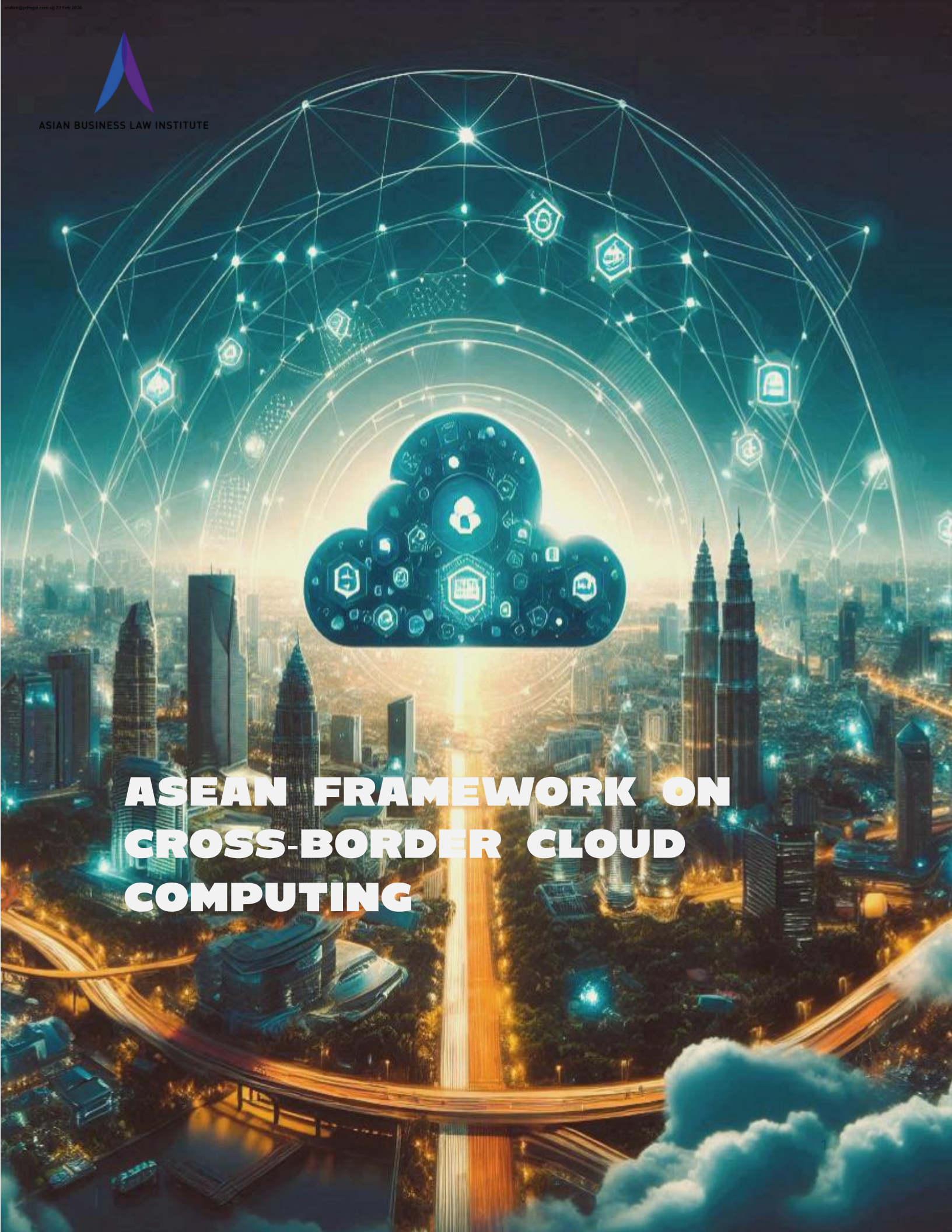
rahim@pdlegal.com.sg 23 Feb 2026

ASIAN BUSINESS LAW INSTITUTE



ASEAN FRAMEWORK ON CROSS-BORDER CLOUD COMPUTING

sraham@pulegal.com.sg 23 Feb 2026

About the Asian Business Law Institute

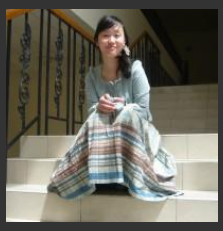
The Asian Business Law Institute is a neutral, non-profit permanent think tank based in Singapore that is dedicated to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

Editors and reviewers

Yeong Zee Kin

Chief Executive, Singapore Academy of Law

Director, Asian Business Law Institute



Catherine Shen

Senior Assistant Director
Asian Business Law Institute

Mark Fisher

Executive Director
Asian Business Law Institute

Disclaimer

Whilst every effort has been made to ensure that the information contained in this report is correct, all authors, their organisations, and the Asian Business Law Institute disclaim all liability and responsibility for any error or omission in this report, and in respect of anything, or the consequences of anything, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or any part of the contents of this report.

COPYRIGHT © 2025 Asian Business Law Institute.

srahim@pdlegal.com.sg 23 Feb 2026

Table of content

Table of content 3
Executive Summary 5
Acknowledgment 6
Summary of Principles of the Framework 7
Background and overview 10
Data, data centre and the digital economy 10
Cloud computing as a key enabler of the digital economy 10
ASEAN Framework on Cross-border Cloud Computing 12
Introduction 15
Two key pillars of legal and regulatory governance for cloud computing 15
Cross-border flow of data 15
Protection of exported data 16
Objectives of the ASEAN Cloud Computing Framework 17
Development of the ASEAN Cloud Computing Framework 18
Structure of the ASEAN Cloud Computing Framework 18
Scope of application of the ASEAN Cloud Computing Framework 19
General Principles 21
General Principle 1 23
General Principle 2 24
General Principle 3 24
General Principle 4 25
General Principle 5 27
General Principle 6 28
Trusted Data Corridor and Specific Principles 31
TDC overview 31
TDC archetypes 31
Specific Principles 32
Specific Principle 1 34
Specific Principle 2 35
Specific Principle 3 35
Specific Principle 4 37
TDC advantages 37

srahim@pdlegal.com.sg 23 Feb 2026

How to set up a TDC in ASEAN 39
Conclusion 42
References 43
Primary sources 43
Secondary sources 44
Annexure: Suggested key contents of an Agreement between AMS A and AMS B on the Establishment of a Trusted Data Corridor 46
Addendum: Application of the ASEAN Cloud Computing Framework to financial and health industries 51
Special circumstances of financial and health industries 51
Application of the ASEAN Cloud Computing Framework to financial and health industries 52
Location of computing facilities and data localisation 52
Public authority access to private sector entity data 53

srahim@pdlegal.com.sg 23 Feb 2026

Executive Summary

Cloud computing is a foundational enabler of the global economy. This is no different in the Association of Southeast Asian Nations (**ASEAN**) region. With over 420 million Internet users and a cloud market projected to grow from $21.78 billion in 2025 to $43.06 billion by 2030, ASEAN is on course to become a major player in global cloud adoption. The wide commercial availability of cloud-based solutions has allowed both the private and public sectors across ASEAN Member States (**AMS**) to leverage the cloud to drive innovation, improve productivity, and optimise operations.

As cloud usage accelerates, there is a pressing need for an interoperable governance framework to ensure the trusted and secure development of cloud in accordance with the law. This is the context in which the ASEAN Framework on Cross-border Cloud Computing (**ASEAN Cloud Computing Framework or Framework**) was conceived and developed.

The ASEAN Cloud Computing Framework targets two key pillars of legal and regulatory governance for cloud computing, i.e., cross-border data flow and protection of exported data. It begins with six **General Principles** that signal ASEAN-wide commitments to advancing cloud development and adoption in a trusted and secure manner. These include commitments to:

- provide assurances for cross-border data transfers for business purposes while limiting data localisation requirements to narrowly defined exceptions;
- develop special rules for cloud services providers where necessary; and
- enhance cross-border cooperation to reduce incidents of conflict of laws and regulatory conflicts.

To operationalise these high-level commitments, the Framework introduces a policy innovation called Trusted Data Corridor (**TDC**) where participating AMSs agree to adopt special rules within designated areas in place of their ordinary national regulations. In a TDC, data can flow freely between designated data centres as long as:

- the data protection standards of the participating AMSs are comparable to each other and in line with international standards; and
- the powers of the public authorities of the participating AMSs to access private sector entity data are aligned with international standards.

These features of a TDC are embodied in four **Specific Principles**, which are accompanied by step-by-step guidance on implementation, such as guidance on conducting a mapping exercise by AMSs to benchmark their applicable laws and regulations against neutral international and/or regional principles, standards and practices.

