Asian Journal of Law and Society (2026), 1–25
doi:10.1017/als.2026.10057

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Between Digital Trade Commitments and Sovereignty: Asian Developing Members' Approaches to the CPTPP's Cross-Border Data Transfers

Duc Anh Nguyen[1,2]

[1]University of Law, Vietnam National University, Hanoi, Vietnam and [2]ANU Law School, Australian National University, Australia
Email: ndanh@vnu.edu.vn

Abstract

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) set an advanced benchmark for digital trade rules by mandating cross-border data transfers and prohibiting data localisation requirements. This article examines how three Asian developing members, Vietnam, Malaysia, and Brunei Darussalam, have implemented these stringent obligations. It shows that the binding CPTPP data-related provisions have driven domestic data law reforms across all three jurisdictions. Although ensuring compliance with the CPTPP's commitments, all domestic data legal regimes retain varying degrees of restrictiveness by preserving their national regulatory autonomy. I argue that while such domestic data measures do not fundamentally breach the CPTPP, they run counter to its liberal spirit of facilitating cross-border data flows and impede digital trade liberalisation in the long term.

Keywords: digital trade; cross-border data transfers; data localisation; CPTPP; developing countries

1. Introduction

In recent years, digital transformation has reshaped global trade law (Burri, 2023a, p. 387). The impacts of digitalisation on global trade make data a central issue in modern international trade law (Burri, 2023b, p. 558). Data is politically sensitive and technically challenging; therefore, it is difficult to regulate (Wolfe, 2019, p. 63). Various data-related issues, such as the free flow of data, data localisation measures, and privacy protection, have emerged as critical and contentious subjects at the World Trade Organization (WTO) and in modern preferential trade agreements (PTAs) (Burri, 2023b, p. 558). Over the last few decades, the WTO has made slow progress in adapting to the new issues in digital trade (Mitchell and Mishra, 2021, p. 85). Its existing rules are relevant albeit inadequate for regulating cross-border data flows and other data-related issues in the digital economy today (Mitchell and Mishra, 2020, p. 1091). By contrast, PTAs compensate for the lack of progress of the WTO and address new issues from the data-driven economy (Burri, 2021, p. 40). Since the early 2000s, global trade law has witnessed a proliferation of deeper and more comprehensive digital trade provisions across PTAs (Elsig and Klotz, 2021, p. 42). As a result, PTAs are an important platform for rule-making in this area, where data-related provisions can be found in dedicated provisions in PTAs (Burri, 2023c, p. 264).

© The Author(s), 2026. Published by Cambridge University Press in association with Shanghai Jiao Tong University. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Among PTAs, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is highly acclaimed as a leading model for digital trade rule-making since its advent (Ni, 2024, p. 1005). Compared with WTO rules, the CPTPP represents a significant advance beyond the General Agreement on Trade in Services (GATS) by facilitating cross-border data flows while preserving governments' right to regulate in the public interest (Hodson, 2019, p. 579). Its success is shown in the diffusion of its digital trade norms across subsequent PTAs[1] (Burri, 2025, p. 153) and domestic regulatory frameworks, particularly in the Americas and the Asia-Pacific region (Gao, 2024, p. 352). However, the CPTPP's potential as a blueprint for a global digital trade framework remains questioned due to limitations in practice, especially insufficient inclusiveness for developing countries (Kelsey, 2018, p. 274). As a result, it is argued that the CPTPP's digital trade governance template is not yet fully suitable as a universal multilateral framework under the WTO (Ni, 2024, p. 1005).

Although digital trade can contribute to developing countries by enhancing connectivity and economic inclusiveness (World Trade Organization, 2023, p. 21), many of them face barriers to fully engaging in the digital economy (Agarwal and Mishra, 2023, p. 297). While the global digital economy is dominated by developed economies (Murthy et al., 2021, p. 1), developing countries face insufficient digital infrastructure, a lack of skilled workforce and limited regulatory capacity to gain economic value from data produced within their border (Mishra, 2024, p. 125). Developing countries become sources of raw data, while big tech companies based in developed countries gain greater benefits from collecting, processing, storing, and exploiting these data flows (Mishra, 2024, p. 129). This implies that data policies are directly linked to inequality if mandating unrestricted free flows of data risks positioning developing members into mere exporters of unprocessed data (Vásquez Callo-Müller and Kugler, 2023, p. 120). Therefore, in the data-driven economy, developing countries lack a comparative advantage.

These asymmetries also extend to digital trade rule-making. There are three dominant data governance models (Burri, 2023d, p. 94), including the United States' market-driven approach, the European Union's rights-based framework, and China's state-centric model (Gao, 2023b, p. 713). They act as rule-makers by incorporating their data regulatory preferences into trade and digital economy agreements, while developing countries, as rule-takers, have limited room to shape their own regulatory frameworks both nationally and internationally (Burri, 2023e, p. 95). These competing data governance models primarily reflect the different national interests and policy priorities (Gao, 2023a, p. 218), thereby triggering inequalities in the digital trade regulatory framework (Burri, 2024, p. 205). Developing countries, with less institutional and regulatory capacity, are required to align with stringent commitments on cross-border data transfer when joining such agreements (Aaronson and Leblond, 2018, p. 271).

Against this background, CPTPP aims to promote cross-border data flow, seeking to limit data protectionism (Burri, 2023f, p. 14). In this context, how do developing members reconcile their domestic data measures with the CPTPP's obligations on the free flow of data? The article uses doctrinal legal methods to analyse the domestic legal frameworks of three developing countries in Asia—Vietnam, Malaysia, and Brunei Darussalam—and examines how they fulfil obligations on cross-border data transfers while retaining regulatory autonomy through national security, public policy, and privacy protection. The article refers to the data restrictiveness typology developed by the Organization for Economic Co-operation and Development (OECD) and argues that although these state

[1] Chile–Uruguay FTA (2016), Singapore–Australia FTA (2016), the Argentina–Chile FTA (2017), the Singapore–Sri Lanka FTA (2018), the Australia–Peru FTA (2018), the Brazil–Chile FTA (2019), and the Australia–Indonesia FTA (2019), the US–Mexico–Canada Agreement (USMCA, 2018), the Japan–US Digital Trade Agreement (2019), and others Digital Economy Agreements (DEAs).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

practices achieve CPTPP's compliance, all three jurisdictions maintain a certain level of restrictiveness over cross-border data flows. Such restrictive tendencies are not fully in line with CPTPP's objectives of facilitating the free flow of data, and may hinder digital trade liberalisation in the long term.

2. CPTPP: an advanced model of digital trade governance

The CPTPP was signed in 2018 by 11 nations, known as the first comprehensive template establishing hard and enforceable rules on cross-border data flow and data localisation.[2] This approach reflects the data governance model of the United States, emphasising the preferences and interests of big technology companies (Kelsey, 2018, p. 273). Its digital trade rules are largely retained from the original Trans-Pacific Partnership (TPP) despite the United States' withdrawal (Brzytwa et al., 2021, p. 452). This section examines the CPTPP's far-reaching data-related provisions (Collins, 2025, p. 263), shown through three elements: cross-border data transfer (Article 14.11 CPTPP), data localisation requirements (Article 14.13 CPTPP), and its specific exception provisions.

2.1. Cross-border data transfers

Article 14.11 CPTPP is one of the core provisions promoting cross-border data transfers. It imposes a positive obligation on parties to "*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.*" Although the CPTPP does not specify what kind of data is covered, the reference to "*including personal information*" implies that the scope of the article covers all forms of data. Compared to the Regional Comprehensive Economic Partnership (RCEP), the coverage of the cross-border data transfer rules in the CPTPP is broader, whereas RCEP only mentions "*information*."[3] In addition, Article 14.11 is binding and enforceable, "*shall allow*" meaning that CPTPP's signatories are bound to align their domestic legal framework with the obligation to allow cross-border data transfer. Importantly, this obligation is enforceable through the CPTPP dispute settlement mechanism if a party adopt inconsistent measures, once the transitional phase expires.[4] The hard-law nature of cross-border data provisions reflects the major shift in both regulatory philosophy and approach in the new era of US FTAs (Gao, 2017, p. 361; Gao, 2018a, p. 68).[5] In contrast, the RCEP imposes a negative obligation whereby parties "*shall not prevent cross-border transfer of information*,"[6] meaning that RCEP prohibits states from creating barriers but does not require them to actively facilitate such data transfer, like "*shall allow the cross-border data transfer*" in CPTPP.[7] Moreover, regarding disputes over cross-border data transfer regulations, RCEP parties are required to consult in good faith, but there are no legal consequences if consultations fail, and no party can initiate a formal and binding dispute settlement mechanism under the CPTPP mechanism.[8] The RCEP's approach to cross-border data transfer is more cautious and flexible, especially for developing countries (Zhai, 2025, p. 45).

[2] There are several FTAs including cross-border data flow provisions before the CPTPP, such as the Dominican Republic–Central America FTA (CAFTA-DR) 2024, Article 14.5(c), and the United States–Korea Free Trade Agreement (KORUS FTA) 2007, Article 15.8. However, these articles remain in soft-law language.

[3] Article 12.15 RCEP.

[4] Article 14.18 CPTPP.

[5] Although the first US FTA regulating cross-border data transfers is the United States–Korea Free Trade Agreement (KORUS FTA), signed in 2007, it is soft law.

[6] Article 12.15(2) RCEP.

[7] Article 14.11(2) CPTPP.

[8] Article 12.17 RCEP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

2.2. Data localisation requirements

While Article 14.11 governs the movement of data, Article 14.13 addresses the physical location where data is processed and stored, also known as data localisation. This is a measure which requires data to be stored within a specific jurisdiction and restricts the transfer of data across borders (OECD, 2023, p. 5). Data localisation measures are not a new phenomenon, and are increasingly adopted as they are subject to countries' jurisdiction (Chander and Lê, 2015, p. 708). Supporter of data localisation justify it to protect their citizens' privacy, maintain national security, and pursue other public policy objectives (Han, 2024, p. 263). By contrast, it is also viewed as a form of trade barrier (Selby, 2017, p. 215). The United States is a notable country consistently opposing data localisation requirements measures (Gao, 2018b, p. 306). Under CPTPP, Article 14.13(2) prohibits party members from imposing data localisation requirements, providing *that* "*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*."[9] While the level of restrictiveness varies across agreements, most data localisation provisions in contemporary PTAs are binding in nature (Burri, 2023c, p. 270). By stipulating "*No parties shall require . . .*," CPTPP establishes an explicit ban on data localisation, meaning that countries are not allowed to adopt data localisation measures as a condition for entering a country's market to conduct business. Compared to the GATS disciplines, Article 14.13 goes beyond that as it prohibits a wider range of localisation measures, including those that might not otherwise violate national treatment or market access obligations (Hodson, 2019, p. 606). Therefore, the CPTPP's approach to data localisation reflects the United States' broader objective of seeking to curb data protectionism (Selby, 2017, p. 218).

