Asian Journal of International Law, 10 (2020), pp. 158–180
doi:10.1017/S2044251319000250
© Asian Journal of International Law, 2019
First published online 23 December 2019

Data Localization and ASEAN Economic Community

Benjamin WONG*
National University of Singapore, Singapore *benjamin.wong@nus.edu.sg*

Abstract
Data localization is a phenomenon that is of increasing global significance, as a growing number of countries impose data localization requirements on data controllers. This paper discusses data localization in the ASEAN context. It proposes a schema of data localization laws which comprises two categories of data localization requirements. This schema is used to examine data localization laws within ASEAN, and it will be shown that there is presently a moderate level of data localization among ASEAN Member States. The paper then discusses how data localization is dealt with in the EU and in ASEAN, addressing some recent developments in the two regimes. It concludes with recommendations for ASEAN's approach to data localization, drawing from the EU regime.

I. THE PROBLEM OF DATA LOCALIZATION

The cross-border flow of data is an essential aspect of the modern world economy. It enables firms to trade and operate internationally, while providing consumers with access to the global market for goods and services. The free flow of data across borders is also a prerequisite for the functioning of the Internet as an unparalleled source of information and mode of communication, offering undeniable benefits to individuals in both developed and developing countries. The Internet economy, which is of growing significance to Southeast Asia, depends upon the free movement of data across national boundaries.[1] Industries outside the Internet economy have also grown

* LLB (National University of Singapore); Advocate and Solicitor (Singapore). Sheridan Fellow, Faculty of Law, National University of Singapore, Singapore. The author would like to thank Teo Jen Min for her invaluable research assistance. Special thanks are owed to Tan Hsien-Li for her helpful pointers, and to the anonymous reviewers for their insightful comments. All errors remain solely the author's own.

1. A recent study has found that the Southeast Asian Internet economy (comprising ride-hailing, online media, online travel, and e-commerce) reached $72bn in 2018, and is projected to grow to $240bn in 2025 to make up eight percent of Southeast Asia's gross domestic product. See Rajan ANANDAN et al., "e-Conomy SEA 2018: Southeast Asia's Internet Economy Hits an Inflection Point", online: <https://www.thinkwithgoogle.com/_qs/documents/6870/Report_e-Conomy_SEA_2018_by_Google_Temasek_121418_cpsLjlQ.pdf>.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

increasingly reliant on their ability to move data across borders; this ability enables firms to obtain, among other things, access to such third-party services as cloud computing, data analytics, and payroll management from foreign service providers.

Data localization, however, has introduced a degree of friction to the cross-border movement of data. Data localization describes the phenomenon wherein a country causes data to be kept within the geographical territory of that country. Countries achieve data localization in large part by imposing data localization requirements on entities who possess or control data (hereinafter referred to as "data controllers"). Data localization requirements may either prevent data controllers from moving data out of the territory, or force data controllers to perform certain actions on data within the territory; both types of data localization requirements inhibit the flow of data across borders.

There are often legitimate reasons for a country to impose data localization requirements. However, a key concern is that data localization serves as an inhibitor of trade in services and, more generally, as an obstacle to economic integration. Much has also been said in the (predominantly negative) academic commentary on the potential harms caused by data localization: having detrimental effects on data security, raising the costs of doing business, inhibiting the development of certain industries, facilitating government surveillance and oppression, and posing a threat to the functioning of the Internet.[2]

Data localization requirements have proliferated in the international arena, as an increasing number of countries impose rules forcing data to be kept within their own territories. In Asia, a notable recent example of data localization is found in China's Cybersecurity Law, which provides that operators of key information infrastructure in China who collect or produce personal data or important information must store the data within China.[3] The Indian government has also published a draft data protection bill which seeks to impose restrictions on the cross-border transfer of personal data outside India, and contains a requirement for data fiduciaries to store at least one copy of their personal data within India.[4]

Southeast Asia is no exception to this trend. Southeast Asian countries have, too, begun to impose various forms of data localization requirements. While there are often good reasons for these data localization requirements, there is a risk that they may hinder regional economic integration. This risk calls for a principled, predictable, and rules-based approach to data localization. In this regard, the Association of Southeast Asian Nations [ASEAN] may serve well as a platform upon which ASEAN Member States can develop a co-ordinated approach to data localization.[5]

---

2. See Anupam CHANDER and Uyên P LÊ, "Data Nationalism" (2015) 64 Emory Law Journal 677 at 679–81; Konstantinos KOMAITIS, "The "Wicked Problem" of Data Localization" (2017) 2 Journal of Cyber Policy 355 at 357–62; Erica FRASER, "Data Localisation and the Balkanisation of the Internet" (2016) 13 SCRIPTed 359.

3. *Cyber Security Law of the People's Republic of China*, art. 37.

4. *Personal Data Protection Bill 2018*, ss. 40, 41.

5. ASEAN consists of ten Southeast Asian Member States: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam. It has been argued that free trade agreements are in a better position than the international trade rules to address data localization measures: see Mira BURRI, "The Regulation of Data Flows Through Trade Agreements" (2017) 48 Georgetown Journal of International Law 407 at 443.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

This paper will focus on data localization in the context of ASEAN economic integration. The question this paper seeks to address is: How should ASEAN, as a regional economic community, approach the issue of data localization? The rest of the paper is organized as follows. Part II discusses how data localization is dealt with under the existing rules of international trade law, and the role that ASEAN can play in regulating the practice of data localization. Part III examines the current state of data localization laws in the ASEAN Member States, using a simple comparative framework. Part IV looks to the European Union [EU], which has recently made significant advances in dealing with the problem of data localization, as a potential source of insights applicable to the ASEAN context. Part V provides an analysis of how data localization is presently dealt with under existing ASEAN norms, and proposes improvements to ASEAN's approach to data localization. Part VI concludes.

II. DATA LOCALIZATION, INTERNATIONAL TRADE, AND THE ROLE OF ASEAN

Data localization requirements may have "potentially significant trade implications".[6] They may be inconsistent with countries' trade liberalization obligations, as they have the effect of a non-tariff barrier to trade in services.[7] Indeed, it has been alleged that countries are engaging in the practice of "data protectionism", and that some data localization requirements "appear to be motivated by traditional protectionist impulses to increase local investment and employment opportunities".[8]

Because of its trade implications, data localization is to some extent regulated by the international trade rules of the World Trade Organization [WTO]. It is necessary to first examine how the WTO rules apply to data localization, as a baseline, in order to answer the question of what role ASEAN has to play in regulating data localization. This paper proceeds to discuss the application of WTO rules to data localization.

A. *Data Localization Under WTO Rules*

Data localization requirements may contravene the rules under the General Agreement on Trade in Services [GATS].[9] The GATS applies to measures affecting

6. United Nations Conference on Trade and Development [UNCTAD], "Data Protection Regulations and International Data Flows: Implications for Trade and Development" (United Nations 2016) at 14.