This tiering structure is an innovation by the Framework in recognition of the diverse national conditions of AMSs and is aimed at encouraging adoption by AMSs. An accompanying Addendum explores how the Framework can be applied to finance and health, two critical regulated industries where requirements on data protection and storage are particularly stringent.

By promoting trust, interoperability, and legal and regulatory clarity, the ASEAN Cloud Computing Framework lays the foundation for trusted and secure cloud adoption that benefits both citizens and businesses across ASEAN.

Asian Business Law Institute

25 September 2025

srahim@pdlegal.com.sg 23 Feb 2026

Acknowledgment

For valuable comments and insightful discussions throughout the project on ASEAN Cloud Computing Framework, the Asian Business Law Institute (**ABLI**) would like to record its gratitude to:[1]

- Jason Bay, Director (COO's Office), Sea Limited
- Papon Charoenpao (Managing Partner), Worawit Nitiborrirak (Senior Associate) and Lester Kuo (Associate) of PDLegal Asia (Thailand) Co., Ltd.
- Anastasia Su-Anne Chen, Director, Drew & Napier LLC
- Chester Chua, Head of APAC AI & Cybersecurity Policy, Google Cloud
- JJ Disini (Managing Partner), Ofelia Leaño (Special Counsel) and Paula Filart (Senior Associate), Disini Buted Disini Law Office
- Gerard Quek (Deputy Managing Partner), Mato Kotwani (Partner) and Elizabeth Wong (Associate), PDLegal LLC
- Yolande Goh, SVP, Global Regulatory, Public Policy, Privacy & Compliance, Equinix
- Derek Ho, Deputy Chief Privacy, AI & Data Responsibility Officer, Mastercard
- Danny Kobrata (Partner and Head of Corporate and Technology Practice Group), Talitha Vania Sahaly (Associate), Gilang Sephia Alfarisi (Junior Associate), and Muhammad Gibransyah Kusumahwardhana (Paralegal), K&K Advocates
- Pattaravadee Kongcharoenniwat, Bunnasomboon Chaiparinya (Aaron) and Krittin Pollagan, Partners, JTJB International Lawyers
- Lam Chung Nian, Partner, WongPartnership LLP
- Jeth Lee (Regional Director, Legal, Asia-Pacific), Microsoft
- Sunil Nambiar, Head of Operations for Group Strategy, Sustainability and Communications, YCH Group
- Bryan Tan (then Partner, Reed Smith)
- Jeremy Tan (Partner), Elaina Foo (Senior Associate) and Florence Seow (Associate), Bird & Bird ATMD LLP
- Thai Gia Han (Senior Associate & Head of IP & TMT Practice Group), Tran Tu Xuan (Legal Assistant), and Nguyen Trung Nghia (Legal Assistant), Indochine Counsel
- Alex Toh, Partner, Magellan Law LLP
- Tong Lai Ling (Partner), Raja, Darryl & Loh
- Penny Wong Sook Kuan (Partner), Rahmat Lim & Partners
- Dr Yap Kwong Weng, CEO of Vietnam SuperPort™ and Head of Group Strategy, Sustainability & Communications, YCH Group
- Yu Ken Li, Group Data Protection Officer, Advance Intelligence Group

ABLI also expresses its gratitude to the Asia Internet Coalition for engaging its members in discussions on data and digital economy matters of interest.

[1] In alphabetical order of surname. The Asian Business Law Institute similarly extends its gratitude to many others who have provided feedback but prefer to remain anonymous.

srahim@pdlegal.com.sg 23 Feb 2026

Summary of Principles of the Framework

Recognising the vital role of cloud computing in maintaining dynamism and enhancing competitiveness in the digital economy, the economic and social benefits of personal data protection in the digital economy, and the importance of such protection in enhancing confidence in the digital economy;

Further recognising the need to facilitate cross-border data flows to achieve greater adoption of cloud computing in ASEAN and expand cooperation among ASEAN Member States in the digital economy; and

Acknowledging the borderless nature of cloud computing, the role of cloud services providers in providing cloud computing services, and the unique operational circumstances faced by those providers;

ASEAN Member States agree to promote the adoption of, and the adherence to, the following General Principles and Specific Principles:

General Principle 1

ASEAN Member States affirm their commitment to fostering an environment that supports the trusted and secure deployment and use of cloud computing by public and private sectors.

General Principle 2

ASEAN Member States affirm that the provision and regulation of cloud computing in general, and the use of data, including personal data, in cloud computing in particular, must be in accordance with the law.

General Principle 3

ASEAN Member States commit to further facilitating cross-border data flows in ASEAN in a manner that, among others, is aligned with relevant international and regional principles, guidelines and standards, including but not limited to the principles stated in the ASEAN Framework on Personal Data Protection adopted at Bandar Seri Begawan, Brunei Darussalam on 25 November 2016, the ASEAN Framework on Digital Data Governance adopted at Bali, Indonesia on 6 December 2018 and the ASEAN Data Management Framework endorsed in January 2021.

General Principle 4

ASEAN Member States agree that none shall impose any measure to require the use or location of computing facilities onshore as a condition for conducting business in their respective territory, unless such a measure is adopted to achieve a legitimate public policy objective, provided that the measure

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

srahim@pdlegal.com.sg 23 Feb 2026

General Principle 5

ASEAN Member States agree that where appropriate, special rules may be developed to provide greater legal clarity and regulatory coherence for cloud computing and cloud services providers.

General Principle 6

ASEAN Member States agree to promote cooperation between and among each other to reduce regulatory conflicts in cloud computing, such as where data, including personal data, are held in or accessed from multiple ASEAN Member States.

In relation to the Trusted Data Corridor, the following Specific Principles apply.

Specific Principle 1

Subject to the assurance that participating ASEAN Member States of a Trusted Data Corridor (**TDC**) share comparable standards for the protection of personal data in the TDC, the transfer of personal data in the TDC may take place without the need for any further authorisation which may otherwise be required under the domestic legal framework of a participating ASEAN Member State.

Specific Principle 2

Participating ASEAN Member States of a TDC agree not to impose any data localisation requirement on the transfer of personal data in the TDC except under the exceptional circumstance, and subject to the safeguards, stated in General Principle 4.

Specific Principle 3

Participating ASEAN Member States of a TDC affirm that access to data held by private sector entities in the TDC shall be provided for and regulated by their respective domestic legal framework.

Such a legal framework shall be binding on the public authorities of a participating ASEAN Member State, be aligned with international principles or guidelines that operate under the rule of law, and set out the purposes, conditions, limitations and safeguards concerning access by public authorities to data held by private sector entities.

Specific Principle 4

Participating ASEAN Member States of a TDC agree that when their respective public authorities need to seek access to data held by private sector entities that are hosted in the TDC, those public authorities shall

a. seek access directly from the enterprise customers of the cloud services providers, wherever practicable; and

b. where it is impracticable for them to seek access directly from the enterprise customers of the cloud services providers, clarify the role of the cloud services providers in fulfilling such access requests, such as providing subscriber information of their enterprise customers.

srahim@pdlegal.com.sg 23 Feb 2026

Photo by Sigmund on Unsplash

BACKGROUND AND OVERVIEW

srahim@pdlegal.com.sg 23 Feb 2026

Background and overview

Data, data centre and the digital economy

Although there is no universal definition, the digital economy is widely understood to mean economic activities powered by digital technologies and characterised by online interactions, as opposed to the traditional, or brick-and-mortar, economy dominated by physical and offline touchpoints.

The digital economy plays an increasingly important role in the modern economic landscape. Citing estimates from the World Bank, the World Economic Forum said in an August 2022 report that the digital economy contributed to over 15% of global gross domestic product (**GDP**) and that it has been growing at two and a half times faster than the physical world GDP in the past decade.[2] A similar growth trajectory can be observed in Southeast Asia. The region's digital economy is on track to hit $600 billion in gross merchandise value (**GMV**) by 2030, with upside potential to reach $1 trillion GMV by 2030.[3] Profitability of the digital economy in Southeast Asia is also on the rise after earlier years of growth-focused investment.[4]

Data represent a key input factor in the digital economy. Data and their use in business scenarios are exhorted by some as a defining aspect of the digital age,[5] and recognised by others as a production factor.[6] Another data-related backbone of the digital economy is data centre. Data centres house the digital processing capabilities that host, process and transmit data to power the systems, applications and services, such as cloud computing, which are integral to essential daily activities around the globe and around the clock. Global data centre capacity is forecasted to expand by 177% by 2030, and the market is expected to reach $4 trillion by the same year.[7] Southeast Asia is quickly emerging as a major global data centre market. Members of the Association of Southeast Asian Nations (**ASEAN**) are increasingly represented on the global data centre location map, with over 350 data centres hosted across eight out of the ten ASEAN Member States (**AMSs**) as of August 2024.[8]

Cloud computing as a key enabler of the digital economy

The ever-expanding digital economy and the boom in data centre investment (both globally and in Southeast Asia) have accentuated the role of cloud computing as a key enabler of digital transformation.