2.3. Specific exception provisions

Data localisation and cross-border data flows are interrelated (Potluri et al., 2020, p. 3). As such, the coverage of both Articles 14.11 and 14.13 in CPTPP may overlap, and both are therefore subject to certain exception mechanisms. In particular, both articles recognise a party's regulatory autonomy (Burri and Kugler, 2024, p. 407), which allows them to maintain "*its own regulatory requirements' on cross-border transfers of information* and *the use of computing facilities*."[10] The CPTPP preserves the members' right to regulate when allowing them to maintain domestic measures to restrict data flows and adopt data localisation, provided that such measures pursue a "*legitimate public policy objective*."[11] Unlike other general exception provisions in Chapter 29, the article-specific exceptions in Articles 14.11(3) and 14.13(3) are novel and are not provided in previous FTAs (Hodson, 2019, p. 601). Therefore, it is unsurprising that the CPTPP does not define what constitutes a "*legitimate public policy objective*" or provide a list of accepted grounds.

Articles 14.11(3) and 14.13(3) set out two conditions, and their legal language is largely modelled on the WTO general exceptions. First, the measure must not be applied in a manner that constitutes "*arbitrary or unjustifiable discrimination or a disguised restriction on trade*." This reflects the *Chapeau test* of Article XX of the GATT 1994 and Article XIV of the GATS 1994. Second, the measure must not impose "*restrictions greater than those necessary to achieve its legitimate policy objective*." This proportionality test in the CPTPP is akin to the concept of the necessary test in the WTO jurisprudence. These non-discrimination conditions are similar to the WTO exception schemes (Mitchell and Mishra, 2021, p. 102), although the CPTPP exception provisions are more tailored (Burri and Kugler, 2024, p. 423).

[9] Article 14.13(2) CPTPP.
[10] Article 14.11(1) and Article 14.13(1) CPTPP.
[11] Article 14.11(3) and Article 14.13(3) CPTPP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

The main difference is that the exception provisions in GATT/GATS provide a list of policy objectives, while the CPTPP's ones are designed with more flexibility and subject to interpretation. Without a list of public policy objectives, the scope of the CPTPP exceptions is unclear, revealing a level of legal ambiguity (Burri, 2023f, p. 14). As such, clarifying the scope of these exceptions helps CPTPP members not to feel threatened that a horizontal obligation on data flows or a ban on data localisation would restrain their ability to regulate the internet for legitimate purposes (Mitchell and Mishra, 2019, p. 407). However, this legal uncertainty is also deliberate to encourage CPTPP parties to accept binding commitments on cross-border data transfers and the location of computing facilities (Peng, 2022, p. 779). Compared to the RCEP exceptions, its members can also adopt restrictive data measures to achieve a legitimate public policy objective. However, RCEP retains a similar "*chapeau*" but replaces the "*necessity test*" with a "*self-judging*" mechanism, allowing members to determine for itself whether the measure is "*necessary to achieve a legitimate public policy objective*."[12] The e-commerce chapter is also excluded from the binding dispute settlement mechanism under Chapter 19 of the RCEP, making its commitments unenforceable as a soft-law commitment.[13]

In conclusion, data-related provisions are a relatively new phenomenon, appearing primarily in the dedicated e-commerce chapters of PTAs and in only a limited number of agreements (Burri and Polanco, 2020, p. 211). While CPTPP is not the first to include such data-related rules, it elevates them into a benchmark framework that has subsequently influenced later PTAs (Burri et al., 2024, p. 207). Widely recognised as a benchmark model for digital trade governance, whether CPTPP's provisions effectively contribute to global digital trade governance or pose implementation challenges for developing countries is an open question. The following sections will explore these issues in further detail.

3. Developing countries in CPTPP and the choice of jurisdictions

To examine how developing countries implement CPTPP's obligations on free flow of data, this section first identifies which CPTPP members are regarded as "developing." It then explains the study's focus on Asian developing members among the 11 CPTPP parties. It is not straightforward to precisely determine which countries are developing or developed. In the international system, labelling them is sometimes controversial, contested, and heterogeneous (Farias, 2024, p. 651). Classifying developed and developing countries varies across international institutions (Farias, 2022, p. 7). Each organisation uses different criteria and indicators to classify its members in line with its specific objectives, operational mandates, and functions.

Within the WTO, there are no agreed-upon definitions of "*developed*" and "*developing*" countries. As a legal principle, the WTO grants special and differential treatment (SDT) to promote equitable and sustainable development, which provides developing members with concessions, such as a longer implementation period, more trading opportunities, and receiving capacity-building support and technical assistance… (World Trade Organization, 2026a). Although SDT provisions were not meant to completely exempt developing countries from obligations (Hegde and Wouters, 2021, p. 571), and their effectiveness remains in question (Tania et al., 2024, p. 123), developing countries tend to take priority in receiving such rights. Instead, the WTO has set a self-declaration mechanism, under which WTO members can self-determine whether they are "*developed*" or "*developing*" countries (World Trade Organization, 2026b). Therefore, it would be inadequate to determine the dichotomy based on one indicator. This study refers to other

[12] Article 12.14(3) and Article 12.15(3) RCEP.
[13] Article 12.17 RCEP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

factors, such as income, economic development, and digital readiness, to ensure a more objective assessment. According to the International Monetary Fund (IMF), the World Economic Outlook divides the world into two groups only: "*advanced economies*" and "*emerging and developing economies*" (IMF, 2023). In contrast, the World Bank differentiates them by income level: *Low-income*, *Lower-middle-income*, *Upper-middle-income*, and *High-income* (The World Bank, 2026). In terms of digital connectivity, access and capacity, the International Telecommunication Union (ITU) measures the digital readiness based on four tiers: *High ICT Development*,*Upper-middle ICT Development*, *Lower-middle ICT Development*, and *Low ICT Development* (International Telecommunication Union, 2025, pp. 5–7).[14] This study uses these indicators to assess and categorise 11 countries of the CPTPP.

Despite different methodological approaches used by international institutions, their classification results are broadly consistent. As shown in Table 1, 6 out of the 11 CPTPP members can rationally be regarded as developing countries (Chile, Mexico, Peru, Brunei Darussalam, Malaysia, and Vietnam), constituting more than half of the membership. Across the four systems, the IMF, the World Bank, the WTO, and the ITU, six developing countries consistently rank in the lowest categories across all indicators. Even for a high-income economy like Brunei, its classification as developing is justified here by its WTO self-declaration and its specific digital infrastructure challenges noted by the ITU, which distinguish it from advanced counterparts like Singapore or Australia.

Regarding the choice of jurisdictions, this study focuses on three Asian developing countries—Brunei Darussalam, Malaysia, and Vietnam—rather than the Latin American members (Chile, Mexico, and Peru), to examine how they navigate the CPTPP's stringent obligations on cross-border data transfers and reconcile these commitments with domestic regulatory sovereignty. Latin American members have achieved a high degree of regulatory convergence of digital trade and data governance through decades of participation in PTAs (Polanco, 2021, p. 298). At the regional level, Latin American members set out regional rules for cross-border data transfer as a shared policy objective through their treaty practice (Vásquez Callo-Müller and Sucker, 2026, p. 4). At the global level, Latin American states have pioneered the integration of digital trade and binding data flow disciplines in PTAs[15] (Polanco, 2025, p. 635). Even before joining CPTPP, Mexico incorporated such provisions into the Mexico–Panama FTA in 2014, which is the first agreement to include a binding provision on cross-border information flows (Polanco, 2021, p. 289). This approach was later solidified in the CPTPP and USMCA.[16] Chile is also a leading Latin American actor in shaping cross-border data transfer rules in bilateral and plurilateral digital trade negotiations as a founding member of the Digital Economy Partnership Agreement (DEPA), and Peru is in the process of acceding (Vásquez Callo-Müller and Sucker, 2026, p. 6). The influence of Latin American countries is also shown in quantitative evidence. According to the Trade Agreement Provisions on Electronic-commerce and Data (TAPED) database, PTAs concluded by Latin American countries account for 33% of all trade agreements worldwide, containing digital trade provisions (Polanco, 2021, p. 271). Therefore, their domestic legal frameworks and treaty practices demonstrate that Latin American countries have acted as active rule-makers in digital trade rule-making, not just a rule-taker since joining CPTPP.

[14] The ICT Development Index (IDI), developed by the International Telecommunication Union (ITU), measures a country's overall level of information and communication technology (ICT) development, including access, usage, and digital skills.

[15] Similar hard rules on data flows have been widely incorporated into many PTAs concluded by Chile, Argentina, Peru, Mexico, and Brazil. Article 4.3 DEPA Article 8.10 Chile–Uruguay FTA; Article 11.6 Argentina–Chile FTA; Article 13.11 Australia–Peru FTA; Article 19.11 USMCA; Article 10.12 Brazil–Chile FTA.

[16] Article 14.11 CPTPP and Article 19.11 USMCA.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Table 1. Mapping the CPTPP members as developed and developing countries

Countries	IMF (World Economic Outlook Database 2023)	World Bank (GNI 2023)	WTO (self-declare status)	ITU (digital readiness)	Overall
Australia	Advanced economy	High income	Developed	High	Developed
Canada	Advanced economy	High income	Developed	High	Developed
Japan	Advanced economy	High income	Developed	High	Developed
New Zealand	Advanced economy	High income	Developed	High	Developed
Singapore	Advanced economy	High income	Developed	High	Developed
Chile	Emerging & developing	High income	Developing	Upper-middle	Developing
Mexico	Emerging & developing	Upper middle income	Developing	Upper-middle	Developing
Peru	Emerging & developing	Upper middle income	Developing	Upper-middle	Developing
Brunei Darussalam	**Emerging & developing**	**High income**	**Developing**	**Upper-middle**	**Developing**
Malaysia	**Emerging & developing**	**Upper middle income**	**Developing**	**Upper-middle**	**Developing**
Vietnam	**Emerging & developing**	**Lower middle income**	**Developing**	**Lower-middle**	**Developing**

In contrast, when joining a typical US-led digital trade governance model like CPTPP, the Southeast Asian cluster (Brunei, Malaysia, and Vietnam), as norm takers, are required to adapt to externally driven digital trade and cross-border data transfer provisions. Compared to Latin American countries, the divergence and fragmentation in domestic data laws of Asian countries have hindered the free flow of cross-border data in Asia (Zhao, 2024, p. 504). They adopt cautious regulatory approaches to unrestricted data movements (van der Marel, 2022, p. 103). As such, retaining its domestic laws on data, more sovereignty-oriented frameworks make them more suitable subjects for exploring the tension between international commitments and domestic regulatory autonomy.

