be left behind as economic digitalization advances.

Within the ASEAN data-policy space a small cluster of countries – Singapore, Australia, and New Zealand especially – have been identified to play an outsized role in policy making. This may be beneficial not only for driving the data agenda forward and adapting it to technological and societal developments, but also in working towards an increasing unification in approaches within trade agreements the region participates in. However, as mega-regional trade agreements with binding clauses on cross-border data flows are likely to take significant amounts of time to negotiate and implement, it is important that national governments as well as regional organizations take smaller steps to facilitate this process and facilitate data flows in the near term. This includes formalizing existing policy frameworks, supporting SMEs in the compliance process, smoothing the policy implementation process through policy sandboxes, and working bilaterally to align national PDPAs and create new data flow agreements.

# VIII. References


Aaronson, S. A. (2019). Data is different, and that's why the world needs a new approach to governing cross-border data flows. *Digital Policy, Regulation and Governance*, *21*(5), 441–460.

AMTC. (2018). *Micro-revolution: The new stakeholders of trade in APAC*. Asia Pacific MSME Trade Coalition. https://accesspartnership.com/wp-content/uploads/2023/01/singles-msme-report-apac.pdf

APEC. (2023, June). *What is the Cross-Border Privacy Rules System*. Asia-Pacific Economic Cooperation. https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system

ASEAN. (n.d.). *Development of Micro, Small, and Medium Enterprises in ASEAN (MSME)*. ASEAN.Org. Retrieved 19 July 2023, from https://asean.org/our-communities/economic-community/resilient-and-inclusive-asean/development-of-micro-small-and-medium-enterprises-in-asean-msme/

ASEAN Secretariat, & European Commission. (2023). *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*. https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf

BakerMcKenzie. (n.d.). *Global Data Privacy & Security Handbook*. Baker McKenzie Resource Hub. Retrieved 19 July 2023, from https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security

BakerMcKenzie. (2021, November 2). *ASEAN: Adopting the ASEAN Model Contractual Clauses for cross-border data transfers*. Baker & McKenzie. https://insightplus.bakermckenzie.com/bm/data-technology/asean-adopting-the-asean-model-contractual-clauses-for-cross-border-data-transfers_1

Bauer, M., Lee-Makiyama, H., Van der Marel, E., & Verschelde, B. (2014). *The costs of data localisation: Friendly fire on economic recovery*. ECIPE Occasional Paper.

Burri, M. (2022). Approaches to digital trade and data flow regulation across jurisdictions: Implications for the future ASEAN-EU agreement. *Legal Issues of Economic Integration*, *49*(2).

Burri, M., Vasquez Callo-Mueller, M., & Kugler, K. (2022). *TAPED: Trade Agreement Provisions on Electronic Commerce and Data*. https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/

Casalini, F., González, J. L., & Nemoto, T. (2021). *Mapping commonalities in regulatory approaches to cross-border data transfers*.

Chin, Y.-C., & Zhao, J. (2022). Governing cross-border data flows: International trade agreements and their limits. *Laws*, *11*(4), 63.

Chow, Desmond (P2D Solutions). (2023, June 19). *Experience with ASEAN Cross-Border Data Flow Policies* [Personal interview].

Dunne, A., Gomez, M. F., Gosse, J., Hoffreumon, C., von Zeebroeck, N., & Bughin, J. (2022). *Survey of Businesses on the Data Economy*. European Commission, Ipsos Belgium, iCite. https://digital-strategy.ec.europa.eu/en/library/survey-businesses-data-economy-2022

EU-ASEAN Business Council. (2020). *Data Governance in ASEAN: From Rhetoric to Reality*. https://www.eu-asean.eu/wp-content/uploads/2022/02/DATA-GOVERNANCE-IN-ASEAN-FROM-RHETORIC-TO-REALITY-2020.pdf

Ferracane, M. F., & van der Marel, E. (2021). Regulating Personal Data. *World Development Report 2021 Background Paper*.

Girot, C. (2018). *Regulation of Cross-Border Transfers of Personal Data in Asia*. Asian Business Law Institute.

Global Data Alliance. (2023). *Cross-Border Data Policy Index*. https://globaldataalliance.org/resource/cross-border-data-policy-index/

González, J. L., Sorescu, S., & Kaynak, P. (2023). *Of bytes and trade: Quantifying the impact of digitalisation on trade* (273; OECD Trade Policy Papers). OECD. https://doi.org/10.1787/11889f2a-en

Goodman, M. P., & Risberg, P. (2021). *Governing Data in the Asia-Pacif ic* (CSIS Briefs). Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210420_Goodman_Governing_Data_Asia-Pacific_1.pdf?VersionId=vb_GpIqV2cC5Wg6zKXIfC1MXNgfvU2w8

Google, Temasek, & Bain 7 Company. (2022). *E-Conomy SEA 2022*. https://economysea.withgoogle.com/report/