7. Non-tariff barriers have been recognized as having the potential to "undermine the economic integration process" and the realization of an economic community in ASEAN: see Myrna S AUSTRIA, "Non-Tariff Barriers: A Challenge to Achieving the ASEAN Economic Community" in Sanchita Basu DAS, Jayant MENON, Rodolfo SEVERINO, and Omkar Lal SHRESTHA, eds., *The ASEAN Economic Community: A Work in Progress* (Singapore: ISEAS Publishing, 2013), at 32.

8. Burri, *supra* note 5 at 448; Susannah HODSON, "Applying WTO and FTA Disciplines to Data Localization Measures" (2019) 18 World Trade Review 579 at 581.

9. For more comprehensive analyses on how the GATS applies to data localization, see Hodson, *supra* note 8; Diane A. MACDONALD and Christine M. STREATFEILD, "Personal Data Privacy and the WTO" (2014) 36 Houston Journal of International Law 625; Mira BURRI, "The Governance of

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

trade in services, covering four possible modes of trade in services across borders.[10] Under the GATS, WTO members are subject to various obligations to liberalize trade in services. Some GATS obligations are of general application, applying to all WTO members and all service sectors.[11] Other obligations are specific, and function on the basis of commitments that WTO members have made in respect of specific service sectors. WTO members may lay down commitments to permit access to foreign services and service suppliers into their markets (market access commitments) under Article XVI, and commitments to treat foreign services and service suppliers no less favourably than their domestic counterparts (national treatment commitments) under Article XVII.

GATS market access obligations may apply to data localization requirements, because such requirements may serve as barriers to the cross-border provision of services by foreign service suppliers. For example, if Country A imposes a strict rule against the transfer of data out of its territory, such a rule will prevent a foreign data storage firm (whose servers are located in Country B) from providing data storage services to customers in Country A. The foreign data storage firm may then have to forgo entry to Country A's market, or incur significant costs to site data storage facilities within the territory of Country A.[12]

Another simple example may be given in relation to medical services. If Country A imposes a data localization measure to the effect that Patient X's medical data must be kept within the territory of Country A and not transferred outside Country A, such a requirement could restrict the ability of a medical service provider in Country B to provide medical services to Patient X in Country B. This is because reference to a patient's medical records may be necessary for the provision of medical treatment to that patient, and the data localization measure imposed by Country A prevents the transfer of Patient X's medical records to the medical service provider located in Country B.[13]

However, although data localization can pose barriers to trade, it cannot be gainsaid that countries have legitimate concerns relating to the movement of data out of their territories. There can be a diverse range of objectives underlying data localization requirements, including "privacy, cybersecurity, national security, public order, law enforcement, taxation, and industrial development, among others".[14] Under

---

Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation" (2017) 51 UC Davis Law Review 65.

10. *General Agreement on Trade in Services*, art. 1. Mode 1, where the service is provided from the territory of one country into the territory of another, is of particular relevance here, because these are the services that are the most likely to be affected by data localization requirements. Mode 2, where the service is provided in the territory of one country to the consumer of another country, may also be implicated.

11. For example, the Most Favoured Nation treatment obligation under art. II and the transparency obligation under art. III.

12. This is an example of a restriction on Mode 1 trade in services, where the service moves across the border.

13. This is an example of a restriction on Mode 2 trade in services, where the customer moves across the border.

14. Martina F. FERRACANE, "Restrictions on Cross-border Data Flows: A Taxonomy" (2017) ECIPE Working Paper 1/2017 at 5.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

the GATS, countries are permitted to derogate from their trade liberalization commitments on the basis of specified countervailing public policy objectives. Data localization requirements may be exempted under Article XIV, which exempts measures necessary to maintain public order and to secure compliance with laws or regulations, among other things. Article XIVbis can also exempt data localization measures as measures necessary to protect national security interests.

Here, some legitimate public policy objectives that are relevant to data localization may be suggested.[15] First, a key justification for data localization is that of national security. There is now a recognition of cyberspace as a domain of military operations (the newest addition to the conventional domains of land, air, sea, and space), and there are growing concerns over the risks of cyber espionage.[16] The gathering of data by foreign adversaries through surveillance and intelligence operations poses a threat to national security, because that data can be used to discover and exploit a country's vulnerabilities. By data localization, countries hope to prevent potentially sensitive data from falling into the wrong hands. Even though data localization may not offer complete protection against a determined and well-resourced adversary, it can still increase the costs of data-gathering operations.[17]

Second, the need of state agencies to access data is another justification for data localization. A law enforcement agency, for example, may require electronic evidence relating to suspected criminal activity, and it is simply easier for the law enforcement agency to demand and obtain access to that electronic evidence if it is stored in a location over which the law enforcement agency has jurisdiction. Where data is stored locally, law enforcement agencies can use local processes to gain access to the data. Where the data is stored offshore, however, such processes are not available, limiting the law enforcement agency's access to the data. While it is in theory possible for the law enforcement agency to request co-operation from foreign data controllers or foreign state agencies, there is no guarantee that such co-operation will be forthcoming, particularly where the law enforcement agency has weak leverage over the foreign entities.

Third, the protection of individual privacy is a "legitimate policy objective which should be accommodated in trade rules governing data transfers".[18] Countries afford varying levels of protection to personal data, with some countries offering little to no legal protection. If a data controller is permitted to transfer personal data from a protective country to a less-protective country, the data controller may effectively circumvent the protections offered by the protective country. There is therefore a need for protective countries to ensure that personal data that is transferred out of their territories will continue to receive an adequate level of protection. This is ordinarily achieved by imposing a requirement for data controllers to ensure that the recipient country confers a comparable level of protection, and/or a requirement for data

15. See also John SELBY, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" (2017) 25 International Journal of Law and Information Technology 213.

16. Gian Piero SIROLI, "Considerations on the Cyber Domain as the New Worldwide Battlefield" (2018) 53 International Spectator 111.

17. Selby, *supra* note 15 at 228.

18. Hodson, *supra* note 8 at 3.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

controllers to implement added safeguards for personal data that they wish to transfer out of the territory.

It has sometimes been asserted that data localization requirements are ineffective in achieving their purported objectives,[19] and that broadly framed data localization requirements which are more restrictive than necessary to achieve their policy objectives tip into data protectionism.[20] However, in the author's view, a blanket rejection of data localization cannot be sustained, because the actual motivations and consequences of particular data localization requirements are ultimately fact-specific.