4. Implementation of CPTPP data commitments: how do Asian developing members approach?

4.1. Vietnam

4.1.1. Vietnam's domestic legal framework

The CPTPP entered into force in Vietnam in 2019, considered the first new-generation FTA in Vietnam. Accession required Vietnam to revise, supplement, and pass a wide range of domestic regulations to ensure compliance (VCCI, 2021). At the time of joining the CPTPP, Vietnamese laws on data governance were still nascent, fragmented, and unified (Hang, 2024, p. 15). To examine how Vietnam implements its CPTPP commitments on cross-border data transfer, this section will divide it into two phases, before and after 2023, to highlight the development of data regulations in Vietnam.

a) Before 2023: Fragmented Regulations and Cybersecurity-driven Regulatory Approach

Prior to 2023, privacy and data protection rules existed but were fragmented across multiple sectoral legal regulations (Greenleaf, 2014, p. 361). There were no explicit regulations on cross-border data transfers. Instead of facilitating data flows, the Vietnamese legal framework this time reflected a state-centric and national security-driven approach. To illustrate, the Law on Cybersecurity 2018 and the Decree No. 53/2022/ND-CP on Guiding the Law on Cybersecurity introduce stringent data localisation requirements, applicable to both domestic and foreign enterprises.[17] To foreign companies providing online services in Vietnam,[18] if their services are used to violate Vietnam's cybersecurity laws and they fail to cooperate with the Ministry of Public Security (MPS), such foreign enterprises are required to establish a local branch and representative office in Vietnam.[19] The MPS has the authority to issue a written request ordering data storage or local presence, and the enterprises must comply within 12 months.[20] Beyond privacy and personal data protection, the Law on Cybersecurity 2018 is political and underpinned by political ideology and commitments to national security (Bui and Lee, 2022, p. 641). It also aims to prevent the use of the internet to disseminate information and ideas hostile to the State or contrary to the socialist ideology.[21] It is clear that this framework reveals a

[17] Article 26.3 Law on Cybersecurity 2018 & Article 26.1 of the Decree No. 53/2022/ND-CP.

[18] Online services involve: (i) telecommunication, storing and sharing data in cyberspace, (ii) providing national or international domain names to service users in Vietnam, (iii) e-commerce, online payment, payment intermediary, transport connection services through cyberspace, social networks and social media, online video games; (iv) providing, managing, or operating information in cyberspace in the form of messages, voice calls, video calls, e-mails, online chats.

[19] Article 26.3 Law on Cybersecurity 2018. Article 26.4 Decree No. 53/2022/ND-CP.

[20] Article 27.3 Law on Cybersecurity 2018.

[21] Article 1 and Article 4 Law on Cybersecurity 2018.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

strategic approach that aligns with the concept of data sovereignty rather than viewing data from a digital trade liberalisation perspective under the CPTPP.

b) From 2023: A Dedicated but State-Centred Governance Framework

Vietnam has the first comprehensive and dedicated legal document for personal data protection since the advent of the Decree No. 13/2023 ND-CP on Personal Data Protection (Decree No. 13/2023 ND-CP). However, rather than promoting individual freedom and the integrity of information flows, the Decree also prioritises state oversight and centralised control over information flows with the goal of consolidating national security and policy objectives (Huynh, 2024, p. 553). Accordingly, cross-border transfer of personal data is allowed but not freely under a stringent notification-based mechanism.[22] Personal data can be transferred abroad only after the data controller or processor completes a dossier to assess the cross-border data transfer (known as Data Protection Impact Assessment—DPIA), and then submits it to the MPS[23] to assess and require the completion of the dossier.[24] This administrative monitoring mechanism places a burden of proof on businesses and raises the compliance costs of conducting cross-border data transfers. Furthermore, Decree No. 13/2023 empowers the MPS with a broad discretionary authority to evaluate, inspect, or suspend data transfers if they are deemed to violate the national interests and national security.[25] While legally permissible, cross-border data transfer remains conditional, reflecting a state's oversight over the free movement of data.

Seven years after the CPTPP entered into force, Vietnam has carried out substantial digital regulatory reforms by introducing a new generation of data-related laws, including the Law on Data 2024, Personal Data Protection Law 2025 (Vietnamese Personal Data Protection Law [PDPL] 2025), and Law on Cybersecurity 2025. These new legal regimes provide clearer legal basis for cross-border data transfer mechanisms and introduce more transparent regulatory procedures.

In particular, Article 23(1) of the Law on Data 2024 sets out a principle allowing organisations and individuals to transfer data to and from Vietnam, with their lawful rights and interests protected by the State.[26] However, transfers abroad impose strict conditions on two types of data to protect legitimate policy objectives,[27] which are *important data*[28] and *core data*.[29] Accordingly, the transfer of two categories of data must ensure the protection of national interests, public order, and the legitimate rights of data subjects,[30] and both are determined based on lists issued by the Prime Minister.[31] Similarly, the Vietnamese LPDP 2025 also permits cross-border transfers of personal data[32] but sets a conditional regulatory approach by mandating both domestic and foreign entities must prepare and submit a DPIA dossier to the specialised data protection authority within 60 days from the first cross-border transfer.[33] The DPIA dossier is submitted only once

[22] Article 13.1 Decree No. 13/2023 ND-CP.

[23] The Department of Cybersecurity and High-Tech Crime Prevention (A05) of the Ministry of Public Security.

[24] Articles 25.5 and 13.3 Decree No. 13/2023 ND-CP.

[25] Articles 25.3 and 25.7 Decree No. 13/2023 ND-CP.

[26] Article 23.1 Law on Data 2024.

[27] Article 23.2 Law on Data 2024.

[28] Article 1.6 Law on Data 2024 "*Important data is data that can impact national defense, security, foreign affairs, macroeconomics, social stability, health and public safety in the list issued by the Prime Minister*."

[29] Article 1.7 Law on Data 2024 "*7. Core data is important data that directly impacts national defense, security, foreign affairs, macroeconomics, social stability, health and public safety in the list issued by the Prime Minister*."

[30] Article 23.3 Law on Data 2024.

[31] Articles 1.6 & 1.7 Law on Data 2024.

[32] Article 20.5 Vietnamese LPDP 2025.

[33] Article 20.1 and Article 20.1 Vietnamese LPDP 2025.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

throughout the operation of the organisation and must be updated only when significant changes arise.[34] There is an important change in that the new law replaces the intensive dossier-reviewing approach in Decree No. 13/2023 NC-CP with a post-monitoring mechanism. In this context, businesses are permitted to conduct transfers after fulfilling notification and filing obligations, thereby substantially reducing administrative burdens for cross-border data transfer. Nevertheless, the State retains supervisory and intervention power where national security and interests are implicated, including periodic (no more than once a year) and *ad hoc* inspections in cases of violations or data breaches[35] and the transfers are suspended immediately if "*they may cause harm to national defense or security.*"[36] Another regulatory change lies in the institutional calibration of the data governance framework. The new LPDP 2025 introduces a more independent and dedicated institution, "*specialized data protection authority*" to supervise cross-border data transfer transactions rather than the MPS under Decree No. 13/2023. However, this appears to be a strategic legal design rather than a shift towards an independent public authority mechanism like the EU,[37] since Article 33 explicitly defines this authority as "*an agency affiliated with the Ministry of Public Security.*" Importantly, this institutional choice reinforces the central role of the state in the regulation of cross-border data flows. With regards to data localisation requirements, the newly enacted Cybersecurity Law 2025 continues imposing an explicit obligation requiring certain categories of data to be stored in Vietnam and requiring foreign service providers within its scope to establish a branch or representative office to ensure network information security.[38]

In conclusion, after 2023, Vietnam has established a more comprehensive and dedicated legal regime governing cross-border data flows. Despite these regulatory developments, the state-centric data governance model remains unchanged, in which cross-border data transfers are plainly allowed but still subject to strict state oversight to safeguard national interests and national security. At the same time, Vietnam continues to impose data localisation requirements for specified categories of data and local presence requirements under the cybersecurity regime. These measures reflect a specialised data governance model that prioritises regulatory sovereignty and national security over the liberalisation of data flows in digital trade.

4.1.2. Vietnam's implementation

Vietnam's implementation of the CPTPP's strict data-related obligations reflects a gradual progress of legal and institutional adaptation rather than full liberalisation. At the beginning, Vietnam's domestic data legal framework for cross-border data flow appeared to conflict with CPTPP's obligations, which prohibit members from requiring businesses to use or locate computing facilities as a condition for market access. However, Vietnam initially utilised the transitional mechanism under Article 14.18(2), which provides a temporary exemption from state-to-state dispute settlement for two years[39] since the CPTPP entered into force in Vietnam.[40] In addition, Vietnam reached bilateral agreements

[34] Article 20.3 and Article 22 Vietnamese LPDP 2025.

[35] Article 20.4 Vietnamese LPDP 2025.

[36] Article 20.5 Vietnamese LPDP 2025.

[37] Article 51 GDPR "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')."

[38] Article 25.3 Law on Cybersecurity 2025.

[39] Article 14.18(2) CPTPP.

[40] CPTPP entered into force for Vietnam on 14 January 2019. This date is 60 days after Vietnam deposited its accession documents, which it did on 15 November 2018. Therefore, Vietnam could not be subject to the dispute

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

with CPTPP members to extend the grace period from two to five years.[41] CPTPP signatories also agreed not to initiate disputes over Vietnam's cybersecurity measures on data localisation requirements. During this period, Vietnam has undertaken substantial legislative reforms governing cross-border data transfers. The PDPL 2025 shifted to a *post-monitoring mechanism* which greatly reduces administrative barrier and provides more predictable legal framework. These arrangements do not ease Vietnam's obligation on cross-border data transfer but meaningfully allow Vietnam more time to align its domestic legal framework with the CPTPP's obligation to permit cross-border transfers. The extension underscores Vietnam's regulatory capacity constraints and reveals how important regulatory cooperation is in the early stage of implementing sensitive digital commitments.