Broadly speaking, cloud computing is the provision of hosted information technology (**IT**) services and resources via the Internet. Compared to on-premises computing where applications and data are run

---

2 Zia Hayat, "Digital trust: how to unleash the trillion-dollar opportunity for our global economy", *World Economic Forum*, 17 August 2022.

3 Sapna Chadha, "How Southeast Asia can become a $1 trillion digital economy", *World Economic Forum*, 12 December 2023.

4 "e-Conomy SEA 2024 report: Profitability push in Southeast Asia's digital economy delivers 2.5X profits in two years as businesses focus on monetisation", *Temasek*, 5 November 2024.

5 Corrado, C. et al. (2022), "The value of data in digital-based business models: Measurement and economic policy implications", *OECD Economics Department Working Papers*, No. 1723, OECD Publishing, Paris.

6 Liza Mark and Maisy Chang, "China's Data as a Fifth Market Production Factor – an Asset on Your Balance Sheet", *Haynes Boone*, 23 September 2024.

7 "Global data centre market is projected to reach US$4 trillion by 2030", *Knight Frank*, 13 April 2025.

8 "We take a look at Southeast Asia's rising popularity as a data centre hub", *Tech Collective*, 29 August 2024.

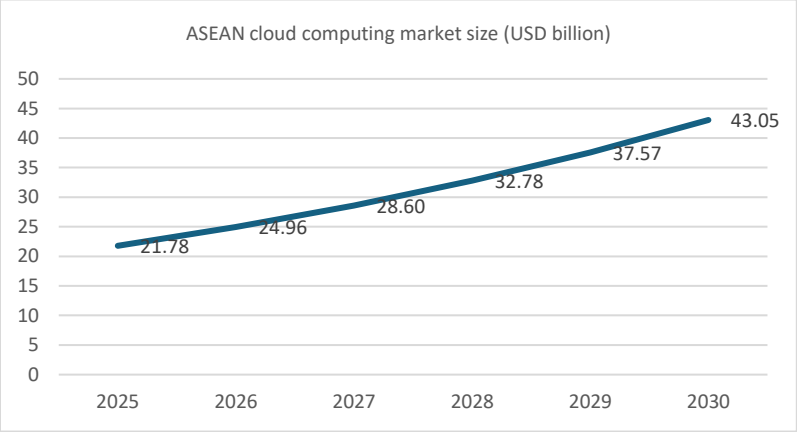
srahim@pdlegal.com.sg 23 Feb 2026

and managed on a user's own hardware and software infrastructure, cloud computing offers scalability, cost-effectiveness and accessibility. It is scalable because cloud services providers (**CSPs**) are able to adjust computing resources on demand by leveraging virtual servers in data centres in tandem with changes in service demand.[9] It is cost-effective because businesses no longer need to maintain local infrastructure such as a local server which comes with hefty upfront investment and ongoing maintenance cost.[10] It is accessible because cloud computing enables business data to be available anytime and anywhere, as long as an Internet connection is in place.

With these advantages and more, cloud computing is a key propeller behind today's global economy even as it becomes increasingly digitalised and inter-connected. This is no different in ASEAN.

Although considered relatively late in cloud adoption due to a myriad of challenges such as cost and digital infrastructure readiness,[11] ASEAN, with more than 460 million Internet users, has made significant strides in advancing cloud utilisation over recent years. Estimated at $21.78 billion in 2025, the ASEAN cloud computing market is expected to reach $43.06 billion by 2030, a compound annual growth rate of 14.6% during the forecast period.[12] In 2021, AMSs spent $5.4 billion on public cloud services,[13] a figure forecasted to grow over two-fold by 2026.[14] Cloud infrastructure revenue in ASEAN stood at $2.18 billion in 2022, a 25% increase year-on-year, with AMSs such as Indonesia, the Philippines, Thailand and Vietnam reporting growth up to 30%.[15]

Figure 1: ASEAN cloud computing market (2025 to 2030)



9 Paul Estrach, "Scalability in Cloud Computing: A Deep Dive", *MEGA*, 18 August 2023.

10 Don Hall, "Cost Savings & Benefits of Cloud Computing", *TechnologyAdvice*, last updated 18 June 2024.

11 Asyran Zarizi Bin Abdullah, Wan Isni Sofiah Wan Din, Zalili Binti Musa and Razulaimi Bin Razali, "A Review of Cloud Computing Implementation in ASEAN Countries", at The 6th International Conference on Software Engineering & Computer Systems, *IOP Publishing*.

12 "ASEAN Cloud Computing Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)", *Mordor Intelligence*, last updated 7 July 2025.

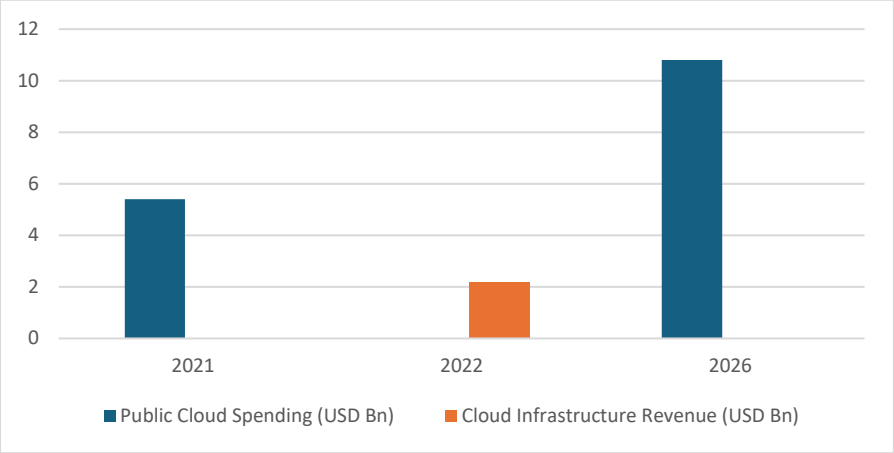
13 According to Google, a public cloud is a model where public cloud services providers, such as Google, make computing services available on demand to organisations and individuals over the public Internet. Public cloud uses shared infrastructure, which is in contrast to private cloud which uses an organisation's dedicated infrastructure. See "What is a Public Cloud", *Google*, undated.

14 "Spending on public cloud services in ASEAN countries in 2016 and 2021 with a forecast for 2026", *Statista*, 18 September 2024.

15 Kavita Panda, "Switch to cloud: ASEAN takes the lead", *ASEAN Business Partners*, undated.

srahim@pdlegal.com.sg 23 Feb 2026

Figure 2: ASEAN cloud spending and infrastructure revenue (2021 to 2026)



Further, despite in varying stages of development, AMSs are all experiencing a surge in implementation of digital solutions thanks to their rapidly modernising digital infrastructure and a burgeoning middle class that is becoming more technologically adept. Cloud computing plays a pivotal role in this process by driving innovation, enhancing competitiveness, and enabling the digital transformation of key industries, benefiting both public and private sectors. It is therefore not surprising that the importance of developing a common framework or a set of common principles for cloud computing is never lost on policymakers in the region. The ASEAN ICT Master Plan 2020 aims to, among others, "promote cloud utilisation in public and private sectors" and "develop best practice guide for information and network security in ASEAN, including cloud computing".[16] The ASEAN Digital Master Plan 2025, among others, calls for the publication of a policy or regulatory framework on "cloud data" in ASEAN, such as rules on personal data protection, privacy and access.[17]

ASEAN Framework on Cross-border Cloud Computing

The above macro-economic background sets the scene for the conception and development of the ASEAN Framework on Cross-border Cloud Computing (**ASEAN Cloud Computing Framework, or Framework**).

Over the years, policymakers in ASEAN have exerted considerable efforts to implement and advance data governance.