B. *A Role for ASEAN in Regulating Data Localization*

While the GATS can work to discipline data localization requirements, it has certain limits in this regard. It does not contain provisions dealing explicitly with data localization, nor is there WTO jurisprudence expressly considering data localization, with the consequence that there is "significant legal uncertainty" about how data localization requirements will be treated under the GATS.[21] Hodson has provided an excellent analysis of how data localization may fit within the GATS legal framework,[22] which reveals that the fit is a rather awkward one. For example, to make the claim that a data localization requirement has contravened the GATS market access obligation, that data localization requirement would have to be framed as a limitation on the "total number of service operations or on the total quantity of service output expressed in terms of designated numerical units" in the form of a quota, thereby violating Article XVI(2)(c);[23] this requires a fairly liberal reading of Article XVI(2)(c),[24] and even then it is questionable whether it will successfully catch all forms of trade-restrictive data localization requirements. There are also difficulties with framing data localization requirements to fit the Article XIVbis security exemption, as it is not clear which of the clauses under Article XIVbis would exempt data localization requirements imposed (during peacetime) for the purposes of national security. Finally, the GATS market access obligation is commitment-based, so if a WTO member has not made a relevant commitment, the market access obligation will pose no constraints on that WTO member's ability to impose data localization requirements. These are structural difficulties which are unlikely to be resolved soon.

In view of the foregoing limits of the GATS, it is suggested that ASEAN is an appropriate forum for the regulation of data localization in the Southeast Asian

19. Chander and Lê, *supra* note 2 at 713–35. Commenters have suggested, for example, that data localization requirements do not in fact enhance data security—what really matter are the security practices adopted to protect the data, wherever the data is located.

20. Ike BRANNON and Hart SCHWARTZ, "The New Perils of Data Localization Rules" (2018) 41 Regulation 12 at 12.

21. Hodson, *supra* note 8 at 18.

22. *Ibid.*, at 5–19.

23. *Ibid.*, at 13.

24. This difficulty is not limited to data localization requirements: see Mitsuo MATSUSHITA and Aya IINO, "Cross-Border Gambling and Betting Services Under WTO Disciplines" (2006) 1 Asian Journal of Comparative Law 1 at 14.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

region. As Burri has noted, preferential trade venues "benefit from swifter solutions, clearer provisions, as well as often deeper commitments".[25] Elsewhere, attempts have already been made to solve the data localization problem through non-WTO solutions. One example may be found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP], to which four ASEAN Member States are signatories:[26] Chapter 14 of the CPTPP, addressing electronic commerce, contains provisions that deal directly with data localization. Article 14.11 provides that parties must permit the cross-border transfer of information by electronic means for the conduct of business by covered persons, while Article 14.13 prohibits any party from requiring a covered person to use or locate computing facilities in the territory of that party as a condition for conducting business in their territory.[27] This is evidence that plurilateral and regional fora can be viable platforms for addressing the issue of data localization.

There are good reasons for ASEAN to set its own clear regional standards for data localization. ASEAN can account for regional characteristics and the particular interests of its Member States, making standards that work for all its Member States. These standards can curb temptations to engage in data protectionism, ensuring that short-term domestic gains are not prioritized over the economic needs of the region.[28] At the same time, these standards can account for the particular legitimate needs of ASEAN Member States to localize data in certain circumstances. Regional standards will also enable ASEAN to act in unity when engaging in trade negotiations with other entities.

III. DATA LOCALIZATION IN ASEAN MEMBER STATES

In this section, the paper examines the current state of the law in ASEAN Member States. Since ASEAN Member States have implemented a variety of data localization requirements, it is necessary to first establish a clear comparative framework upon which these data localization requirements can be analyzed. The paper proceeds to set out that comparative framework, drawing on similar frameworks proposed by other authors.

A. *Comparative Framework*

Several authors have sought to establish taxonomic systems to classify data localization requirements.[29] For example, Kaplan and Rowshankish have suggested that there

25. Burri, *supra* note 9 at 127.
26. Namely Brunei, Malaysia, Singapore, and Vietnam.
27. To be clear, it is not suggested here that ASEAN should simply adopt the CPTPP solution.
28. As will be discussed in Part V below, the practice of data localization by ASEAN Member States may detract from ASEAN's drive towards greater regional economic integration.
29. See James M. KAPLAN and Kayvaun ROWSHANKISH, "Addressing the Impact of Data Location Regulation in Financial Services" (2015) Global Commission on Internet Governance Paper Series

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

are four categories of data localization regulations. In decreasing degrees of stringency, they are: (2) geographical restrictions on data export; (2) geographical restrictions on data location; (3) permission-based regulations; and (4) standards-based regulations.[30] Geographical restrictions on data export require that data controllers keep their data within the geographical bounds of the country, entirely preventing the transfer of any copy of the data out of the country. Geographical restrictions on data location require that data controllers keep a local copy of their data within the geographical bounds of the country, but permit the transfer of other copies of that data out of the country. Permission-based regulations require that data controllers obtain permission or consent from data subjects before transferring their data out of the country. Standards-based regulations require that data controllers meet certain standards relating to privacy and security before they are permitted to transfer data out of the country.

It is argued that a simpler approach is to focus on the necessary distinction between two types of data localization requirements, namely: (1) local processing requirements, which require data controllers to process data within the territory of the country, and (2) transfer limitation requirements, which restrict the transfer of data out of the territory of the country.[31] This approach is simpler because it avoids the need to generate a multiplicity of categories, while exhaustively covering the types of data localization requirements that countries may impose. It is broadly aligned with the taxonomic system proposed by Ferracane, who categorizes restrictions on data flow into "strict" restrictions and "conditional" restrictions, where strict restrictions are those that require data to be stored locally, while conditional restrictions are those that impose conditions on the cross-border transfer of data.[32] Likewise, Casalini and López González have proposed two indicative taxonomies of cross-border data regulations, the first dealing with restrictions on cross-border data flow and the second dealing with local storage requirements.[33]

Accordingly, it is suggested that a straightforward comparative framework would be to ask two separate questions about the regulatory regime of each country under investigation. The first question is the "local processing" question: What requirements are there on data controllers to process data within the territory of the country? Examples of local processing requirements include requirements to keep a local copy of the data (local copy requirement) and requirements to perform certain actions on the data locally (local action requirement). The second question is the "transfer limitation" question: To what extent is the data controller restricted from transferring

14/2015; Ferracane, *supra* note 14; Francesca CASALINI and Javier López GONZÁLEZ, "Trade and Cross-Border Data Flows" (2019) OECD Trade Policy Papers 220.

30. Kaplan and Rowshankish, *supra* note 29 at 1–2.

31. The distinction is necessary because these two types of data localization restrictions differ in kind and not merely in degree: local processing requirements mandate that data controllers do certain things with their data locally, but they say nothing about whether the data can be transferred out of the country, while restrictions on transfer of data prevent data from leaving the country, but are silent on what must be done with the data in the country.