Against this backdrop, Vietnam still maintains state control over cross-border data flow by mandating the submission of a DPIA dossier and retaining broad supervisory authority to suspend the data transfers if causing risks to national defence or security. In addition, Vietnam continues reaffirming mandatory data localisation requirements for specific categories of data and covered foreign service providers on the ground of cybersecurity protection.

The question is whether such domestic measures are inconsistent with the CPTPP's obligations concerning the free flow of information across borders and data localisation prohibition. The answer is not straightforward as the CPTPP also allows parties to adopt or maintain measures necessary to achieve legitimate public policy objectives.[42] Vietnam relies heavily on these exception provisions by framing its data localisation and regulatory oversight requirements as necessary to safeguard national security and cybersecurity. Such reliance can be justifiable. In international trade law, national security has been long recognised as legitimate regulatory justification (Van Den Bossche and Zdouc, 2021, p. 591) and WTO jurisprudence has uncovered the State's right to invoke security interest to justify trade-restrictive measures (Prazeres, 2020, p. 137). Beyond the WTO, national security exceptions have been more replicated and tailored in trade and investment agreements with broader scopes to address non-traditional security challenges nowadays and the need for the state to have enough policy space (Esplugues, 2018, p. 115). Therefore, Vietnam's inconsistent measure to restrict data flow can be justifiable if not applied in an arbitrary or unjustifiably discriminatory manner and do not impose restrictions greater than are necessary to achieve those objectives.[43]

In conclusion, the analysis reveals that although Vietnam's legal framework provides a clearer and more predictable mechanism for cross-border data flows, it continues to maintain data localisation and local presence requirements for specified categories of data under the cybersecurity regime. These reforms still remain a level of restriction to the free flow of data in practice, reflecting Vietnam's cautious balancing between regulatory sovereignty with its international commitments to digital trade liberalisation. However, such an approach will not sustain the liberalisation of digital trade envisaged by the CPTPP.

settlement mechanism under Chapter 28 in relation to Article 14.11 (Cross-Border Transfer of Information by Electronic Means) and Article 14.13 (Location of Computing Facilities) from 14 January 2019 to 14 January 2021.

[41] The bilateral agreements could be diplomatic notes, exchange of letters, memorandum of understanding . . . between governments. For example, exchange of letters between Vietnam and Australia, Canada, Malaysia, New Zealand, Japan dated 8 March 2018.

[42] Article 14.11(3) and Article 14.13(3) CPTPP.

[43] Article 14.11(3) and Article 14.13(3) CPTPP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use , available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

4.2. Malaysia

4.2.1. Malaysia's domestic legal framework

The Personal Data Protection Act 2010 (PDPA) is the applicable law governing data privacy and cross-border data transfers in Malaysia. PDPA 2010 came into force in 2013, as the first comprehensive legislation on personal data protection. In the region, the advent of the PDPA 2010 makes Malaysia the first ASEAN country to adopt a specific law on data protection (Yusoff, 2011, p. 132). One of the salient features of PDPA 2010 is its reference to international frameworks and soft-law instruments including the EU Data Protection Directive (95/46/EC), the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the APEC Privacy Framework (Prasetyoningsih et al., 2024, p. 161). However, being established before the CPTPP, PDPA 2010 was not originally designed to accommodate cross-border data rules under the CPTPP or adequately address emerging data-related issues nowadays (Dhali et al., 2022, p. 143).

The core legal tension is in Section 129 (S.129) PDPA 2010, which prohibits the transfer of personal data outside Malaysia unless the conditions are met. In principle, transfers are permitted where the destination jurisdiction appears on an *Adequate Protection List*, publicly gazetted by the Minister.[44] This mechanism mirrors the adequacy approach adopted in the EU data protection regime (Tee, 2002, p. 265), whereby transfers are allowed only to countries providing an equivalent level of protection.[45] However, since the enactment of the PDPA in 2010, no adequate protection list of approved jurisdictions has ever been issued. As a result, most data transfers must rely on narrow exceptions under S.129(3), including explicit consent, contractual necessity, public interest, reasonable precautions, and safeguards.[46] In general, PDPA 2010 imposes a restriction on the free movement of data across borders, reflecting a sovereignty-based regulatory model that prioritises sovereign control over data mobility and trade facilitation. The ministerial approval model and a non-existent whitelist stand in tension with CPTPP commitments on cross-border data transfer.

However, since 2020, Malaysia has reformed PDPA 2010 to align with international standards, which also facilitates the implementation of its commitments under the CPTPP with the amendment of the PDPA in 2024 and the issuance of the Cross-Border Data Transfer Guidelines No.3/2025 (CBPDT Guidelines) under Section 48(g) PDPA 2010. While the amended PDPA 2024 sets out the updated legal framework for cross-border data transfer outside of Malaysia, the Guidelines provide detailed and procedural guidance to ensure compliance under S.129 PDPA. In general, the new framework provides a clearer legal basis for cross-border data flow with two substantive changes. First, the previous whitelist-based adequate protection mechanism has been removed. Although the explicit public interest exception has been removed, the Minister retains discretionary authority in determining permitted transfers under the revised framework. Instead, under the amended regime, cross-border data transfers are now permitted if one of the prescribed statutory conditions or recognised exceptions under S.129(2)–(3) is satisfied, as further elaborated in the CBPDT Guidelines 2025:

First, similar law or adequate protection. A transfer is permitted if the destination jurisdiction falls within one of two statutory grounds: (i) it has laws in force which are "*substantially similar*" to the PDPA; or (ii) it ensures an "*adequate level of protection*" for personal data, at least equivalent to the level of protection provided by the PDPA.[47] Regarding the former, to determine substantial similarity, data controllers need to

[44] To be gazetted refers to the act of being officially published in the Government's official journal for the purpose of conferring legal effect. Section 129(1) of the Personal Data Protection Act 2010.

[45] Article 45 GDPR.

[46] S.129(3)a–S.129(3)h of the Personal Data Protection Act 2010.

[47] S.129(2) PDPA 2010.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

conduct a risk assessment of the legal framework of the receiving countries (similar to a transfer impact assessment—TIA).[48] The assessment aims to ensure the personal data protection regimes in the recipient jurisdiction.[49] Findings of the TIA are valid up to three years. After that, if the relevant foreign law changes during that period, the data controller must review whether the amended law remains substantially similar to the PDPA.[50] Unlike Vietnam's DPIA regime, which prioritises consideration of national defence and security, and public interests,[51] Malaysia focuses on the protection of personal data in commercial transactions and private sectors (Prasetyoningsih et al., 2024), modelled on international data protection frameworks (Yusoff, 2011). About the latter condition, to determine whether receiving countries have an *adequate level of protection* for the Malaysian PDPA, data controllers also must conduct a TIA.[52] The purpose of this is to examine factors such as security measures and policies; legally enforceable obligations; data protection law enforceability and compliance mechanism; regulatory authority comparable to Malaysia's Department of Personal Data Protection . . . [53] Findings also last up to three years and must be reassessed if foreign laws change.[54]

Second, exceptions for cross-border data transfers under PDPA 2010. Besides two statutory principles for cross-border data transfers, the PDPA also recognises multiple exceptions under Section 129(3). These exceptions are elaborated through the CBPDT Guidelines 2025 with interpretation and procedural guidance to ensure compliance.

I. Consent of the Data Subject: A transfer proceeds if the data subject has given explicit consent.[55] The data subject is provided with a written notice which details (i) the class of third parties who will receive the data and (ii) the purpose of the transfer. The consent must be recorded and stored by the data controller as proof of compliance. If the data subject cannot give consent, a transfer may still be permitted to mitigate harm to the data subject, provided that reasonable efforts have been made to obtain consent.[56] In limited cases where consent cannot be obtained, transfers remain possible to mitigate harm.
II. Necessary for Contract or Vital Interests: Transfers are allowed necessary for performing or concluding a contract to which the data subject is a party, or to protect the data subject's vital interests.[57] The CBPDT Guidelines interpret the term "*necessary*" as not meaning "*absolutely essential*" but denotes a transfer made for a specific purpose directly connected with the contractual obligations of the data controller.[58] The transfer must not be routine or general but linked to the core purpose of the contract. Data controllers are expected to assess whether the purpose of the transfer could reasonably be achieved by other means.[59] Where the transfer is for the conclusion or performance of a contract with a third party at the data subject's request or in their interest, the request must be in writing or recorded. The data controller must ensure that the interest of the data subject is

[48] Para 5.3 CBPDT Guidelines 2025.
[49] Paras 5.4 CBPDT Guidelines 2025.
[50] Paras 5.6–5.7 CBPDT Guidelines 2025.
[51] Article 20.5 Vietnamese LPDP 2025 & Article 25.8 Decree No. 13/2023 ND-CP.
[52] S.129(2)(b) PDPA 2024.
[53] Paras 6.3 CBPDT Guidelines 2025.
[54] Paras 6.5–6.6 CBPDT Guidelines 2025.
[55] S.129(3)(a) PDPA.
[56] S.129(3)(e) PDPA 2010 & Paras 11.1–11.2 CBPDT Guidelines 2025.
[57] S.129(3)(b), (c), (g) PDPA 2010.
[58] Paras 8.3–9.4 CBPDT Guidelines 2025.
[59] Paras 8.3–8.5 CBPDT Guidelines 2025.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

clear, direct, targeted, and substantial, such as travel arrangements, ensuring a data subject's family holiday.[60]

III. Legal Purposes: Data is transferred abroad when necessary for legal proceedings and for obtaining legal advice, or for establishing, exercising, or defending legal rights.[61] The CBPDT Guidelines also broaden this to include proceedings before courts, tribunals, administrative bodies, and regulatory authorities, as well as alternative dispute resolution such as mediation or arbitration.[62] However, this ground does not apply to speculative or potential cases; it covers only ongoing or imminent legal matters, or situations involving pre-action correspondence and formal regulatory requests.

IV. Reasonable Precautions and Due Diligence: Under S.129(3)(f) PDPA 2010, transfers are permissible where data controllers take reasonable precautions and exercise due diligence to ensure compliance with PDPA standards.[63] Furthermore, the CBPDT Guidelines 2025 clarify this as a flexible safeguard mechanism, allowing data controllers to rely on recognised frameworks, such as binding corporate rules, standard contractual clauses, or certification schemes that demonstrate equivalent protection standards.[64] For example, an intra-group transfer under a Binding Corporate Rules (BCRs) is valid if the policy is legally binding, sets out the applicable jurisdictions, ensures equivalent protection, and grants enforceable data-subject rights and complaint mechanisms. This exception reflects Malaysia's shift towards a risk-based accountability approach, enabling organisations to justify cross-border transfers through demonstrable compliance measures rather than prior government authorisation.