In November 2016, the ASEAN Framework of Personal Data Protection which includes seven ASEAN Principles of Personal Data Protection was endorsed at the then ASEAN Telecommunications and Information Technology Ministers Meeting, laying the foundation for subsequent data governance efforts in the region. Developed in alignment with the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the *APEC Privacy Framework* (2015),[18] the ASEAN Principles of Personal Data Protection include, among others, principles on putting in place security

16 The ASEAN ICT Master Plan 2020, *ASEAN Secretariat*, 2021.

17 ASEAN Digital Master Plan 2025 (adopted at the 1st ASEAN Digital Ministers Meeting (**ADGMIN**) on 21 to 22 January 2021), p 74.

18 See Guidance for Use of ASEAN Model Contractual Clauses for Cross-border Data Flows in Singapore (Personal Data Protection Commission of Singapore, 22 January 2021), fn 2.

srahim@pdlegal.com.sg 23 Feb 2026

safeguards to appropriately protect personal data[19] and on cross-border transfer of personal data only with consent or the assurance of consistent protection.[20] This was followed by the ASEAN Framework on Digital Data Governance adopted in December 2018 which provides a set of guiding principles aimed at harmonising data governance across ASEAN in support of the digital economy by focusing on four core strategic priorities.[21] In 2021, the ASEAN Data Management Framework, endorsed by the 1st ASEAN Digital Senior Officials' Meeting, takes the 2016 ASEAN Framework of Personal Data Protection further by, among others, referring to international technical standards such as those developed by the International Standards Organization as guidance that organisations may rely on to assess how their data, whether on-prem and on cloud, should be managed throughout the data life cycle.

Developed on the basis of the prior ASEAN frameworks mentioned above, the ASEAN Cloud Computing Framework represents a coherent progression of ASEAN's data governance efforts and is a timely value-accretive addition to the policy and regulatory guidance toolkit that AMSs and businesses operating in ASEAN can refer to in light of accelerating cloud adoption.

One unique feature of the ASEAN Cloud Computing Framework is its tiered structure. Taking into account circumstances unique to cloud computing and CSPs, it contains six high-level principles for general application (**General Principles**), four specific principles developed under a policy innovation called Trusted Data Corridor to operationalise the General Principles (**Specific Principles**), and an addendum focusing on two key regulated industries, finance and health.

With this tiering innovation, the ASEAN Cloud Computing Framework not only espouses general tenets but also provides actionable signposts for AMSs to implement the General Principles so that AMSs can make the most effective use of the Framework to promote trusted and secure adoption of cloud computing on an even larger scale. A continuation of the data governance work ASEAN has carried out over the years, the Framework aims to empower AMSs to make better use of cloud computing to drive innovation, enhance competitiveness, and enable further digital transformation in the region for public good.

---

19 ASEAN Framework on Personal Data Protection (adopted at Bandar Seri Begawan, Brunei Darussalam, on 25 November 2016), Art 6(d).

20 ASEAN Framework on Personal Data Protection (adopted at Bandar Seri Begawan, Brunei Darussalam, on 25 November 2016), Art 6(f).

21 ASEAN Framework on Digital Data Governance (adopted at Bali, Indonesia, on 6 December 2018 November 2016).

Photo by Ales Nesetril on Unsplash

INTRODUCTION

srahim@pdlegal.com.sg 23 Feb 2026

Introduction

Two key pillars of legal and regulatory governance for cloud computing

It is trite that the delivery and use of cloud computing involves the storage and processing of vast volumes of data, including personal data. Cloud computing centralises and manages numerous applications that rely on data to function, from e-commerce applications which provide a seamless online shopping experience for consumers worldwide to customer relationship management applications commonly used by corporations. Cloud computing also boasts advanced processing capabilities such as pattern analytics which are often employed to process and analyse data to enhance product functionality and improve user experience.

From a legal and regulatory governance standpoint, cross-border flow of data and protection of exported data are the two aspects that can be said to have the most relevance to cloud computing and CSPs. Why is this so?

By way of background, behind every cloud service lies a data centre which hosts the physical infrastructure for the entire cloud operation. To deliver cloud services, a CSP usually organises its cloud infrastructure into different geographical regions where it operates multiple data centres. Such a geographical region is known as a "cloud region". Examples of cloud regions include East United States, West Europe, Asia Pacific, etc. One cloud region may contain multiple cloud "availability zones" (**AZ**). A cloud AZ is a logical grouping of physical data centres that are located nearby (which may be in different countries) in a particular cloud region. In other words, a cloud AZ may sometimes cross geographical boundaries and encompass multiple jurisdictions, and cloud services provided by one CSP out of a single cloud AZ are often hosted out of two or more data centres situated in different jurisdictions.[22]

Simply put, a CSP's cloud infrastructure layout is inherently cross-border. A single cloud AZ may be hosted out of data centres located in different jurisdictions, and cloud services may be provided out of cloud AZs that are not located in their users' jurisdictions.

Cross-border flow of data

A borderless infrastructure layout demands data to flow into every corner of the infrastructure. A case in point for ASEAN is the outsourcing industry. Some AMSs, such as Malaysia[23] and the Philippines,[24] are major global players in business process outsourcing and IT outsourcing, while others, such as Vietnam,[25] are emerging as preferred outsourcing destinations. Millions of jobs have been created across ASEAN by the outsourcing industry, especially in IT, customer service, and back-

---

22 For more detailed explanations of cloud region and cloud availability zone (**AZ**), and other technical aspects of cloud services delivery, see *Establishing a Trusted Data Corridor in ASEAN* (Asian Business Law Institute, December 2024).

23 For example, revenue of Malaysia's business process outsourcing (**BPO**) market is projected to reach $1.56 billion in 2025 and to grow annually at 5.8% from 2025 to 2029. See "Business Process Outsourcing – Malaysia", *Statista*, undated.

24 According to the IT and Business Process Association of the Philippines, the Philippine BPO industry recorded revenue of $38 billion in 2024, up 7% on a year-on-year basis, with IT, finance, payroll and customer service being the top four most outsourced services. See Frances Alyssa Briñas, "The State of Outsourcing in the Philippines: Key Statistics for 2025", *KDCI*, 7 March 2025.

25 Vietnam's outsourcing market is projected to reach almost $698 million in 2025. With annual growth of 16.38%, the country could generate $880 million from outsourcing by 2028. See "IT outsourcing fetches nearly US$700 million", *Viet Nam News*, 3 January 2025.

srahim@pdlegal.com.sg 23 Feb 2026

office processing. ASEAN is also an attractive destination for multinational corporations (**MNCs**) to set up regional hubs thanks to factors such as an expanding economy[26] and cost-effective operations.

The outsourcing industry is intrinsically linked with cross-border data flow. Outsourcing relies heavily on the continuous exchange of data between an outsourcing service provider and its clients who are often located in places different from the service provider. For illustration, a call centre located in one AMS needs real-time access to the customer databases of a client in order to support the client's customers who are not just in that AMS but also in other AMSs and beyond. Further, many MNCs centralise certain functions, primarily back-office operations such as IT, in outsourcing hubs in ASEAN, and those operations require the transfer of back-office data such as financial or human resource data to function. Increasingly, such outsourcing arrangements also tend to employ a centralised system which may sometimes be located in a third jurisdiction. For example, an MNC, which has its regional headquarters in one AMS, may utilise an outsourced call centre in another AMS and subscribe to a cloud-based customer relationship management SaaS, or software as a service, solution hosted out of yet another AMS. In these circumstances, cross-border data flow makes it possible for MNCs to consolidate and manage global operations from a single "port of call" while ensuring that information can be accessed seamlessly across different jurisdictions.

Conversely, if cross-border data flow is restricted by requirements that mandate local storage of data (e.g., financial data) or the use of local computing facilities, an MNC using a global CSP for back-office operations will be confronted with fragmented operations (i.e., some data can flow across borders but others cannot) or risk being non-compliant if the flow of those "restricted" data is not limited to local servers.

Protection of exported data

As mentioned above, cloud services provided by one CSP out of a single cloud AZ are often hosted out of two or more data centres situated in different but nearby jurisdictions. This architecture is mainly designed for benefits such as scalability, reduced latency, redundancy and failover.[27]

When a CSP transfers the data of one enterprise customer from that customer's home country (e.g., a data centre in country A) to another country (e.g., a data centre in country B) in the same cloud AZ for storage and/or processing, those data become "exported data" from the perspectives of country A and the customer, i.e., data exported from country A to country B. The presence of those same data in the data centre in country B creates a legal connection that is hitherto non-existent between the "exported data" and country B. This territory-based nexus makes it possible for public authorities in country B to access those data more easily than they otherwise would be able to had the data remained in the data centre in country A. This is because country B's public authorities can now rely on, among others, their own laws (i.e., laws of country B) to obtain access rather than on the legal, judicial or other official arrangements with country A.