32. Ferracane, *supra* note 14 at 3.

33. Casalini and López González, *supra* note 29 at 16.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

a copy of the data out of the country? This question admits a range of answers, ranging from "absolute restriction on transfer" through "qualified restriction on transfer" to "no restriction on transfer". It is this two-question analysis that this paper will apply going forward.

Having set out the comparative framework, this paper will now apply that framework in examining the data localization requirements that have, to date, been imposed by ASEAN Member States.[34] Best efforts have been made here to be as accurate as possible. This survey focuses on general, rather than sector-specific, data localization requirements.

B. *Brunei*

No existing data localization requirements imposed by Brunei were found.[35]

C. *Cambodia*

No existing data localization requirements imposed by Cambodia were found.

D. *Indonesia*

Data localization requirements are imposed by Government Regulation No 82 of 2012 concerning Operation of Electronic Systems and Transactions [Indonesia OEST Regulation]. Article 17(2) of the Indonesia OEST Regulation stipulates that operators of electronic systems for public services must locate data centres and disaster recovery centres in Indonesia for the purposes of law enforcement, protection, and the enforcement of Indonesia's national sovereignty over the data of its citizens. This provision has the effect of imposing both local copy and local action requirements.[36]

Ministerial Regulation No 20 of 2016 concerning Protection of Personal Data in Electronic Systems [Indonesia PPDES Regulation] was passed pursuant to Article 15 (3) of the Indonesia OEST Regulation. Article 22 of the Indonesia PPDES Regulation specifies that operators of electronic systems domiciled in Indonesia transferring personal data outside Indonesia must co-ordinate with relevant authorities by reporting certain information relating to the transfer—it is, however, not clear if approval from said authorities must be obtained for the transfer. In any case, Article 22 imposes a qualified restriction on the transfer of personal data out of Indonesia.

In addition, Article 17(1) of the Indonesia PPDES Regulation specifies that data centres and disaster recovery centres of operators of electronic systems for public

34. As of 15 April 2019.

35. The Government of Brunei has developed a data protection policy containing elements of data localization, but that policy only relates to state agencies.

36. A draft amendment has been issued by the Indonesian government clarifying the application of art. 17(2), but it remains uncertain whether or when it will take effect: see "Dirjen Aptika: Data Elektronik Strategis Wajib Dikelola di Indonesia" *Kominfo* (12 February 2019), online: Kominfo <https://www.kominfo.go.id/content/detail/16337/dirjen-aptika-data-elektronik-strategis-wajib-dikelola-di-indonesia/0/berita_satker>.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

services used for the process of personal data protection must be located in Indonesia. This adds to the local copy and local action requirements set out in Article 17(2) of the Indonesia OEST Regulation.

E. *Laos*

No existing data localization requirements imposed by Laos were found.

F. *Malaysia*

The Malaysian Personal Data Protection Act 2010 [Malaysia PDPA] is the main data protection legislation in Malaysia.[37] Section 129 of the Malaysia PDPA imposes a qualified restriction on the transfer of personal data out of Malaysia. Section 129 (1) provides that a data user cannot transfer personal data out of Malaysia except to places specified by the Minister of Communications and Multimedia; Section 129(2) requires that these places have laws that are similar to the Malaysia PDPA, or that confer at least an equivalent level of protection to personal data.[38] Section 129(3) then lists the circumstances under which a data user may transfer personal data out of Malaysia notwithstanding Section 129(1), for example, where the data subject has given consent for the transfer.

G. *Myanmar*

No existing data localization requirements imposed by Myanmar were found.

H. *The Philippines*

Data protection in the Philippines is governed by the Data Privacy Act of 2012 (Philippines DPA).[39] Section 21 of the Philippines DPA imposes an obligation of accountability on personal information controllers who transfer personal information to third parties for processing, "whether domestically or internationally"; the personal information controller must use "contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party". This imposes a qualified restriction on the transfer of personal data out of the Philippines.

I. *Singapore*

The Personal Data Protection Act 2012 [Singapore PDPA] governs data protection in Singapore.[40] Section 26 of the Singapore PDPA prohibits organizations from transferring

37. Act 709.
38. Similar requirements are imposed by the Philippines, Singapore, and Thailand; see below.
39. Republic Act No 10173.
40. No 26 of 2012.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

personal data out of Singapore unless certain prescribed conditions are met, to ensure that "organizations provide a standard of protection to personal data so transferred that is comparable" to the protection conferred by the Singapore PDPA. Singapore therefore imposes a qualified restriction on the transfer of personal data out of Singapore.

The conditions are prescribed in subsidiary legislation. Regulation 9(1) of the Personal Data Protection Regulations 2014 sets out the following conditions that must be met by the transferring organization before transferring personal data outside Singapore: the transferring organization must take appropriate steps to (1) ensure that it will comply with the data protection obligations under the Singapore PDPA while it remains in possession or control of the personal data, and (2) ensure that any recipients of the personal data outside Singapore are bound by legally enforceable obligations to protect the personal data to a standard comparable to that under the Singapore PDPA.[41]

J. *Thailand*

On 28 February 2019, Thailand passed its Personal Data Protection Act [Thailand PDPA], making it the most recent ASEAN Member State (at the time of writing) to enact data protection legislation.[42] Section 27 of the Thailand PDPA imposes a qualified restriction on the transfer of personal data out of Thailand, as it prohibits the transfer of personal data to a country that provides a lower level of protection to personal data. This prohibition is subject to certain exceptions (for example, where the transfer is made with the data subject's consent), and the Thai Personal Data Protection Committee may declare that certain countries do not offer a lower level of protection to personal data.

K. *Vietnam*

Decree No 72/2013/ND-CP of July 15, 2013, on the management, provision, and use of Internet services and online information [Vietnam Decree 72] took effect on 1 September 2013. Vietnam Decree 72 requires certain categories of entities to have "at least one server system in Vietnam serving the inspection, storage, and provision of information at the request of competent state management agencies, and settlement of customers' complaints about the service provision", namely: organizations and enterprises that establish aggregated information websites;[43] organizations and enterprises that establish social networks;[44] providers of information content services on mobile telecommunications networks;[45] and online game service providers.[46] This in effect imposes both local copy and local action requirements on the specified entities.

41. s. 362/2014.
42. The analysis that follows is based on a draft version of the legislation: "Personal Data Protection Act" *ETDA ICT Law Center*, online: <https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act>.
43. *Ibid.*, art. 24.2.
44. *Ibid.*, art. 25.8.
45. *Ibid.*, art. 28.2.
46. *Ibid.*, art. 34.2.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

Table 1. Comparative table of data localization requirements in ASEAN Member States.

Country	Local processing	Transfer limitation
Brunei		
Cambodia		
Indonesia	Local copy and action (Indonesia OEST Regulation). Local copy and action (Indonesia PPDES Regulation).	Qualified restriction (Indonesia PPDES Regulation).
Laos		
Malaysia		Qualified restriction (Malaysia PDPA).
Myanmar		
Philippines		Qualified restriction (Philippines DPA).
Singapore		Qualified restriction (Singapore PDPA).
Thailand		Qualified restriction (Thailand PDPA).
Vietnam	Local copy (Vietnam Law on Cybersecurity). Local copy and action (Vietnam Decree 72).	