Although the PDPA 2024 amendments on cross-border data transfer remain limited in scope and institutional design (Greenleaf, 2025, p. 1), the amendment to the PDPA 2010, as well as the CBPDT Guidelines 2025, establishes a clearer, comprehensive, risk-based framework for cross-border personal data transfers. By grounding transfers in protection standards rather than prior ministerial approval, Malaysia enhances legal certainty and better facilitates the modern digital economy.

4.2.2. Malaysia's implementation

CPTPP became effective for Malaysia in late 2022, while the PDPA 2010 had been enacted more than a decade before. Interestingly, implementing the CPTPP requires modest adjustments to Malaysian domestic law in line with the CPTPP's e-commerce regulations (Azmi and Jeong, 2020, p. 66). With an updated legal regime in 2024, Malaysia's applicable legal framework is broadly compatible with the CPTPP cross-border data obligations.

Although PDPA does not impose explicit data localisation requirements, it regulates cross-border data transfers through conditions under S.129. The PDPA retains its regulatory autonomy to restrict cross-border data flows overseas and sets out conditions for that. However, its regulatory sovereignty serves as a mechanism of accountability rather than state control, as it aims to protect the privacy and personal data of citizens. The ultimate purpose of these conditions set out in S.129 PDPA is to assess risks and ensure accountability in data transfer abroad. Under the amended PDPA, data controllers have the burden of proof to demonstrate that a transfer meets the standards of "*substantially similar*

[60] Paras 9.1–9.4 CBPDT Guidance 2025.
[61] S.129.(3)(d) PDPA 2010.
[62] Paras 10.1–10.3 CBPDT Guidance 2025.
[63] S.129(3)(f) PDPA 2010.
[64] Paras 12.1–12.4 CBPDT Guidance 2025.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

law" or "*an equivalent level*" of protection in the recipient jurisdictions. This regulatory calibration avoids imposing restrictions greater than are required to achieve the objective, thus satisfying the necessity and proportionality tests under Articles 14.11 and 14.13 of the CPTPP.

Additionally, domestic measures such as TIA, BCRs, Standard Contractual Clauses (SCCs), or certification schemes are equally applied in a non-discriminatory manner to both foreign and domestic businesses when conducting cross-border data transfers. This fair application helps Malaysia to avoid an arbitrary or discriminatory treatment or constitutes a disguised restriction on trade under Articles 14.11(3) and 14.13(3) CPTPP. On the one hand, the Malaysian legal regime remains restrictive by stipulating a prohibitive default rule rather than being fully free for data flow. On the other hand, Malaysia's legal framework on cross-border personal data transfers basically fulfils the obligations and does not conflict with the CPTPP's commitments. From a restrictive, ministerial-control model to a risk-based framework, Malaysia's recently revised data protection regime demonstrates its effort to reconcile domestic privacy regulations with international trade obligations. These reforms bring Malaysia closer to the CPTPP's objectives of facilitating digital trade.

4.3. Brunei Darussalam

4.3.1. Brunei's domestic legal framework

The CPTPP entered into force for Brunei Darussalam in 2023. Unlike Malaysia, Brunei has not enacted dedicated legislation governing personal data before the CPTPP. In 2025, Brunei introduced the Personal Data Protection Order (PDPO) as the country's first comprehensive data protection regime. The PDPO 2025 applies to individuals, private entities, and non-governmental organisations operating in Brunei that process personal data in the course of their activities,[65] while government agencies are not.[66] In particular, under S.24 PDPO 2025, the transfer of personal data outside Brunei is permissible but subject to statutory conditions. No organisation is allowed to transfer data abroad unless it ensures that the foreign recipient provides a level of protection comparable to that under the PDPO.[67] This provision reflects the principle of "*adequacy*," similar to the EU GDPR[68] and Malaysia's PDPA 2010, which requires equivalence in protection standards rather than allowing unrestricted data flows. Accordingly, the organisation transferring data abroad must ensure the recipient provides a standard of protection equivalent to Brunei's PDPO 2025 (*comparable level of protection*).[69]

Furthermore, S.24(2)-(4) PDPO 2025 sets out discretionary exemptions from the "*prescribed requirements*" through an administrative mechanism, Technology Industry of Brunei Darussalam (AITI Authority).[70] This state agency holds the power to grant an exception on a case-by-case basis upon written application.[71] The organisation applying for the exemption must justify the request by showing that it has taken suitable measures to protect the data and that the transfer will not undermine the level of protection guaranteed under the PDPO. This exemption mechanism raises critical concerns regarding

[65] Section 2 Personal Data Protection Order 2025.

[66] Government agencies are required to manage personal data responsibly under existing frameworks, including the Data Sharing Guidelines and the Official Secrets Act.

[67] Section 24.1 Personal Data Protection Order 2025.

[68] Article 45 GDPR.

[69] Section 24(1) Personal Data Protection Order 2025.

[70] Section 2 Personal Data Protection Order 2025 "Authority" means the Authority for Info-communications Technology Industry of Brunei Darussalam established by Section 3 of the Authority for Info-communications Technology Industry of Brunei Darussalam Order, 2001 (S 39/2001).

[71] Sections 4 & 5 Personal Data Protection Order 2025 regulate functions and duties of Authority.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

legal certainty and transparency. Specifically, S.24(3)(a) stipulates that such exemptions "*need not be published in the Gazette*" and may be revoked "*at any time*." These powers emphasise a broad administrative discretion of the AITI Authority to determine conditions for exemptions, which may include restrictions on the type of data, duration of transfer, or specific security measures. Lack of publication on exceptions reduces transparency and predictability for other organisations seeking similar exemptions, thereby creating legal uncertainty for ongoing data flows. Furthermore, the AITI Authority also has the power to "*add to, vary or revoke any condition*" or the exemption itself "*at any time*."[72] On the one hand, this mechanism gives the data protection state agency strong control to adapt to new challenges and norms without amending the PDPO itself. On the other hand, Section 24.4 PDPO also implies continuous regulatory oversight since the exemption is not permanent but subject to ongoing administrative review rather than operating as permanent approvals. While this promotes accountability, it escalates burdens and compliance costs for organisations.

4.3.2. Brunei's implementation

Regarding data location requirements, the PDPO 2025 does not explicitly impose data localisation mandates, which indicates alignment with CPTPP Article 14.13. Regarding Brunei's implementation of cross-border data transfer regulations, Brunei's framework does not appear to create a legal conflict with Article 14.11 CPTPP that obligation "*shall allow the cross-border transfer of information by electronic means*," as cross-border transfers outside Brunei remain legally permissible although subject to conditions, particularly where the receiving jurisdiction provides a comparable level of protection. This adequacy requirement can be justified to pursue the legitimate public policy objective under the CPTPP exception framework to protect the fundamental right to privacy and the personal data of its citizens. Accordingly, Brunei's compliance with cross-border data flows ensures compatibility with the CPTPP's rule on data flows.

However, the discretionary exemption mechanism in S.24(2)–(4) raises concern about whether such measures are arbitrary, discriminatory, and more restrictive than necessary when the AITI Authority can "*grant, modify, or revoke exemptions at any time*" and its decisions "*need not be published in the Gazette*." Applying these conditions reveals a potential risk of non-compliance with the CPTPP, that such domestic measures must be applied in a manner that does not constitute an arbitrary or unjustifiable discrimination or a disguised restriction on trade, especially where exemptions are granted on a case-by-case basis by the AITI Authority without clear public criteria or procedural safeguards. This administrative discretion and exceptions under S.24(2)–(4) may constitute an element of arbitrariness. In addition, the CPTPP transparency obligation mandates that each party shall ensure that its laws, regulations, procedures, and administrative rulings of general application are promptly published or made available.[73] In this context, the unpublished and discretionary exception mechanism makes it difficult to assess whether Brunei's framework satisfies the CPTPP requirements that restrictions on cross-border data transfers should not be applied more restrictively than necessary to achieve legitimate public policy objectives.

In conclusion, Brunei's domestic legal framework for cross-border data governance does not violate the provisions in the CPTPP. The country preserves national sovereignty and administrative discretion to regulate cross-border data transfers. The lack of legal clarity and procedural transparency in its implementation could expose Brunei to risks of inconsistency or non-compliance with data commitments in CPTPP.

[72] Section 24(4) Personal Data Protection Order 2025.

[73] Article 26.2(1) CPTPP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

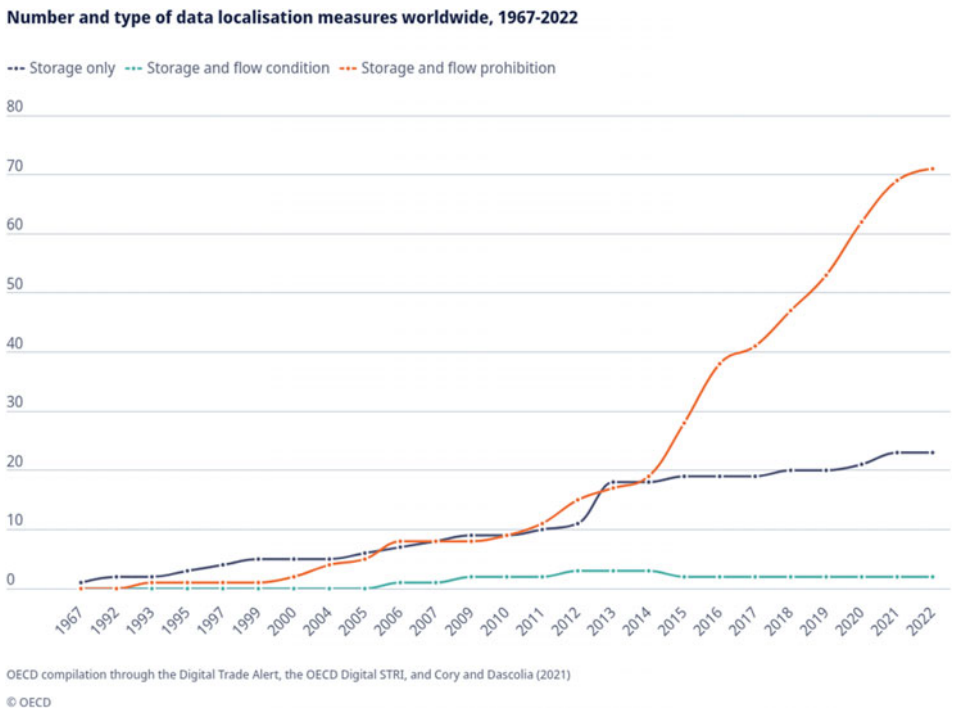


Figure 1. Number of data localisation measures worldwide 1976–2022 *Source:* OECD (2026)

5. Measuring the level of data restrictiveness: compliance, but at what cost?

In recent years, data-restrictive measures have been increasingly adopted across jurisdictions (see Figure 1). In other words, adopting domestic data measures is not a recent trend. According to the OECD, there were nearly 100 data localisation measures adopted across 40 countries by 2023. Notably, these measures are more prevalent in non-OECD countries, many of which are developing countries (OECD, 2023, p. 13). Governments not only have the right but also the responsibility to protect the privacy and security of the data of their citizen as it flows across borders (Chander and Lê, 2015, p. 739). Beyond privacy, they have adopted data localisation measures on many grounds, such as to ensure access to information for regulatory purposes, safeguard national security, strengthen digital security by keeping processing domestic, and promote data protectionism to build domestic capacity in the data-driven economy (OECD, 2023, pp. 6–7). While the United States frequently views data localisation measures as barriers to digital trade and the free flow of information, several competing states employ such measures as instruments of digital sovereignty to challenge US dominance in the global digital economy (Selby, 2017, p. 227).