This jurisdictional "hook" creates a dilemma for CSPs. Continuing with the example above, when a CSP receives a request from a public authority in country B for access to the "exported data", given

---

26 Currently the world's fifth largest economy, ASEAN is projected to become the world's fourth-largest economy by 2030. See "The Structure of ASEAN Economy", *ASEAN Statistical Brief Volume IV*, ASEANstats, January 2024.

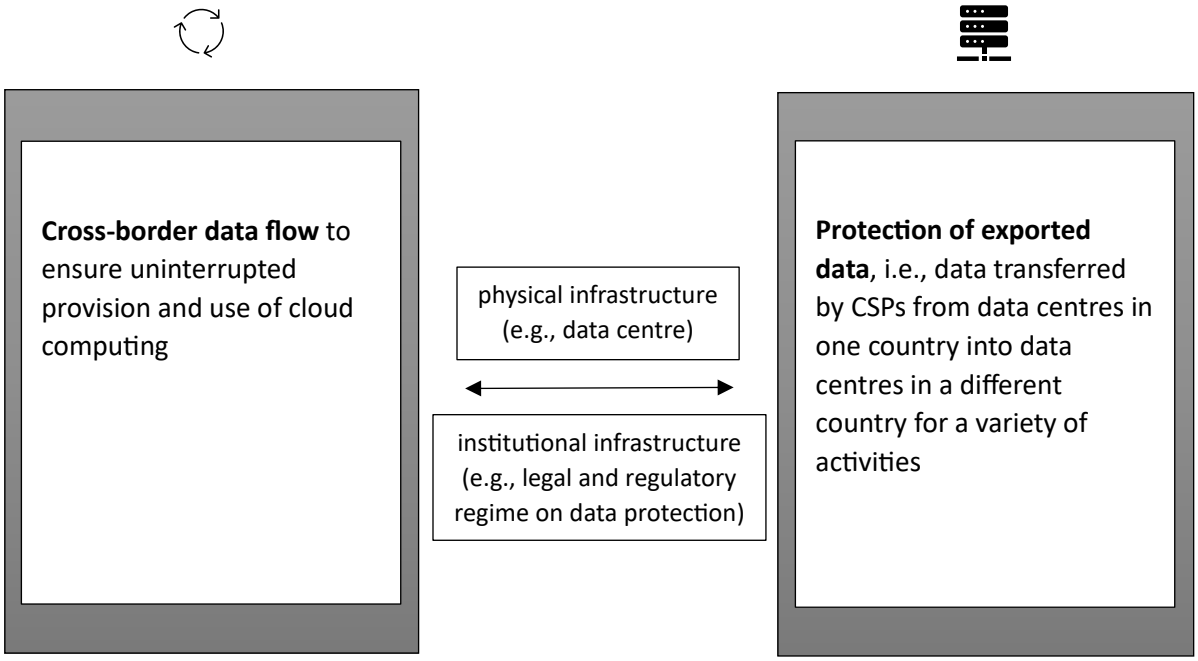
27 For example, Microsoft Azure calls this "distributed data centre architecture" where IT and data storage services can be provided among a network of physically dispersed data centres. See Datacentre architecture and infrastructure, *Microsoft*, 8 May 2024. See also Mark Freeman, "Distributed Data Centre Architecture: Ensuring Scalability", *Gable*, 5 March 2024.

srahim@pdlegal.com.sg 23 Feb 2026

the difference between the laws of country A and those of country B, the CSP may have to confront a situation where compliance with the access request will result in it violating the laws of country A while non-compliance will result in it violating the laws of country B. The fact that most of the time CSPs are not owners of the data for which access is requested for further complicates the picture as they also need to manage their relationship with enterprise customers who are owners of the data requested for.

Such conflict of laws issues have become more pressing for ASEAN as the bloc quickly asserts itself as a global data centre hot spot[28] and more data centres located in ASEAN are "drafted" into the service architecture of global CSPs. Given the potential legal and reputational risks at stake, players in the cloud ecosystem tend to closely scrutinize the protection afforded to exported data in prospective markets before making any investment, business or operational decision. It is no exaggeration to say that the level of protection given to such data has a direct impact on the perception of trust in a country's cloud and digital infrastructure. In fact, the ASEAN Digital Master Plan 2025 lists the development of "access rules" as one important initiative.[29]

Figure 3: Two key pillars of legal and regulatory governance for cloud computing



Objectives of the ASEAN Cloud Computing Framework

The ASEAN Cloud Computing Framework is directed at these two key pillars of legal and regulatory governance for cloud computing. Through General Principles and Specific Principles, it is designed to further facilitate cross-border flows of data, including personal data, across ASEAN, and ensure protection of exported data by balancing the legitimate needs of public authorities to access private

---

28 Kang Wan Chern, "South-east Asia emerges as global data centre hot spot as AI usage rises", *The Straits Times*, 14 October 2024. See also "Harnessing ASEAN's Data Center Boom: Opportunities for Operators, Investors & Tech Providers", *ARC Group*, 21 March 2025.

29 ASEAN Digital Master Plan 2025 (adopted at the 1st ADGMIN on 21 to 22 January 2021), p 74.

srahim@pdlegal.com.sg 23 Feb 2026

sector entity data and the assurance and clarity desired by CSPs and other private sector entities that such access adheres to international and/or regional standards, norms and practices.

Accordingly, the ASEAN Cloud Computing Framework serves the following objectives:

- assisting ASEAN policymakers to attract increased inflows of cloud investment by further enhancing trust in the region's cloud ecosystem through an enabling and facilitative institutional infrastructure that is aligned with well-accepted principles, guidelines, standards and practices;
- encouraging private sector entities to make greater use of cloud computing by providing guarantees of cross-border data flow and assurances of safeguards in relation to data transferred from one AMS to another AMS for storage, processing and other activities; and
- enabling businesses and individuals alike to participate in ASEAN's growing digital economy with greater confidence by consistently demonstrating strong commitment to data protection notwithstanding rapid technological advancement.

Development of the ASEAN Cloud Computing Framework

The ASEAN Cloud Computing Framework is developed based on a comprehensive landscape study conducted among AMSs in relation to the protection of exported data in cloud services delivery. That study culminated in two outputs:

(a) a 94-page compendium where the legal framework of each AMS on public authority access to private sector entity data is examined;[30] and

(b) a policy proposal called Trusted Data Corridor whose key features are summarised in subsequent sections here.[31]

Two facilitated virtual workshops were conducted in August 2025 with a diverse range of representatives from AMSs to validate findings and discuss recommendations.[32]

Further, as mentioned above, the ASEAN Cloud Computing Framework draws upon previous ASEAN work in data governance, such as the ASEAN Framework on Personal Data Protection, the ASEAN Framework on Digital Data Governance, and the ASEAN Data Management Framework.

Structure of the ASEAN Cloud Computing Framework

The ASEAN Cloud Computing Framework adopts a tiered structure, taking into account circumstances unique to cloud computing and CSPs.

---

30 Landscape Study of ASEAN Framework on Cross-border Cloud Computing (Asian Business Law Institute, March 2025).

31 Establishing a Trusted Data Corridor in ASEAN (Asian Business Law Institute, December 2024).

32 The first workshop was held on 4 August 2025 to validate findings and recommendations of the landscape study. The workshop lasted close to two hours, and drew attendance from representatives of the ASEAN Secretariat, representatives from ASEAN Member States Brunei, Indonesia, Laos, Malaysia and Singapore, as well as representatives of ASEAN's dialogue partner the United States. The second workshop was held on 22 August 2025 to apprise attendees of the proposed principles. The workshop similarly lasted close to two hours, and was attended by representatives of the ASEAN Secretariat, representatives from ASEAN Member States Brunei, Cambodia, Indonesia, Laos, Myanmar, Malaysia, the Philippines and Singapore, representatives of ASEAN's dialogue partner India and the United States, as well as representatives from Timor Leste.

srahim@pdlegal.com.sg 23 Feb 2026

It starts with six ASEAN-level General Principles which advocate for high-level government commitment and support for further development of cloud computing in ASEAN in a secure and trusted manner. Thereafter, it introduces a policy innovation called Trusted Data Corridor as a concrete use case to illustrate how the General Principles can be put into action. The Trusted Data Corridor innovation is accompanied by four Specific Principles to operationalise the corresponding General Principles.