Subsequently, Vietnam enacted its Law on Cybersecurity No 24/2018/QH14 [Vietnam Law on Cybersecurity], which took effect on 1 January 2019.[47] The Vietnam Law on Cybersecurity is aimed at "protecting national security and securing social order and safety on cyberspace".[48] "Cyberspace" is broadly defined in Article 2.3, as meaning "the network of information technology infrastructure, including telecommunication networks, the Internet, computer networks, information processing and control systems, and databases, where humans perform social behaviours without being limited by space and time". In relation to data localization, Article 26.3 imposes a local copy requirement on cyberspace service providers who process personal or user data:

> Local and foreign enterprises that provide services on telecommunication networks and the internet, and value added services on cyberspace in Vietnam and are involved in gathering, exploiting, analysing or processing data on personal information or service users' relations or data created by the service users in Vietnam, shall store such data in Vietnam for such period as is specified by the Government.

L. *Comparative Table*

The data localization requirements of the ten ASEAN Member States are summarized in Table 1. Generally speaking, there is presently a moderate level of data localization among the ASEAN Member States. There is convergence in terms of restrictions on cross-border transfer of personal data, as several ASEAN Member States have

47. The analysis that follows is based on a draft version of the legislation. "Vietnam Law on Cybersecurity", online: <https://auschamvn.org/wp-content/uploads/2018/06/Draft-Cyber-Security-Law-Version-20-ENG.docx>.

48. *Ibid.*, art. 1.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

imposed data protection adequacy requirements (that a data controller transferring data out of the country ensure that the personal data receives a comparable level of protection in the recipient country). Local processing requirements remain the exception rather than the norm. However, the local processing requirements that have thus far been implemented appear broadly drafted, potentially catching a wide range of data controllers and types of data.

IV. THE EU APPROACH TO DATA LOCALIZATION

This paper will now examine how EU law applies to data localization. There is an increasing recognition, by EU institutions, that the internal market rules of the EU proscribe the imposition of unjustified and disproportionate data localization requirements by EU Member States. Significant recent developments have occurred in the EU in this respect. It will be useful to observe how EU law addresses the issue of data localization, as it may reveal lessons relevant to the ASEAN context.

A. *Data Localization as Infringement of Freedoms of Movement*

The establishment of a single European internal market is one of the core objectives of the EU project: Article 3(3) of the Treaty on European Union [TEU] provides that the EU "shall establish an internal market".[49] The creation of an internal market requires market integration among the various EU Member States, and market integration requires the elimination of trade barriers. Thus Article 26 of the Treaty on the Functioning of the European Union [TFEU] provides that the EU "shall adopt measures with the aim of establishing or ensuring the function of the internal market", and that the internal market comprises "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured".[50]

The TFEU contains specific provisions on freedoms of movement, of which two freedoms are particularly relevant in the context of data localization, namely: (1) the freedom of establishment in the territory of another EU Member State, and (2) the freedom to provide services to a person in another EU Member State. Article 49 of the TFEU provides for the freedom of establishment, prohibiting restrictions on the freedom of a person of one EU Member State to establish itself in the territory of another EU Member State. The freedom of establishment permits a person to "participate, on a stable and continuous basis, in the economic life of a member state" other than its state of origin.[51] Article 56 of the TFEU provides for the freedom to provide services. This prohibits restrictions on the freedom to provide services to persons in EU Member States other than the EU Member State in which the service

49. Consolidated Version of the Treaty on European Union, 26 October 2012, OJ C326/13.
50. Consolidated Version of the Treaty on the Functioning of the European Union, 26 October 2012, OJ C326/47.
51. Case C-55/94 *Gebhard v. Consiglio dell"Ordine degli Avvocati* [1995] ECR I-4165; [1996] 1 CMLR 603 at [25].

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

provider is established. "Service" is given a broad definition in Article 57 of the TFEU as economic activities normally provided for remuneration and not governed by the freedoms of movement for goods, capital, and persons. The freedom to provide services is supplemented by provisions in secondary legislation such as the Services Directive and Electronic Commerce Directive.[52]

The freedoms of movement are not absolute, and Member States can legitimately impose effective restrictions on those freedoms. However, such restrictions must comply with fairly stringent criteria. The Court of Justice of the European Union [CJEU] has held in *Gebhard* that:[53]

> [N]ational measures liable to hinder or make less attractive the exercise of fundamental freedoms guaranteed by the Treaty must fulfil four conditions: they must be applied in a non-discriminatory manner; they must be justified by imperative requirements in the general interest; they must be suitable for securing the attainment of the objective which they pursue; and they must not go beyond what is necessary in order to attain it.

Data localization requirements potentially implicate both the freedom of establishment and the freedom to provide services. Data localization requirements can impede the freedom of establishment, in particular where a Member State prevents an entity established in its territory from transferring data out of its territory, thus deterring that entity from shifting its operations and establishing itself in the territory of another Member State. The potential for data localization to restrict the freedom to provide services has been explained in Part II of this paper.

The European Commission has recognized that data localization requirements have the potential to restrain freedoms of movement, and has proposed a new "principle of free movement of data" in response. In its Data Economy Communication, the European Commission expressed a clear view that "unjustified data location restrictions impair the freedom to provide services and the freedom of establishment",[54] and stated that:[55]

> [A]ny member state action affecting data storage or processing should be guided by a "principle of free movement of data within the EU", as a corollary of their obligations under the free movement of services and the free establishment provisions of the Treaty and relevant secondary legislation.

The view of the European Commission on the inconsistency of data localization requirements with the freedoms of movement has significant import, in the light of the European Commission's power under Article 258 of the TFEU to enforce EU Member States' Treaty obligations. Indeed, the European Commission has warned

52. Directive 2006/123/EC of 12 December 2006 on services in the internal market [2006] OJ L376/36; Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

53. *Gebhard*, *supra* note 51 at [37]. See also Case C-76/90 *Säger v. Dennemeyer & Co Ltd* [1991] ECR I-4221 at [15].