More importantly, domestic data measures are becoming more restrictive (OECD, 2023, p. 13). The analysis in Section 4 shows that the legal frameworks of Vietnam, Malaysia, and Brunei all impose restrictions on cross-border data flow, albeit at different levels. To evaluate it, this article refers to several analytical frameworks, focusing on two forms of data regulations: data localisation and cross-border data transfers.

5.1. First, data localisation regulations

The analysis begins with a general classification based on the agent-based model (ABM), which divides data localisation regulations into three types: *(i) no restrictions, (ii) less restrictive, (iii) highly restrictive* (see Table 2) (Potluri et al., 2020, p. 3). Under this model, the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Table 2. Assessment of data localisation regulations of Malaysia, Vietnam, and Brunei

Categories	Descriptions	Countries
No restriction	No restrictions where there is no data localisation restriction. This allows free and unconditional flow of data.	
Less restrictive	Less restrictive where countries allow data flows, but subject to specific conditions.	**Malaysia, Vietnam, and Brunei**
Highly restrictive	Highly restrictive means countries impose explicit data localisation measures and prohibit cross-border data flows.	

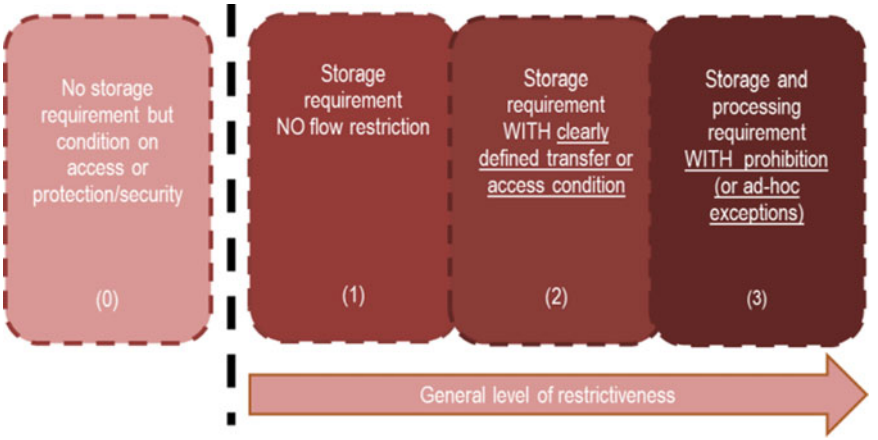


Figure 2. A typology of data localisation measures and requirements for data flow *Sources:* OECD (2023)

legal frameworks of Malaysia, Vietnam, and Brunei fall within the *less restrictive* category as none of these jurisdictions impose explicit data localisation requirements or completely prohibit cross-border data flows. Instead, cross-border data transfers are permitted, albeit under a conditional mechanism. However, this classification remains so broadly general and relative that it cannot fully capture the different levels of data restrictiveness across all jurisdictions. Although Malaysia, Vietnam, and Brunei all allow cross-border data transfers, the legal conditions, administrative mechanisms, and scope of exceptions established are divergent.

When regulating cross-border data transfer, states rely on conditional transfer mechanisms and discretionary oversight at varying levels. As discussed earlier, Malaysia, Vietnam, and Brunei have different approaches to cross-border data localisation. To further analyse these defferences, this paper refers to a more specific analytical framework, "*A typology of data localization measures and requirements for data flow*," which was developed in 2023 by OECD experts (see Figure 2 and Table 3) (OECD, 2023). It assesses restrictiveness along three key theoretical dimensions: (i) whether localisation obligation exists, (ii) the legal and practical restrictiveness of cross-border data transfer, and (iii) the degree of regulatory discretion and transparency governing such transfers. The result shows different national approaches to domestic data localisation regulations: Brunei's prohibitive sovereignty model, Vietnam's conditional sovereignty approach, and Malaysia's liberal compliance-based framework.

Vietnam's recent post-2025 legislative framework, including the Law on Data 2024, the LPDP 2025, and the new Law on Cybersecurity 2025, maintains explicit mandatory

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Table 3. Assessment of domestic data localisation regulations in Malaysia, Vietnam and Brunei

Categories	Descriptions	Countries evaluated
Category 0: No local storage requirement, but condition on access or protection/ security	No obligation to store data domestically, but conditions may apply to access, security, or protection.	
Category 1: Local storage requirement—NO flow restriction	Measures requiring that data be stored or retained domestically, while permitting unrestricted cross-border storage or processing. The objective is to ensure local availability without limiting international data flows.	
Category 2: Local storage requirement—WITH clearly defined transfer or access condition	Frameworks imposing local storage or processing obligations but allowing data transfer abroad under specified and transparent legal or technical conditions. The flow of data is conditional but not prohibited.	**Malaysia and Vietnam**
Category 3: Local storage and processing requirement—WITH flow prohibition (or ad hoc exceptions)	Highly restrictive regimes mandating domestic storage and processing while prohibiting or severely limiting cross-border transfers, subject only to discretionary or case-by-case exemptions. These reflect sovereignty-centered or security-driven control over data flows.	**Brunei**

data localisation requirements, while establishing conditional data flow mechanisms, moving away from Category 3. Accordingly, cross-border data transfers are permitted but subject to clearly defined legal conditions, including DPIA filing obligations, regulatory supervision, and the possibility of suspension where national security or national interests are implicated. At the same time, the Law on Cybersecurity 2025 maintains mandatory data localisation requirements for specified categories of data and requires certain foreign service providers to establish a local branch or representative office. Although these requirements may be justified under the CPTPP's legitimate public policy exceptions, they nevertheless preserve a high degree of state control over cross-border data flows. Therefore, I place Vietnam within Category 2, but at its restrictive end, where conditional transfer mechanisms coexist with regulatory discretion.

Malaysia falls within Category 2, but its approach is different from Vietnam's. Following PDPA amendments 2024 and the issuance of the Guidelines 2025, Malaysia has moved from ministerial approval mechanisms to a risk-based framework. Transfers are permitted where substantial similarity or adequacy is demonstrated through TIA. The Guidelines further elucidate clear statutory exceptions (e.g., consent, contractual necessity, and law enforcement purposes). As such, Malaysia remains within Category 2 but represents its liberal approach where conditional transfers are regulated by more predictable and transparent legal procedure.

Brunei is placed in Category 3 because the PDPO 2025 regulates cross-border data transfer through a prohibitive default rule and broad administrative discretion. The AITI Authority may grant exemptions on a case-by-case basis, without publication, and may revoke them at any time. The absence of procedural transparency and the reliance on *ad hoc* exemptions show that Brunei maintains a data sovereignty approach where localisation and discretionary authorisation restrict cross-border data flows.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use , available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

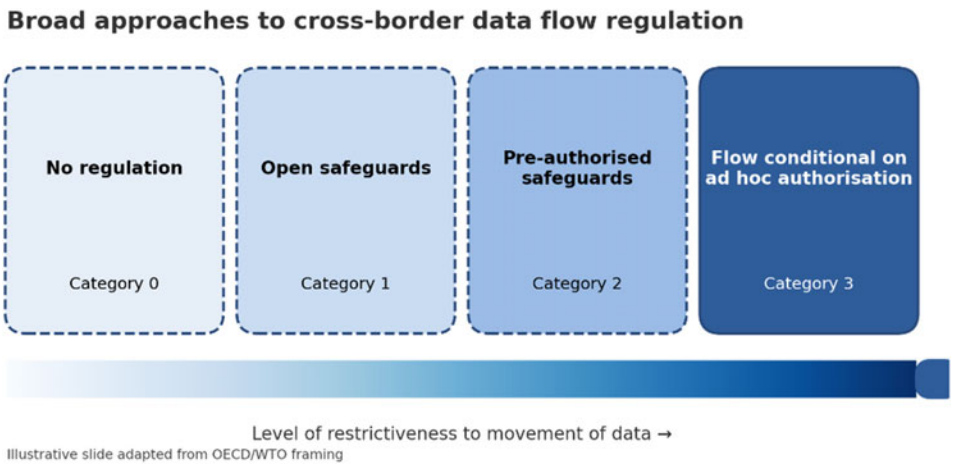


Figure 3. Types of cross-border data flow regulations *Source:* OECD and WTO (2025, p. 16)

Table 4. Assessment of cross-border data flow regulations of Malaysia, Vietnam, and Brunei

Categories	Descriptions	Countries evaluated
Category 0: No regulation	No cross-border data flow regulation because there is no privacy and data protection law. This implies no restriction on data movement, but may affect firms' willingness to transfer data.	
Category 1: Open safeguards	Transfers are allowed with greater discretion to the private sector. Mechanisms include ex post accountability, contracts governing data flows, or private sector-led adequacy decisions.	
Category 2: Pre-authorised safeguards	Transfer allowed but subject to a pre-determined and transparent public sector approval mechanism established by public authorities. In the absence of an adequacy decision, transfers still proceed through contractual clauses or using binding corporate rules, or among other mechanisms.	**Malaysia**
Category 3: Conditional/*ad hoc* authorisation	Transfers permitted only on a case-by-case basis, subject to review and approval by relevant authorities. Applies to personal data for privacy reasons and also to broader categories of "important data," including national security.	**Vietnam and Brunei**

5.2. Second, cross-border data transfer regulations

Regarding regulations on cross-border data transfer, the paper also adopts the OECD analytical framework, which provides a more systematic taxonomy for evaluating the degree of restriction of cross-border data regulations and state intervention in cross-border data flows (OECD and WTO, 2025, p. 16). This framework divides four groups from no regulation to conditional or *ad hoc* authorisation mechanisms as illustrated in Figure 3 and Table 4.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Applied to Vietnam, Malaysia, and Brunei, this taxonomy reveals that all three legal regimes embed varying degrees of restrictiveness. Malaysia is placed in Category 2, as its amended PDPA 2010 and the Guidelines 2025 permit data transfers abroad under predefined statutory and contractual conditions. Transfers are allowed if the receiving jurisdiction provides "*substantially similar*" or "*adequate*" protection or falls within one of the specified exceptions, such as consent or contractual necessity. This rule-based, risk-assessment approach no longer requires prior ministerial authorisation, thus representing a conditional but liberal model consistent with the pre-authorised safeguard category. In contrast, Vietnam and Brunei fall within Category 3 due to their reliance on state-centric and discretionary approval mechanisms. Vietnam's current framework permits cross-border data transfers subject to mandatory compliance obligations, including DPIA filing requirements, regulatory notification, and post-transfer supervisory powers. The competent authority retains broad powers to inspect, suspend, or restrict transfers on grounds of national security or public interest. Similarly, Brunei's PDPO 2025 establishes a default prohibition on cross-border transfers. Cross-border data transfers are permitted when the adequacy level of protection is ensured. However, the AITI Authority can grant case-by-case exemptions issued by it.