All the principles proposed in this Framework are preceded by a chapeau that underpins common appreciation among AMSs on (a) the vital role of cloud computing in maintaining dynamism and enhancing competitiveness in the digital economy, (b) the economic and social benefits of personal data protection, and the importance of such protection in enhancing confidence, in the digital economy, (c) the need to further facilitate cross-border data flows to increase cloud adoption in ASEAN and expand digital economy cooperation among AMSs, and (d) the borderless nature of cloud computing, the role of CSPs, and the unique operational circumstances faced by them.

An Addendum is appended at the end to provide AMSs with guidance on the application of the Framework to finance and health industries.

Scope of application of the ASEAN Cloud Computing Framework

The ASEAN Cloud Computing Framework provides voluntary and non-binding guidance to promote greater adoption of cloud computing in ASEAN in a trusted and secure manner. It is not intended to constitute or create obligations under domestic or international law and will not, *in itself*, give rise to any legal process or create any legally binding or enforcement obligations.

The borderless nature of cloud computing means cooperation among AMSs takes on heightened significance to address issues such as regulatory conflicts. AMSs are thus encouraged to pursue bilateral or multilateral arrangements to further strengthen collaboration in furtherance of the objectives of the Framework wherever practicable, such as by entering into separate agreements on the establishment and administration of a Trusted Data Corridor. These separate agreements may impose legally binding obligations on AMSs depending on their exact nature and form.

srahim@pdlegal.com.sg 23 Feb 2026

GENERAL PRINCIPLES

srahim@pdlegal.com.sg 23 Feb 2026

General Principles

This section of the ASEAN Cloud Computing Framework lists six General Principles for adoption at the whole-of-ASEAN level. Each directed at a specific angle, the General Principles, as a whole, serve to demonstrate ASEAN-wide consensus and commitment to further promote the adoption of cloud computing in a trusted and secure manner to ride on the wave of digital transformation, create economic and employment opportunities, and uplift living standards in the region.

In summary, the General Principles are:

General Principle 1	ASEAN Member States affirm their commitment to fostering an environment that supports the trusted and secure deployment and use of cloud computing by public and private sectors.[33]
General Principle 2	ASEAN Member States affirm that the provision and regulation of cloud computing in general, and the use of data, including personal data, in cloud computing in particular, must be in accordance with the law.
General Principle 3	ASEAN Member States commit to further facilitating cross-border data flows in ASEAN in a manner that, among others, is aligned with relevant international and regional principles, guidelines and standards, including but not limited to the principles stated in the ASEAN Framework on Personal Data Protection adopted at Bandar Seri Begawan, Brunei Darussalam on 25 November 2016, the ASEAN Framework on Digital Data Governance adopted at Bali, Indonesia on 6 December 2018 and the ASEAN Data Management Framework endorsed in January 2021.
General Principle 4	ASEAN Member States agree that none shall impose any measure to require the use or location of computing facilities onshore as a condition for conducting business in their respective territory, unless such a measure is adopted to achieve a legitimate public policy objective, provided that the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.[34]
General Principle 5	ASEAN Member States agree that where appropriate, special rules may be developed to provide greater legal clarity and regulatory coherence for cloud computing and cloud services providers.
General Principle 6	ASEAN Member States agree to promote cooperation between and among each other to reduce regulatory conflicts in cloud computing, such

33 Reference of wording is taken partially from the ASEAN ICT Masterplan 2020 (ASEAN Secretariat, 2021), p 23.

34 Reference of wording is taken partially from Digital Economy Partnership Agreement (**DEPA**) Article 4.4.

srahim@pdlegal.com.sg 23 Feb 2026

	as where data, including personal data, are held in or accessed from multiple ASEAN Member States.

Each of the six General Principles is explained in detail below.

srahim@pdlegal.com.sg 23 Feb 2026

General Principle 1

ASEAN Member States affirm their commitment to fostering an environment that supports the trusted and secure deployment and use of cloud computing by public and private sectors.

General Principle 1 is the opening principle of the Framework and sets the overall tone. It affirms commitment at the highest level from AMSs on two fronts: (a) to further the development of cloud computing across ASEAN; and (b) to ensure such development proceeds in a trusted and secure manner, so that cloud computing is developed, deployed and used for public good.

Many AMSs already have policies and guidelines in place to support the trusted and secure development of cloud computing, while others are in the process of formulating such policies and guidelines. These efforts are testament to the consensus among AMSs around the commitment enumerated in this General Principle.

Table 1: Select examples of AMS' cloud computing policies and guidelines

	AITI Strategic Plan 2020 to 2025 listing the development and implementation of a cloud policy as one enabling programme[35]
	currently drafting, among others, an "Open Data, Cloud First" policy[36]
	sector-specific cloud regulations, such as the Financial Services Authority (Otoritas Jasa Keuangan (OJK)) Regulation No. 10/POJK.05/2022 on IT-Based Collective Funding Services
	upcoming national cloud policy which is expected to focus on enhancing public service innovation and efficiency, driving economic competitiveness, ensuring data security and user trust, and promoting digital inclusivity among citizens[37]
	DICT Department Circular No. 010 issued in 2020 modifying the country's Cloud First Policy as initially prescribed in the 2017 DICT Department Circular No. 2017-002[38]
	a slew of guidelines, technical reference and standards to foster cloud service providers and promote cloud computing security and incident response[39]

35 AITI Strategic Plan 2020 to 2025 (Authority for Info-communications Technology Industry of Brunei Darussalam, undated), at p 34.

36 Rapid Sun, Cambodia Digital Transformation (Ministry of Post and Telecommunications, 16 January 2025), at p 22.

37 Danial Azhar and Rozanna Latiff, "*Malaysia plans national cloud policy, AI regulations*", *Reuters*, 1 October 2024.

38 "Amendments to Department Circular No. 2017- 002 Re: Prescribing the Philippine Government's Cloud First Policy", Department of Information and Communications Technology, 2 June 2020.

39 "Cloud Computing and Services", Infocomm Media Development Authority, last updated 23 May 2024.

srahim@pdlegal.com.sg 23 Feb 2026

	Standards for the Maintenance of Cybersecurity in Cloud Computing Systems B.E. 2566 (2023)[40] issued in September 2024 to specify cloud security governance and cloud infrastructure security and operations
	Decree No. 163/2024/ND-CP, detailing the implementation of the 2023 Telecommunications Law and clarifying, among others, the obligations of providers of cloud computing services[41]

General Principle 2

ASEAN Member States affirm that the provision and regulation of cloud computing in general, and the use of data, including personal data, in cloud computing in particular, must be in accordance with the law.

General Principle 2 affirms the importance of rule of law, including the protection of personal data, in the pursuit of AMSs to further promote and regulate cloud computing.

The rule of law undergirds efforts to increase cloud adoption in ASEAN by providing a predictable and transparent legal environment that fosters trust and encourages innovation. It encourages investment in cloud infrastructure by providing CSPs and data centre operators with clarity on legal and regulatory expectations. It allows users to use cloud computing with greater confidence, knowing that their data are protected despite those data being in constant transit across borders. An explicit commitment to rule of law among AMSs is also conducive to promoting the interoperability of standards in ASEAN as comparability is more likely to be achieved when there is baseline commonality.

General Principle 3

ASEAN Member States commit to further facilitating cross-border data flows in ASEAN in a manner that, among others, is aligned with relevant international and regional principles, guidelines and standards, including but not limited to the principles stated in the ASEAN Framework on Personal Data Protection adopted at Bandar Seri Begawan, Brunei Darussalam on 25 November 2016, the ASEAN Framework on Digital Data Governance adopted at Bali, Indonesia on 6 December 2018 and the ASEAN Data Management Framework endorsed in January 2021.

If General Principles 1 and 2 set the tone and scene for the Framework, General Principle 3 focuses on cross-border data flow, one key pillar of legal and regulatory governance for cloud computing.

Globally, jurisdictions adopt different stances towards cross-border data flows. Some are considered more permissive and allow international data flows as long as the recipient jurisdictions have data

40 "Standards for the Maintenance of Cybersecurity in Cloud Computing Systems B.E. 2566 (2023)" (National Cyber Security Committee, adopted 3 September 2024).

41 "Vietnam: New telecom decree clarifies rules on data center, cloud computing and OTT communications services", *Baker McKenzie*, 7 January 2025.

srahim@pdlegal.com.sg 23 Feb 2026

protection standards comparable to their own or have other safeguards, such as contractual clauses, in place. On the other end of the spectrum, there are jurisdictions whose rules on cross-border data transfers are considered restrictive. Jurisdictions in this category usually have regulations that require data to be localised or that transferors meet specific criteria, such as obtaining prior regulatory approval, before data can cross borders. The same disparity in stance is observed among AMSs.