54. Commission, "Building a European Data Economy" (Communication) COM (2017) 9 final (Data Economy Communication) at 3.

55. *Ibid.*, at 7.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

that it will "launch infringement proceedings to address unjustified or disproportionate data location measures" if necessary.[56]

The European Commission has recognized, however, that there are certain exceptional contexts in which data localization measures may be justified and proportionate, "especially before effective cross-border cooperation arrangements are put in place"; examples of such exceptional contexts include the securing of data relating to critical energy infrastructure, ensuring the availability of electronic evidence for law enforcement authorities, and the local storage of data in public registers.[57] It should be pointed out here that any data localization requirement imposed must fulfil the criteria set out in *Gebhard*—this significantly limits the range of acceptable data localization requirements.[58]

B. *Specific Norms Against Data Localization Within the EU*

Apart from the Treaty rules, there exist specific secondary EU legislation that collectively govern the processing of data within the EU. At present, the EU data governance regime may be conceptualized as a bifurcated one, establishing separate regulatory regimes for personal data and non-personal data. Both regimes generally proscribe the imposition of data localization requirements by EU Member States.

Where personal data is concerned, the main relevant secondary legislation is the General Data Protection Regulation [GDPR].[59] The GDPR, adopted pursuant to Article 8 of the EU Charter of Fundamental Rights and Article 16 of the TFEU, sets out the rules pertaining to data protection and the free movement of personal data. The GDPR supersedes the older Data Protection Directive [DPD] which, unlike the GDPR, was not directly binding on EU Member States, thereby resulting in fragmentation and divergences in data protection across the EU Member States. The GDPR has since harmonized data protection rules across all EU Member States, ensuring equivalent levels of data protection across the EU, thereby obviating any need for barriers to the free flow of personal data among EU Member States. Accordingly, EU Member States should not restrict the free flow of personal data within the EU; this is expressly stipulated in Article 1(3) of the GDPR, which provides that the free movement of personal data within the EU "shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".[60]

56. *Ibid.*, at 8.

57. *Ibid.*, at 6.

58. See *ibid.*, at 7, where the European Commission notes that data localization requirements must be "carefully justified under the Treaty and relevant secondary law to verify that they are necessary and proportionate to achieve an overriding objective of general interest".

59. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

60. *Ibid.*, art. 1(3). This does not, however, preclude restrictions on the free flow of personal data for other reasons; neither does it cover non-personal data. See also art. 1(2) of the proposed ePrivacy Regulation (Commission, Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

In respect of non-personal data, the EU adopted Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union [NPDR] on 14 November 2018. The aim of the NPDR is to ensure the free flow of non-personal data within the EU.[61] It expressly prohibits data localization requirements, unless justified on grounds of public security. "Data localization requirement" is given a broad definition in Article 3(5) of the NPDR, as:

> [A]ny obligation, prohibition, condition, limit or other requirement provided for in the law, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law … which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State.

In order to address the concern that authorities of an EU Member State may be unable to access data processed in another EU Member State, the NPDR also provides for the right of authorities to obtain access to data for the performance of their official duties. The NPDR establishes a co-operation mechanism for data access, empowering an authority of one EU Member State to request assistance for data access from authorities of other EU Member States.[62] Authorities from whom assistance has been requested are obliged to respond to the request.[63] EU Member States are also permitted to impose sanctions for failures to comply with obligations to provide data and, in exceptional circumstances, impose "strictly proportionate interim" re-localization measures.[64]

C. *Data Localization vis-à-vis Third Countries*

It should be noted that the EU internal market rules and secondary legislation described above only prohibit restrictions on the free movement of data *within the EU*. They do not prohibit the restriction of data flows to third countries outside the EU.

Indeed, EU rules positively restrict the movement of personal data to third countries. Transfers of personal data to third countries or international organizations are subject to strict conditions under the GDPR, in order to prevent the level of data protection provided by the GDPR from being undermined.[65] In essence, personal data can only be transferred out of the EU (1) pursuant to an Article 45 adequacy decision by the European Commission determining that the recipient country ensures an adequate level of data protection, (2) pursuant to certain appropriate safeguards specified in Article 46, or (3) in specific situations listed in Article 49.[66]

(Regulation on Privacy and Electronic Communications) COM (2017) 10 final), which uses similar language.

61. Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L305/59, art. 1.
62. *Ibid.*, art. 5.
63. *Ibid.*, art. 7(4).
64. *Ibid.*, art. 4.
65. General Data Protection Regulation, recital 101.
66. This restriction has been subject to some academic criticism suggesting that the EU's restrictions on the transfer of personal data out of the EU do not effectively achieve the aim of personal data

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

The right to data protection is a fundamental right under Article 8 of the EU Charter of Fundamental Rights, and the rules governing the transfer of personal data outside the EU are an implementation of that fundamental right. As such, they cannot be traded off. In one of its Communications, the European Commission made it clear that "the EU data protection rules cannot be the subject of negotiations in a free trade agreement", and that dialogues on data protection and trade negotiations would have to follow separate tracks.[67] This suggests that the EU will be unlikely to offer adequacy decisions as an incentive in trade negotiations with third countries.

In sum, EU Member States are free to localize data within Europe (and are obliged to do so for personal data), but are prohibited from localizing data among themselves. "Data Eurocalization" is consistent with the EU's internal market objective, although whether a similar approach is appropriate in the ASEAN context is questionable; this will be considered below in the next part of this paper.

V. AN ASEAN APPROACH TO DATA LOCALIZATION

Unlike the EU, ASEAN has not expressed any explicit norm for or against data localization. This leaves open the question as to what approach ASEAN should take on data localization. In this regard, there are potentially useful lessons that may be drawn from the experience of the EU, as both ASEAN and the EU are supranational institutions that seek to achieve economic integration among their respective Member States, aiming to establish regional single markets (albeit with different features).

This paper proceeds to assess data localization in the context of existing ASEAN norms, and to suggest relevant lessons that may be drawn from the EU. Differences between ASEAN and the EU, and their implications on the applicability of the EU experience to the ASEAN context, will also be explained.

A. *Data Localization and ASEAN Economic Integration*

The Charter of the Association of Southeast Asian Nations [ASEAN Charter] serves as the constituent instrument of ASEAN.[68] On economic integration, Article 1(5) declares that one of the purposes of ASEAN is to create a "single market and production base" in which there is, among other things, "free flow of goods, services and investment". Article 2(n) further provides that ASEAN Member States shall act in accordance with the principle of "adherence to multilateral trade rules and ASEAN's rules-based regimes for effective implementation of economic commitments

protection. See for example, W. Kuan HON, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens* (Cheltenham, Edward Elgar, 2017), at 318.

67. European Communication, "Exchanging and Protecting Personal Data in a Globalised World" (Communication) COM (2017) 7 final at 9.

68. *Charter of the Association of Southeast Asian Nations*, 20 November 2007.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

and progressive reduction towards elimination of all barriers to regional economic integration, in a market-driven economy". Thus, like the EU, ASEAN has expressed a firm commitment to economic integration and the establishment of a regional economic community.