6. Concluding remarks

Based on the legal analysis of the CPTPP cross-border data framework and the domestic implementation of its cross-border data flow obligations by Vietnam, Malaysia, and Brunei, as well as the assessment of data restrictiveness according to the OECD analytical framework, I put forward several key observations to conclude this paper.

First, the CPTPP's binding digital trade rules pave the way for domestic data regulatory reforms in all jurisdictions. Consistent with the principle that treaty commitments require good-faith implementation,[74] each state has introduced or revised its legal frameworks to address cross-border data transfers and localisation to ensure its compliance. Malaysia amended its long-existing *Personal Data Protection Act 2010* in 2024 and introduced detailed *Cross-Border Data Transfer Guidelines 2025* to align with modern international standards, shifting its cross-border data transfer mechanism towards risk and compliance. Vietnam, after the expiry of its transitional phases, conducted a comprehensive legal reform by formally removing mandatory data localisation requirements and setting out procedural rules for data transfer, strategically reducing overt conflict with CPTPP obligations. Similarly, Brunei enacted its first comprehensive Personal Data Protection Order 2025 to regulate personal data protection and how data is transferred outside the country. Data flows more freely than ever before, making it harder for individuals to protect their privacy, leading to public demand for governments to act. But when data goes beyond a sovereign territory, governments cannot act alone without international cooperation, which, for the moment, leads to trade agreements (Wolfe, 2019, p. 65). Implementation of hard rules in PTAs has catalysed the adoption of domestic privacy legislation, albeit at varying speeds and degrees of sovereignty sensitivity (Burri, 2023e, p. 94). These state practices collectively illustrate the CPTPP's normative influence over domestic rule-making in the data-driven sector and show how trade disciplines can precede, and accelerate, the construction of national privacy and data-protection regimes.

Second, all countries have consistently sought to retain their regulatory autonomy and to tailor the conditions governing cross-border data transfers in accordance with their national priorities. In international trade law, trade is not always superior. In certain

[74] Article 26 Vienna Convention on the Law of Treaties (1969).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

situations, states have some room to deviate from established rules to achieve other priorities, such as national security, public health, public morality, and environmental protection. This regulatory space is commonly referred to as the "*right to regulate*" in international investment law (Titi, 2014), allowing States to exercise their sovereign powers and impose measures on investments in the interest of public welfare (Baltag et al., 2023, p. 385). Interpretive practice in international trade law reveals that the right to regulate is a principle of regulatory autonomy (Mitchell, 2023, p. 465). Nowadays, this principle is embedded in modern digital trade agreements, which recognise that sovereign states allow them to adopt measures necessary to achieve legitimate public policy objectives (Burri and Kugler, 2024, p. 423).

In this context, Vietnam, Malaysia, and Brunei strategically refer to exceptions provided in CTPPP[75] to set out conditions for cross-border data transfers under a conditional mechanism. Malaysia relies on the privacy exception to implement a compliance-based framework focused on accountability and legal equivalence. Vietnam focuses on national security considerations, prioritising state control and cybersecurity through discretionary oversight by the MPS. Brunei applies an adequacy requirement with a discretionary administrative authorisation mechanism. While the legality of these domestic measures remains open to interpretation and application, such practices demonstrate how developing members exercise their regulatory autonomy within the permissible bounds of the CPTPP's digital trade framework. This also reflects their ongoing efforts to reconcile sovereignty with international compliance and to balance the liberalisation of cross-border data flows with the protection of domestic policy objectives.

Third, despite regulatory reforms conducted to ensure compatibility with the CPTPP data obligations, domestic data laws across all jurisdictions reveal a varying level of restriction on data flow. Cross-border data transfers are allowed but subject to certain conditions, such as procedural complexity, security-driven conditions, case-by-case approval mechanisms, and low administrative transparency. Although legally justifiable under CPTPP's general exception provisions,[76] these measures cause persistent tensions between the commitments to facilitate digital trade and the national policy space to regulate digital industries. In practice, restrictive or uncertain transfer conditions may increase compliance costs and reduce legal predictability, which will not sustain digital trade in the long term and go against the spirit of seamless digital trade within the CPTPP framework. The differing and non-uniform approaches governing cross-border data transfers in Malaysia, Vietnam, and Brunei show both the flexibility and the limitations of the CPTPP's digital trade model. On the one hand, the CPTPP provides members sufficient regulatory space to design their own transfer mechanisms, reflecting the Agreement's respect for national policy priorities. On the other hand, the absence of common standards or mutual recognition mechanisms has resulted in fragmented implementation and uneven levels of restrictiveness across jurisdictions.

Acknowledgements. The author expresses sincere gratitude to the Centre for International Law at the National University of Singapore (CIL NUS) for organizing the "AI Sovereignty and International Law" conference, and the speakers for their insightful comments. The author would like to thank the anonymous reviewers for their constructive comments and valuable suggestions. The author is also grateful to Associate Professor Imogen Saunders of the Australian National University for her careful reading of the manuscript and insightful feedback.

Financial support. This research has been done under the research project number "*DHL-25.19.QT*" of the University of Law, Vietnam National University, Hanoi.

[75] Article 14.11(1)(3) & Article 14.13(1)(3) CPTPP.

[76] Chapter 29 CPTPP; Article 14.11(3) & Article 14.13(3) CPTPP.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

References

Aaronson, S. A. and Leblond, P. (2018). 'Another digital divide: The rise of data realms and its implications for the WTO', *Journal of International Economic Law*, 21(2), pp. 245–272.

Agarwal, B. and Mishra, N. (2023). 'Incorporating digital development perspectives in international trade law', in Brożek, B., Kanevskaia, O. and Pałka, P. (eds) *Research handbook on law and technology*. Cheltenham: Edward Elgar Publishing, pp. 296–314.

Azmi, I. M. A. G. and Jeong, C. P. (2020). 'International norms in regulating e-commerce: The electronic commerce chapter of the comprehensive Trans-pacific Partnership Agreement', *International Journal of Business and Society*, 21(S1), pp. 66–80.

Baltag, C., Joshi, R. and Duggal, K. (2023). 'Recent trends in investment arbitration on the right to regulate, environment, health and corporate social responsibility: Too much or too little?' *ICSID Review - Foreign Investment Law Journal*, 38(2), pp. 381–421.

Farias, D. B. L. (2022). 'Which countries are "developing"? Comparing how international organizations and treaties divide the world', *Political Geography Open Research*, 1, article no. 100001.

Farias, D. B. L. (2024). 'Unpacking the "developing" country classification: Origins and hierarchies', *Review of International Political Economy*, 31(2), pp. 651–673.

Brzytwa, E., Cory, N. and Ezell, S. (2021). 'Understanding the TPP agreement e-commerce chapter', in Gantz, D. A. and Huerta-Goldman, J. A. (eds) *The comprehensive and progressive trans-pacific partnership: Analysis and commentary*. Cambridge: Cambridge University Press, pp. 443–457.

Bui, N. and Lee, J.-A. (2022). 'Comparative cybersecurity law in socialist Asia', *Vanderbilt Journal of Transnational Law*, 55(3), pp. 631–679.

Burri, M. (2021). 'Data flows and global trade law', in Burri, M. (ed) *Big data and global trade law*. Cambridge: Cambridge University Press, pp. 11–41.

Burri, M. (2023a). 'Digital transformation as a reshaper of global trade law', in Mathis, K. and Tor, A. (eds) *Law and economics of the digital transformation*. Cham: Springer Nature Switzerland, pp. 387–407.

Burri, M. (2023b). 'The impact of digitalization on global trade law', *German Law Journal*, 24(3), pp. 551–573.

Burri, M. (2023c). 'Creating data flow rules through preferential trade agreements', in Chander, A. and Sun, H. (eds) *Data sovereignty*. New York: Oxford University Press, pp. 264–292.

Burri, M. (2023d). 'Trade law 4.0: Are we there yet?' *Journal of International Economic Law*, 26(1), pp. 90–100.

Burri, M. (2023e). 'Cross-border data flows and privacy in global trade law: Has trade trumped data protection?' *Oxford Review of Economic Policy*, 39(1), pp. 85–97.

Burri, M. (2023f). 'Digital trade rulemaking in free trade agreements', in Collins, D. and Geist, M. (eds) *Research handbook on digital trade*. Cheltenham: Edward Elgar Publishing, pp. 9–27.

Burri, M. (2024). 'Inequalities in digital trade and digital trade regulation', in Askin, E. and Stoll, H. (eds) *Contested equality: International and Comparative Legal Perspectives*. Cheltenham: Edward Elgar Publishing, pp. 203–220..

Burri, M. (2025). 'Digital trade: New design elements in preferential trade agreements', in Claussen, K., Elsig, M. and Polanco, R. (eds) *The concept design of a twenty-first century preferential trade agreement*. Cambridge: Cambridge University Press, pp. 146–167.

Burri, M. and Kugler, K. (2024). 'Regulatory autonomy in digital trade agreements', *Journal of International Economic Law*, 27(3), pp. 397–423.

Burri, M. and Polanco, R. (2020). 'Digital trade provisions in preferential trade agreements: Introducing a new dataset', *Journal of International Economic Law*, 23(1), pp. 187–220.