Such a patchwork of rules means that in practice, data transferors often default to obtaining consent from data subjects for cross-border data transfers. In many jurisdictions, this requires transferors to put in place consent management systems so that they can maintain proper records of consent obtained and update those records over time if data subjects change the consent provided, resulting in considerable operational costs on transferors.

Differing stances among jurisdictions are not surprising because the laws of a jurisdiction are shaped by its unique social, economic, and institutional realities. Therefore, General Principle 3 does not require any AMS to make any sweeping change to its rules on cross-border data transfer. What it does is to call for high-level commitment from all AMSs to make further efforts to facilitate the flow of data across ASEAN in an appropriate manner, and that appropriate manner is shaped by relevant international and regional principles and standards such as those stated in relevant ASEAN frameworks on data protection, governance and management.

Each AMS can pursue its own mechanisms to fulfil the commitments under General Principle 3 guided by its own circumstances. The next section of this Framework puts forward the policy innovation of Trusted Data Corridor as one possible mechanism that AMSs may pursue.

General Principle 3 is also consistent with the approach that the ASEAN Digital Economy Framework Agreement (**DEFA**) currently under negotiation will take according to both the Leaders' Statement on the Development of the ASEAN Digital Economy Framework Agreement (DEFA)[42] and the Framework for Negotiating ASEAN Digital Economy Framework Agreement.[43]

General Principle 4

ASEAN Member States agree that none shall impose any measure to require the use or location of computing facilities onshore as a condition for conducting business in their respective territory, unless such a measure is adopted to achieve a legitimate public policy objective, provided that the measure

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.[44]

---

42 Leaders' Statement on the Development of the ASEAN Digital Economy Framework Agreement (DEFA) adopted at Jakarta, Indonesia on 5 September 2023.

43 Framework for Negotiating ASEAN Digital Economy Framework Agreement endorsed by the ASEAN Economic Community Council on 3 September 2023 in Jakarta, Indonesia.

44 Reference of wording is taken partially from DEPA Article 4.4.

srahim@pdlegal.com.sg 23 Feb 2026

General Principle 4 similarly aims to safeguard cross-border data flows. It is subject to General Principle 3 but goes one step further by focusing on the location of computing facilities.

The location of computing facilities is critical to the development and deployment of cloud services.

Data centres house the physical hardware and networking systems that support the operations of cloud services. Behind every instance of cloud service lies a server hosted in a data centre somewhere in the world. The infrastructure layer of a data centre is physically located in the country where the data centre is built, and includes hardware equipment such as servers, racks and other computing facilities. The physical location of a data centre creates the territory-based nexus that often determines which law applies to, and which regulators have oversight of, the data stored and processed in that data centre.

Conversely, as mentioned earlier, global CSPs deploy their data centre infrastructure in a dispersed manner to offer geographically distributed cloud services for enterprise customers worldwide. They usually pool all data centres located in a single cloud AZ and engage the logical layers[45] of those data centres to deliver cloud services. Such a dispersed cloud structure dovetails well with the transnational and scalable architecture of cloud computing, enabling CSPs to scale up and down their services based on real-time customer demand.

Mandating the establishment or use of local computing facilities is thus detrimental to cloud development and adoption both at business and national levels.

Requiring data to be stored in and processed by onshore computing facilities goes against the global service layout of CSPs, inhibiting their ability to offer scalable and flexible services on a global scale. This will disproportionately affect smaller businesses, the user group that cloud computing sets out to benefit the most as the need for these businesses to invest in proprietary physical data centre infrastructure has been reduced. With the ability to store and process data across multiple locations to ensure uptime and redundancy being one key driver behind CSPs' dispersed data centre and cloud structure, requiring the use of local computing facilities undermines this service resilience feature of cloud computing and introduces vulnerabilities to cloud users. Further, contrary to conventional thinking, mandating the establishment or use of local computing facilities may not benefit local cloud users. Local facilities may not be best-in-class or the most cost-effective. As a result, local users may lose out by being denied early access to the latest processing capabilities or by having to wait longer for the latest technology to come to their region.[46]

At the national level, the substantial investment required to construct, operate and maintain a data centre[47] means that it is often not economically viable for less developed countries to build and maintain data centres on their soil, and global CSPs are unlikely to be attracted to enter a market or make infrastructure investment in a country that mandates the use of local computing facilities due to the lack of scalability of such an arrangement.

---

45 The logical layer of a data centre concerns software and control systems that store, process, and transmit data within a data centre. It is software-driven as opposed to the infrastructure layer of a data centre which is mostly hardware-driven. For more details, see *Establishing a Trusted Data Corridor in ASEAN* (Asian Business Law Institute, December 2024).

46 Yeong Zee Kin, "Cross-Border Data Flows in the Digital Economy" [2025] SAL Prac 14, para 7.

47 The estimated cost for a 700,000-square foot, 60-megawatt data centre in Northern Virginia of the United States, the world's largest data centre market, ranges between $420 million and $770 million. See Mary Zhang, "How Much Does it Cost to Build a Data Center?", *Dgtl Infra LLC*, 5 November 2023.

srahim@pdlegal.com.sg 23 Feb 2026

For the reasons above, General Principle 4 functions to entrench free flow of data across borders as the default by prohibiting any requirement to locate or use computing facilities within a country as a condition for conducting business in that country. At the same time, General Principle 4 recognises there may be exceptional circumstances which may require calibrated forms of restriction. Regulated industries are more likely to fall under such exceptional circumstances.[48] However, any deviation from the default rule must be limited to achieving a legitimate public policy objective and must not be imposed in any manner that is arbitrary, unjustifiable or beyond what is necessary to achieve that objective. In other words, any departure from the default rule is tightly controlled so that it will not undermine the aim of General Principle 4.

The position taken by General Principle 4 is consistent with that taken by various digital economy agreements concluded globally.[49] It also serves to facilitate cross-border data flow contemplated by the upcoming DEFA based on negotiation guidelines. This ensures alignment of the ASEAN Cloud Computing Framework with relevant international and regional instruments to the greatest extent possible.

General Principle 5

ASEAN Member States agree that where appropriate, special rules may be developed to provide greater legal clarity and regulatory coherence for cloud computing and cloud services providers.

Cloud computing brings with it unique circumstances. Those circumstances in turn dictate the business and service delivery realities of CSPs.

Cloud computing is unique because instead of relying on physical hardware or on-premises infrastructure, it offers on-demand access to computing resources online which is made possible by seamless flow of data across borders. However, as mentioned earlier, national stance towards cross-border data transfers remains different, and varying forms and degrees of threats to smooth data flow can be found across the globe.[50]

The role of CSPs in the digital economy is also unique. While they manage vast amounts of data, they collect, store and process those data for their enterprise customers as intermediaries, and are, most of the time, neither the owners nor the controllers of those data. Yet by virtue of their global cloud layout and the increasing usage of their services, CSPs often become the first point-of-contact for receiving and responding to requests of public authorities to access private sector entity data, i.e., data owned by their enterprise customers. This often puts CSPs in a bind: a CSP has to facilitate such requests because failure to do so is likely to result in it violating relevant laws and being exposed to penalties; on the other hand, the CSP has no knowledge of the data requested for or is contractually

48 See Addendum for more details.

49 See for example, DEPA Article 4.4; Agreement between the United States of America and Japan Concerning Digital Trade (signed 7 October 2019) Article 11 and Article 12; Australia-Singapore Digital Economy Agreement (signed 6 August 2020) Article 24; Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership (signed 23 October 2020) Article 8.85; Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore (signed 25 February 2022) Article 8.61-G; Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore (signed 21 November 2022) Article 14.15; and, Agreement on Digital Trade between the European Union and the Republic of Singapore (signed 7 May 2025) Article 5.

50 See, for example, Yeong Zee Kin, “Cross-Border Data Flows in the Digital Economy" [2025] SAL Prac 14, para 7.

srahim@pdlegal.com.sg 23 Feb 2026

not allowed by its enterprise customers to comply with such requests (although it may have the technical means to do so).