To achieve the goal of an ASEAN economic community, ASEAN adopted the ASEAN Economic Community Blueprint 2015 [AEC Blueprint 2015], which has since been superseded by the ASEAN Economic Community Blueprint 2025 [AEC Blueprint 2025].[69] These instruments set out concrete steps to be implemented by ASEAN Member States for economic integration. For the promotion of the free flow of services within ASEAN, the AEC Blueprint 2015 states that ASEAN Member States should remove "substantially all restrictions on trade in services" by 2015 and, in particular, progressively commit to having no restrictions for Mode 1 and Mode 2 trade in services.[70] The AEC Blueprint 2025 contemplates the further advancement of services integration through the future implementation of an ASEAN Trade in Services Agreement [ATISA].[71]

In relation to trade in services, ASEAN has also established norms under the ASEAN Framework Agreement on Services [AFAS]. The AFAS is aimed at enhancing co-operation in services and reducing restrictions to trade in services, contemplating the liberalization of trade in services beyond ASEAN Member States' existing GATS commitments.[72] Article 3 requires ASEAN Member States to "liberalise trade in services in a substantial number of sectors within a reasonable time frame" by eliminating discriminatory measures and market access limitations. As of 2018, ten "packages" of commitments to liberalize trade in services have been implemented by the ASEAN Member States under the AFAS.

Data localization requirements are, arguably, inconsistent with the existing ASEAN economic framework. They detract from the goal of regional economic integration expressed in the ASEAN Charter. In particular, as mentioned in Part II, data localization requirements may inhibit services integration by limiting market access by foreign service suppliers, thereby running counter to the drive to liberalize trade in services under the AFAS and the AEC Blueprints. However, unlike the EU, ASEAN does not yet appear to have expressly recognized the connection between cross-border data flow and services integration, nor has it explicitly identified data localization as a potential inhibitor of trade in services.

B. *Existing ASEAN Norms on Data Localization*

In recent years, ASEAN has begun to pay more attention to data governance and cross-border data flow. While it has not yet adopted a holistic approach to data

69. This goal was formalized in the Declaration of ASEAN Concord II: see *Declaration of ASEAN Concord II (Bali Concord II)*, 11 May 2012.

70. *ASEAN Economic Community Blueprint*, 20 November 2007 at 10.

71. *ASEAN Economic Community Blueprint 2025*, 22 November 2015 at 6. Negotiations on ATISA were concluded at the 33rd ASEAN Summit on 13 November 2018.

72. *ASEAN Framework Agreement on Services*, 15 December 1995, art. 1.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

localization, some norms pertaining to aspects of data localization have emerged. The following paragraphs highlight these norms, in chronological order of adoption by ASEAN.

At the 16th ASEAN Telecommunications and Information Technology Ministers [TELMIN] Meeting, the ASEAN Framework on Personal Data Protection [ASEAN PDP Framework] was adopted.[73] The ASEAN PDP Framework is a framework instrument setting out principles of personal data protection which the ASEAN Member States intend to implement in their domestic laws. The principles espoused in the ASEAN PDP Framework are familiar, similar to established international norms such as those set out in the APEC Privacy Framework and OECD Privacy Framework. In relation to data localization, paragraph 6(f) of the ASEAN PDP Framework provides for a principle of transfer limitation:

> Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles.

Subsequently, the ASEAN Framework on Digital Data Governance [ASEAN DDG Framework] was endorsed.[74] The ASEAN DDG Framework is "aimed at strengthening the data ecosystem, achieving legal and regulatory alignment of data regulations and governance frameworks, and fostering data-driven innovation across ASEAN member states to boost the growth of the digital economy in the region".[75] The ASEAN DDG Framework identifies cross-border data flow as a strategic priority of data governance, and establishes a principle on cross-border data flow which is "intended to maximize the free flow of data within ASEAN to foster a vibrant data ecosystem but at the same time ensure that the data transferred is accorded the necessary protection".[76] Measures pursuant to the principle on cross-border data flow

73. Association of Southeast Asian Nations (ASEAN), "The 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings: Joint Media Statement" (2016), at para. 4; Association of Southeast Asian Nations (ASEAN), "ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN): Framework on Personal Data Protection" (2016). The development of an ASEAN framework on personal data protection was one of the stated initiatives of the ASEAN ICT Masterplan 2020, which was adopted at the previous TELMIN Meeting with a view to advancing the digital economy in the ASEAN region: see Association of Southeast Asian Nations (ASEAN), "The ASEAN ICT Masterplan 2020" (ASEAN Secretariat 2015), at 26.

74. Association of Southeast Asian Nations (ASEAN), "ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN): Framework on Digital Data Governance" (2018). The development of an ASEAN digital data governance framework was a key initiative of the Master Plan on ASEAN Connectivity 2025, which was adopted with the view to promoting physical, institutional, and people-to-people connectivity within the ASEAN region: see Association of Southeast Asian Nations (ASEAN), "Master Plan on ASEAN Connectivity 2025" (ASEAN Secretariat 2016), at 54.

75. Association of Southeast Asian Nations (ASEAN), "The 18th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings: Joint Media Statement" (2018), at para. 4.

76. Association of Southeast Asian Nations (ASEAN), "ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN): Framework on Digital Data Governance" (2018), at para. 20.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

include (1) developing clear and unambiguous rules on the transfer of data from one ASEAN Member State to another, (2) ensuring that requirements imposed on cross-border data transfers are proportionate to the risks associated with the transfers, and (3) building trust by providing adequate protection to transferred data.[77]

Finally, on 22 January 2019, ASEAN adopted its Agreement on Electronic Commerce [ASEAN E-Commerce Agreement]. This agreement contains ASEAN's most direct attempt to address the issue of data localization. Article 7(4) is an endeavours clause which provides that ASEAN Member States agree to work towards "eliminating or minimizing barriers to the flow of information across borders" subject to "appropriate safeguards to ensure security and confidentiality of information" and other legitimate public policy objectives.[78] Article 7(6) prohibits ASEAN Member States from insisting on the location of computing facilities within their own territories as a precondition for doing business in their territories. The provisions of Article 7 are subject to Article 14, which incorporates the exemptions under Articles XIV and XIVbis of the GATS.

Distilling the basic features of the existing ASEAN norms on data localization, the following points may be made. First, like the EU, ASEAN has embraced the free flow of data within the region, the minimization of both transfer limitation requirements and local processing requirements, and the need for clear rules in relation to the transfer of data across borders. Second, ASEAN recognizes that the free flow of data should be subject to legitimate countervailing policy objectives, including those enumerated in Articles XIV and XIVbis of the GATS. Third, one established countervailing policy objective is the protection of personal data and individual privacy, which underpins the differentiated treatment of personal and non-personal data—it is legitimate to subject the cross-border transfer of personal data to limits in order to ensure that the personal data receives adequate protection in the recipient country. In these respects, ASEAN is not dissimilar to the EU.