Burri, M., Vásquez Callo-Müller, M. and Kugler, K. (2024). 'The evolution of digital trade law: Insights from TAPED', *World Trade Review*, 23(2), pp. 190–207.

Chander, A. and Lê, U. (2015). 'Data nationalism', *Emory Law Journal*, 64(3), pp. 677–739.

Collins, D. (2025). 'Digital trade', in Collins, D. and Vadi, V. (eds) *Routledge handbook on international economic law*. London: Routledge, pp. 257–270.

Dhali, M., Hassan, S., Zulhuda, S. and Bt Ismail, S. F. (2022). 'Artificial intelligence in health care: Data protection concerns in Malaysia', *International Data Privacy Law*, 12(2), pp. 143–161.

Elsig, M. and Klotz, S. (2021). 'Data flow-related provisions in preferential trade agreements: Trends and patterns of diffusion', in Burri, M. (ed) *Big data and global trade law*. Cambridge: Cambridge University Press, pp. 42–62.

Esplugues, C. (2018). *Foreign investment, strategic assets and national security*. Cambridge: Intersentia, pp. 115–134.

Gao, H. (2017). 'The regulation of digital trade in the TPP: Trade rules for the digital age', in Chaisse, J., Gao, H. and Lo, C. (eds) *Paradigm shift in international economic law rule-making*. Singapore: Springer Singapore, pp. 345–362.

Gao, H. (2018a). 'Regulation of digital trade in US free trade agreements: From trade regulation to digital regulation', *Legal Issues of Economic Integration*, 45(1), pp. 47–70.

Gao, H. (2018b) 'Digital or trade? The contrasting approaches of China and US to digital trade', *Journal of International Economic Law*, 21(2), pp. 297–321.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Gao, H. (2023a). 'Data sovereignty and trade agreements: Three digital kingdoms', in Chander, A. and Sun, H. (eds) *Data sovereignty: From the digital Silk Road to the return of the state*. New York: Oxford University Press, pp. 213–239.
Gao, R. Y. (2023b). 'A battle of the big three?—Competing conceptualizations of personal data shaping transnational data flows', *Chinese Journal of International Law*, 22(4), pp. 707–787.
Gao, R. Y. (2024). 'The diffusion of a U.S. trade-based approach to international personal data transfers and its implications for national data privacy regulations', *International Data Privacy Law*, 14(4), pp. 352–376.
Greenleaf, G. (2014). 'Vietnam and Indonesia—ASEAN's sectoral laws', in *Asian data privacy Laws: Trade & human rights perspectives*. Oxford: Oxford University Press, pp. 361–388.
Greenleaf, G. (2025). *Malaysia's complex new Guidelines on cross-border data transfers*. Available at: https://doi.org/10.2139/ssrn.5582014 (Accessed: 17 May 2026).
Han, S. (2024). 'Data and statecraft: Why and how states localize data', *Business and Politics*, 26(2), pp. 263–288.
Hang, N. H. B. (2024). 'Addressing fragmentation in Vietnam's data protection laws: Recommendations for a unified legal framework', *Vietnamese Journal of Legal Sciences*, 11(2), pp. 14–26.
Hegde, V. and Wouters, J. (2021). 'Special and differential treatment under the world trade organization: A legal typology', *Journal of International Economic Law*, 24(3), pp. 551–571.
Hodson, S. (2019). 'Applying WTO and FTA disciplines to data localization measures', *World Trade Review*, 18(4), pp. 579–607.
Huynh, T. T. (2024). 'Everyone is safe now: Constructing the meaning of data privacy regulation in Vietnam', *Asian Journal of Law and Society*, 11(4), pp. 530–558.
IMF (2023). World Economic Outlook Database - Groups and aggregates. Available at: https://www.imf.org/en/Publications/WEO/weo-database/2023/April/groups-and-aggregates (Accessed: 24 August 2025).
International Telecommunication Union (2025). Measuring digital development The ICT Development Index 2025. Available at: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICT_MDD-2025-1-PDF-E.pdf (Accessed: 16 June 2026).
Kelsey, J. (2018). 'How a TPP-style e-commerce outcome in the WTO would endanger the development dimension of the GATS acquis (and potentially the WTO)', *Journal of International Economic Law*, 21(2), pp. 273–295.
Mishra, N. (2024). *International trade law and global data governance: Aligning perspectives and practices*. Oxford: Hart Publishing.
Mitchell, A. and Mishra, N. (2020). 'Data at the docks: Modernizing international trade law for the digital economy', *Vanderbilt Journal of Entertainment & Technology Law*, 20(4), pp. 1073–1134.
Mitchell, A. D. (2023). 'The right to regulate and the interpretation of the WTO Agreement', *Journal of International Economic Law*, 26(3), pp. 462–482.
Mitchell, A. D. and 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), pp. 389–416.
Mitchell, A. D. and Mishra, N. (2021). 'WTO law and cross-border data flows: An unfinished agenda', in Burri, M. (ed) *Big data and global trade law*. Cambridge: Cambridge University Press, pp. 83–112.
Murthy, K. V. B., Kalsie, A. and Shankar, R. (2021). 'Digital economy in a global perspective: Is there a digital divide?', *Transnational Corporations Review*, 13(1), pp. 1–15.
Ni, K.-J. (2024). 'Can the CPTPP's digital format on data flows serve a role model for the WTO', *Journal of World Trade*, 58(6), pp. 989–1006.
OECD (2023). *The nature, evolution and potential implications of data localization measures*. Paris: OECD Publishing.
OECD (2026). Cross-border data flows. Available at: https://www.oecd.org/en/topics/cross-border-data-flows.html (Accessed: 23 May 2026).
OECD and WTO (2025). *Economic implications of data regulation: Balancing openness and trust*. Paris: OECD Publishing.
Peng, S. (2022). 'Digital trade', in Bethlehem, D., McRae, D., Neufeld, R. and Van Damme, I. (eds) *The Oxford handbook of international trade law*, 2nd edn. Oxford: Oxford University Press, pp. 771-C29.P48.
Polanco, R. (2021). 'Regulatory convergence of data dules in Latin America', in Burri, M. (ed) *Big data and global trade law*. Cambridge: Cambridge University Press, pp. 268–300.
Polanco, R. (2025). 'Latin America and the regulation of internet and digital trade', in Chehtman, A., Huneeus, A. and Puig, S. (eds) *Latin American international law in the twenty-first century*, 1st edn. New York, NY: Oxford University Press, pp. 613–638.
Potluri, S. R., Sridhar, V. and Rao, S. (2020). 'Effects of data localization on digital trade: An agent-based modeling approach', *Telecommunications Policy*, 44(9), article no. 102022.
Prasetyoningsih, N., Ismail Nawang, N., Putri, W. V. and Amirullah, M. N. R. (2024). 'Legal protection for the personal data in Indonesia and Malaysia', in Moallem, A. (ed) *HCI for cybersecurity, privacy and trust. Lecture Notes in Computer Science*. Cham: Springer Nature Switzerland, pp. 161–169.
Prazeres, T.L. (2020). 'Trade and national security: Rising risks for the WTO', *World Trade Review*, 19(1), pp. 137–148.
Selby, J. (2017). 'Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both?' *International Journal of Law and Information Technology*, 25(3), pp. 213–232.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057

Tania, S., Atkins, M., Cunningham, R. and Anawaratna, A. (2024). 'Reimagining the special and differential treatment provisions in the WTO's dispute settlement understanding', *Asian Journal of International Law*, 14(1), pp. 123–153.

Tee, K.L. (2002). 'Towards a personal data protection regime in Malaysia', *Journal of Malaysian and Comparative Law*, 29, pp. 255–282.

The World Bank (2026). How does the World Bank classify countries? – World Bank Data Help Desk. Available at: https://datahelpdesk.worldbank.org/knowledgebase/articles/378834-how-does-the-world-bank-classify-countries (Accessed: 24 August 2025).

Titi, C. (2014). *The Right to regulate in international investment law*. Baden: Bloomsbury Publishing.

Van den Bossche, P. and Zdouc, W. (2021). *The law and policy of the World Trade Organization: Text, cases, and materials*. Cambridge: Cambridge University Press.

van der Marel, E. (2022). 'Data-related restrictions and digital services trade: Comparing Asia with the rest of the world', in Kang, J. W., Helble, M., Avendano, R., Crivelli, P. and Tayag, M. C. (eds) *Unlocking the potential of digital services trade in Asia and the Pacific*. Manila: Asian Development Bank, pp. 98–127.

Vásquez Callo-Müller, M. and Kugler, K. (2023). 'Digital trade, development, and inequality', *AJIL Unbound*, 117, pp. 116–121.

Vásquez Callo-Müller, M. and Sucker, F. (2026). 'Evolving approaches to cross-border data flows: Latin American and African perspectives', *International Data Privacy Law*, 16(2), article no. ipaf037.

VCCI (2021). Implementing the CPTPP from a law-making perspective: Review of current results and policy implications for the future. Available at: https://wtocenter.vn/an-pham/18499-research-report-implementing-the-cptpp-from-a-law-making-perspective–review-of-current-results-and-policy-implications-for-the-future (Accessed: 10 January 2026).

Wolfe, R. (2019). 'Learning about digital trade: Privacy and e-commerce in CETA and TPP', *World Trade Review*, 18(S1), pp. S63–S84.

World Trade Organization (2023). Digital trade for development. Geneva.

World Trade Organization (2026a). Special and differential treatment provisions. Available at: https://www.wto.org/english/tratop_e/devel_e/dev_special_differential_provisions_e.htm (Accessed: 25 August 2025).

World Trade Organization (2026b). Who are the developing countries in the WTO? Available at: https://www.wto.org/english/tratop_e/devel_e/d1who_e.htm (Accessed: 24 August 2025).

Yusoff, Z. M. (2011). 'The Malaysian personal data protection act 2010: A legislation note', *New Zealand Journal of Public and International Law*, 9(1), pp. 119–136.

Zhai, D. (2025). 'RCEP rules on cross-border data flows: Asian characteristics and implications for developing countries', *Asia Pacific Law Review*, 33(1), pp. 24–45.

Zhao, Z. (2024). 'The dilemma of cross-border data flow and the construction of mutual trust platform in Asia', *Asian Journal of Law and Society*, 11(4), pp. 488–506.

Cite this article: Nguyen DA (2026). Between Digital Trade Commitments and Sovereignty: Asian Developing Members' Approaches to the CPTPP's Cross-Border Data Transfers. *Asian Journal of Law and Society*. https://doi.org/10.1017/als.2026.10057

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 19:07:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/als.2026.10057