Government of Vietnam. (2023, April 17). *Nghị định 13/2023/NĐ-CP bảo vệ dữ liệu cá nhân*. Thư Viện Pháp Luật. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx

Greenleaf, G. (2021). ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4027670

GSMA. (2018). *Regional Privacy Frameworks and Cross-Border Data Flows How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

IMDA Singapore. (2023a, July 13). *Directory of APEC Cross Border Privacy Rules (CBPR) Certified Organisations*. Infocomm Media Development Authority. https://www.imda.gov.sg/how-we-can-help/cross-border-privacy-rules-certification/cbpr-certified-organisations

IMDA Singapore. (2023b, July 13). *Directory of APEC Privacy Recognition for Processors (PRP) Certified Organisations*. Infocomm Media Development Authority. https://www.imda.gov.sg/how-we-can-help/privacy-recognition-for-processors-certification/prp-certified-organisations

International Trade Administration. (2022, February 17). *Thailand Personal Data Protection Act*. International Trade Administration. https://www.trade.gov/market-intelligence/thailand-personal-data-protection-act

Kennedy, G. (2021, February 8). *Finding Harmony – ASEAN Model Contractual Clauses and Data Management Framework Launched*. Mayer | Brown. https://www.mayerbrown.com/en/perspectives-events/publications/2021/02/finding-harmony-asean-model-contractual-clauses-and-data-management-framework-launched

Khumon, P. (2018). Regulation for Cross-Border Privacy in Southeast Asia: An Institutional Perspective. *29th European Regional Conference of the International Telecommunications Society (ITS): 'Towards a Digital Future: Turning Technology into Markets?', Trento, Italy, 1st - 4th August, 2018, International Telecommunications Society (ITS)*.

Khumon, P. (2023, January 31). *Grab Conversations: Data Protection in SEA Ep 2 (Thai perspective)* (S. Anand, Interviewer) [Interview]. https://www.grab.com/sg/blog/public-policy/grab-conversations-data-protection-in-sea-ep-2-thai-perspective/

Lee, Jeth (Microsoft). (2023, May 31). *Experience with ASEAN Cross-Border Data Flow Policies* [Personal interview].

Lim, E. (2020). *Industry Consultations on ASEAN Cross Border Data Flows Mechanism: Model Contractual Clauses*. BSA | The Software Alliance. https://www.bsa.org/files/policy-filings/10062020singaporeaseanmccconsultation.pdf

Lim, J. (2021). Bite the Bullet: The Future of Data Protection Law and Policy in ASEAN. *ASEAN Ideas in Progress Series*, *4*.

Lim, J. Z., Toh, M. H., & Xie, T. (2023). Evaluating the Impact of Digital Economy Collaborations in ASEAN: A Computable General Equilibrium Approach. In P. Cheung & T. Xie (Eds.), *The ASEAN Digital Economy* (1st ed., pp. 8–27). Routledge.

Liu, H.-W. (2018). Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism. *ASEAN Law in the New Regional Economic Order: Global Trends and Shifting Paradigms, Cambridge University Press (Pasha L. Hsieh & Bryan Mercurio Eds., 2019)*.

Liu, J., Sengstschmid, U., & Ge, Y. (2023). *Facilitating Data Flows Across ASEAN: Challenges and Policy Directions* (SSRN Scholarly Paper 4547683). https://doi.org/10.2139/ssrn.4547683

Mitchell, A. D., & Mishra, N. (2019). Regulating cross-border data flows in a data-driven world: How WTO Law can contribute. *Journal of International Economic Law*, *22*(3), 389–416.

PDPC Singapore. (2021). *Guidance for use of ASEAN model contractual clauses for cross border data flows in Singapore*. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.pdf

PDPC Singapore. (2020, June 2). *Singapore Now Recognises APEC CBPR and PRP Certifications Under PDPA*. Personal Data Protection Commission Singapore. https://www.pdpc.gov.sg/News-and-Events/Announcements/2020/06/Singapore-Now-Recognises-APEC-CBPR-and-PRP-Certifications-Under-PDPA

Ryngaert, C., & Taylor, M. (2020). The GDPR as Global Data Protection Regulation? *American Journal of International Law*, *114*, 5–9. https://doi.org/10.1017/aju.2019.80

Spiezia, V., & Tscheke, J. (2020). *International agreements on cross-border data flows and international trade: A statistical analysis*.

Suvannaphakdy, S. (2023, February 17). *Fragmented Digital Regulations are Constraining ASEAN's Digital Economy*. FULCRUM. https://fulcrum.sg/fragmented-digital-regulations-are-constraining-aseans-digital-economy/

US-ASEAN Business Council. (2019). *Digital Data Governance in ASEAN: Key Elements for a Data-Driven Economy*. https://www.usasean.org/system/files/downloads/digital_data_governance_in_asean-key_elements_for_a_data-driven_economy.pdf