C. *Recommendations for ASEAN's Approach to Data Localization*

What more can ASEAN do to regulate the use of data localization requirements by its Member States? Here, three suggestions may be drawn from the EU's approach to data localization. First, there is an argument to be made for explicit recognition that data localization requirements constitute barriers to trade in services, just as the European Commission has done in its Data Economy Communication. This will encourage ASEAN Member States to abide by their existing services liberalization commitments, by removing or moderating such data localization requirements that are inconsistent with those commitments, and by avoiding the enactment of further data localization requirements. Such a recognition would supplement the endeavours undertaking under Article 7(4) of the ASEAN E-Commerce Agreement.

Second, there is a need for clarity on what constitute legitimate public policy objectives that justify derogations from the free flow of data. While the position is tolerably

77. *Ibid.*

78. Notably, art. 7(4)(c) expressly excludes financial services.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

clear in relation to personal data—cross-border transfers of personal data are subject to adequacy restrictions on the basis of the need to protect individual privacy—the same cannot be said for non-personal data. The ASEAN E-Commerce Agreement is vague in this regard, and while Articles XIV and XIVbis of the GATS have been incorporated into the ASEAN E-Commerce Agreement, these too provide limited guidance. Policy objectives that relate specifically to data localization should be identified—the European Commission's Data Economy Communication provides an example of this.[79]

Third, strict standards should be set on the justification of data localization requirements. The ASEAN E-Commerce Agreement seems to set a fairly low standard for restrictions on the cross-border transfer of data, permitting the imposition of such restrictions as and when "legitimate public policy objectives so dictate".[80] It is suggested that any data localization requirements imposed should be targeted so as not to excessively inhibit trade in services, and that viable less-restrictive alternatives to data localization should be adopted where available. Reference may be made here to the *Gebhard* criteria set out by the CJEU.[81] These criteria would essentially require that data localization requirements not only be justified by a public interest, but also be non-discriminatory, effective, and no more restrictive than necessary.

The three suggestions mentioned above could go some way towards advancing ASEAN's approach to the issue of data localization. Through the use of its instruments, ASEAN can promote further convergence among its Member States, while striking an appropriate balance between the desirability of promoting the free flow of data in the region and the legitimate need for ASEAN Member States to restrain that flow in view of public policy concerns.[82]

While useful lessons may be drawn from the EU, two key differences between ASEAN and the EU should also be noted—these differences materially limit the utility of the EU experience to ASEAN. First, commenters have observed that, given the relatively small economic size of the ASEAN region (as compared to that of the EU), there is a need for ASEAN to practice "open regionalism", which entails joining global economic networks and participating in the global supply chain.[83] In other words, it is necessary for ASEAN to achieve not only regional integration, but also integration with the broader global economy. The implication here is that the EU approach to data localization (that is, free movement of data within Europe, but not out of Europe) may have limited applicability to the ASEAN context.

Second, ASEAN and the EU operate on substantially different models of regional integration.[84] While the EU has embraced the use of legal institutions and of instruments

79. Data Economy Communication, *supra* note 54 at 6.

80. *ASEAN Agreement on Electronic Commerce*, 22 January 2019, art. 7(4)(b).

81. Gebhard, *supra* note 51.

82. For an excellent compendium that seeks to facilitate convergence on the regulation of cross-border transfers of personal data across the broader Asia-Pacific region, see Clarisse GIROT, ed., *Regulation of Cross-Border Transfers of Personal Data in Asia* (Singapore, Asian Business Law Institute, 2018).

83. Siow Yue CHIA and Michael G. PLUMMER, *ASEAN Economic Cooperation and Integration: Progress, Challenges and Future Directions* (Cambridge, Cambridge University Press 2015) at 155.

84. See Laurence HENRY, "The ASEAN Way and Community Integration: Two Different Models of Regionalism" (2007) 13 European Law Journal 857.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

binding on its Member States, the ASEAN legal regime is best characterized as a "soft law regime", regulating the conduct of its Member States via "soft mechanisms" rather than "hard legislation".[85] ASEAN has eschewed the use of legally enforceable agreements in its pursuit of economic integration and there is, for the most part, a "noticeable absence of a judicial role in freeing interstate trade and commerce".[86]

ASEAN's preference for soft regulation means that some of the solutions that the EU has developed to minimize the use of data localization requirements may not be available to ASEAN. For example, in the EU there is a fully harmonized data protection regime that is directly and legally binding on all EU Member States, negating the need for any barriers to the transfer of personal data between EU Member States. In contrast, no equivalent harmonized data protection regime exists in ASEAN—the ASEAN PDP Framework is not binding on ASEAN Member States in the way that the GDPR is binding on EU Member States—and it is unlikely that coercive legislation like the GDPR will find acceptance in ASEAN.[87] Since there is no common data protection regulation in ASEAN, and there remains a lack of harmonization in terms of data protection standards among the ASEAN Member States, it is not feasible for the ASEAN Member States to permit the absolute free movement of personal data among themselves, and some restrictions on the transfer of personal data between ASEAN Member States are inevitable.

Another example of an EU solution that may not be viable in the ASEAN context would be the EU's implementation of a co-operation mechanism for data access for state authorities via Articles 5 and 7 of the NPDR.[88] This data access regime addresses the need of state agencies to access data held by data controllers, thereby removing the need for EU Member States to localize data to ensure that their state agencies have access to that data. While it is plausible that a similar co-operation mechanism could be implemented in ASEAN, the effectiveness of such a co-operation mechanism is contingent upon the imposition of legally binding obligations on Member States, which does not presently appear feasible in the ASEAN context.

VI. CONCLUSION

This paper has sought to describe the practice of data localization among the ASEAN Member States, and to explain how ASEAN presently regulates that practice. While

85. Imelda DEINLA, *The Development of the Rule of Law in ASEAN: The State and Regional Integration* (Cambridge, Cambridge University Press 2017) at 130. On the nature of "soft law", see Kenneth W. ABBOTT and Duncan SNIDAL, "Hard and Soft Law in International Governance" (2000) 54 International Organization 421 at 422. ("The realm of soft law begins once legal arrangements are weakened along on or more of the dimensions of obligation, precision, and [adjudicatory] delegation.")

86. Deinla, *supra* note 85 at 162; but cf. Henry, *supra* note 84 at 864–5.

87. See ASEAN PDP Framework, *supra* note 73. Note para. 7, which provides that ASEAN Member States may delay the application of the framework until they are ready to implement it, in view of the varying levels of development among the ASEAN Member States. Note also para. 13, which provides for the amicable settlement of disputes "through consultation or negotiations, without any reference to any third party or international tribunal".

88. See text to ftn. 61–4.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press

positive steps have been taken by ASEAN toward a principled and rules-based approach, there will be a growing need for ASEAN to take a clearer stand as the prevalence of data localization increases in Asia and around the world; this paper has suggested a number of moves that ASEAN may make to address that need.

https://doi.org/10.1017/S2044251319000250 Published online by Cambridge University Press