General Principle 5 is an acknowledgement of these unique circumstances. AMSs thus agree to develop special rules tailored to the operational realities of cloud computing and CSPs under appropriate circumstances. Such special rules serve to, among others, address the uncertainties and challenges highlighted above. Importantly, General Principle 5 does not impose any positive obligation on any AMS to amend their existing legal framework. Rather, the commitment AMSs make is to accommodate the need for the development of special rules. How such special rules, if any, should be worded and their exact scope of application are to be decided by AMSs at their discretion, provided that those special rules should not be contrary to the commitments made by AMSs under General Principles 3 and 4 to facilitate cross-border data flow.

General Principle 6

ASEAN Member States agree to promote cooperation between and among each other to reduce regulatory conflicts in cloud computing, such as where data, including personal data, are held in or accessed from multiple ASEAN Member States.

The fundamental reason behind issues of regulatory conflicts arising in the context of cloud computing is two-fold. First, cloud computing requires delivery of services across borders. Second, multiple states assert jurisdiction over the same cloud computing activity and consequently the same data processed by that activity. One concerning area confronting CSPs is public authority access to private sector entity data.

As explained earlier, the transfer by a CSP of the data of an enterprise customer from that customer's home country (e.g., a data centre in country A) to another country (e.g., a data centre in country B) in the same cloud AZ for storage, processing or any other activity creates a territory-based jurisdictional "hook" for public authorities in country B to directly request for access to those data (or "exported data" from the enterprise customer's perspective) instead of having to rely on official bilateral or multilateral arrangements with country A. The difference between the laws of country A and those of country B means that the CSP may have to confront a situation where compliance with the access request from a public authority of country B will result in it violating the laws of country A while non-compliance will result in it violating the laws of country B.

But this is not the only dilemma the CSP faces in this area.

Where a public authority in country A requests to access the data that have been transferred (or "exported") to country B, if country B has laws that prohibit the disclosure of data to foreign public authorities (e.g., data localisation requirements), the CSP will face the reverse challenge that compliance with the access request will result in it violating the laws of country B while non-compliance is likely to result in it violating the laws of country A.

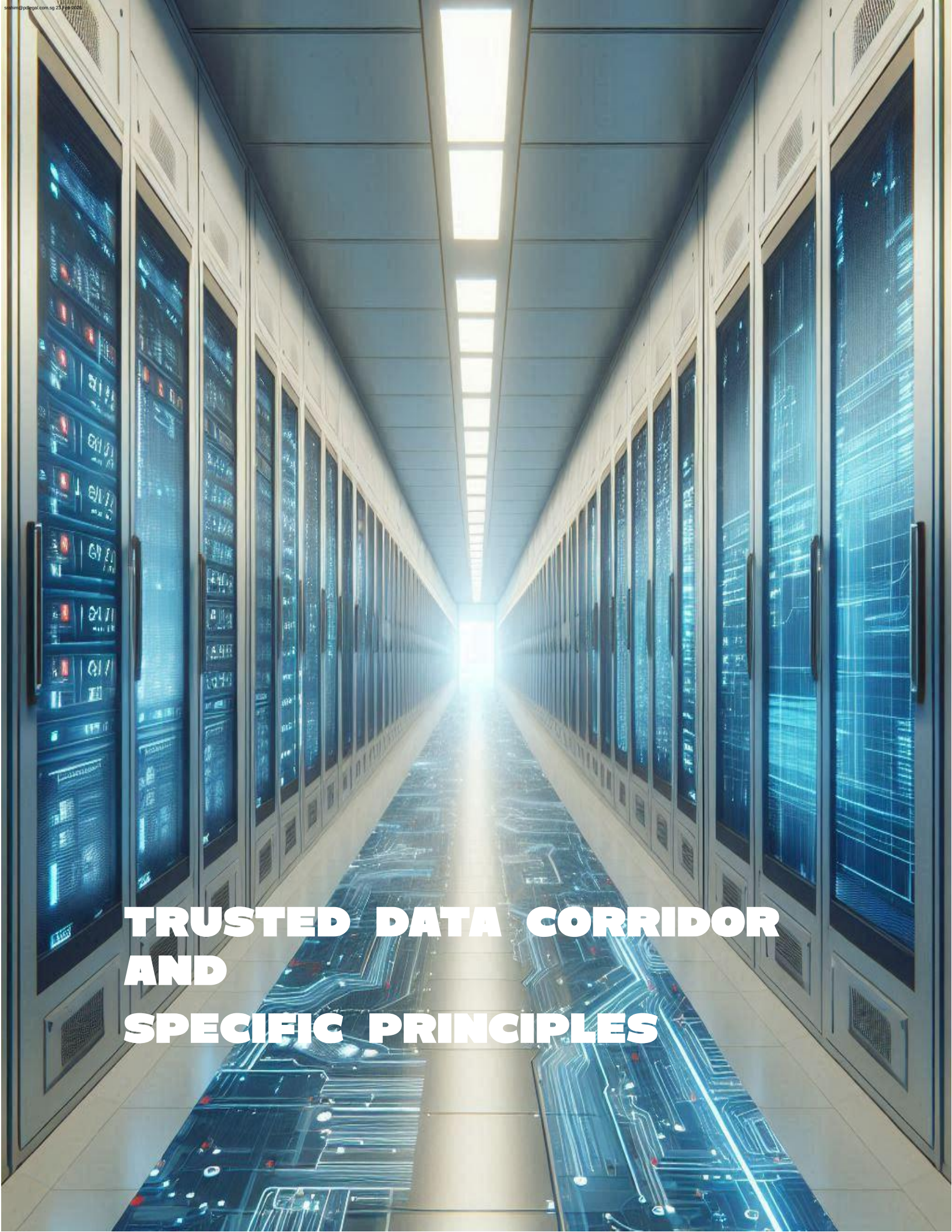
All these challenges are compounded by the fact that CSPs are, most of the time, neither the owners nor the controllers of the data for which access is requested. As those data belong to their enterprise customers, CSPs have the additional business necessity to manage customer relationships, on top of meeting regulatory and compliance requirements.

General Principle 6 demonstrates the understanding among AMSs that issues of regulatory conflicts, such as those described above, create complexities and weaken confidence in the delivery and use of

srahim@pdlegal.com.sg 23 Feb 2026

cloud computing, hindering further cloud adoption. It also demonstrates the shared commitment among AMSs to work together to reduce the occurrence of such issues. As such issues engage the legal and regulatory systems of more than one AMS, government-to-government (**G2G**) cooperation is indispensable in any serious attempt to address such issues. Lastly, General Principle 6 paves the way for AMSs to develop or pursue appropriate mechanisms to raise and resolve issues of regulatory conflicts so that a CSP's compliance with its legal obligations in one AMS will not amount to violation of the laws of another AMS. Some of those mechanisms may be comparatively easier to pursue, such as where relevant authorities of AMSs provide clearer regulatory guidance on the application of pertinent regulations.

srahim@pdlegal.com.sg 23 Feb 2026



TRUSTED DATA CORRIDOR AND SPECIFIC PRINCIPLES

srahim@pdlegal.com.sg 23 Feb 2026

Trusted Data Corridor and Specific Principles

The preceding section lists six General Principles of the ASEAN Cloud Computing Framework. They signal broad consensus among, and high-level commitment of, AMSs to further facilitate and promote the development and adoption of cloud computing while ensuring its robust governance. They lay a solid foundation for the introduction in this section a policy innovation called Trusted Data Corridor (**TDC**)[51] and four accompanying Specific Principles. The TDC is an illustration of a practical use case developed on the basis of the General Principles.

This tiering structure of the Framework aims to provide AMSs with concrete guidance on how to operationalise the General Principles, in addition to espousing top-level endorsement. It addresses the critique[52] levelled from time to time against a proliferation of principles, declarations, policy frameworks and statements for being merely "words on paper". The hope is that the TDC and the Specific Principles can catalyse AMSs into entering binding bilateral or multilateral arrangements to give teeth to this Framework.

TDC overview

A TDC is a governance structure developed under the ASEAN Cloud Computing Framework. Fundamentally, it connects data centres in two or more AMSs to support the secure, seamless and trusted flow, processing and storage of data in participating AMSs, which in turn serves to promote greater cloud adoption and digital economy growth in ASEAN.

A TDC mirrors the approach taken by well-established trade concepts such as "special economic zone" (**SEZ**) and "free trade zone" (**FTZ**). In a nutshell, a participating AMS will apply special rules instead of its ordinary national rules exclusively within a TDC to facilitate the transfer, storage and processing of data, including personal data, into, out of and within the TDC, in a similar way as a state applies special rules in a SEZ or FTZ.

As a TDC is designed to direct at the two key pillars of legal and regulatory governance for cloud computing outlined earlier, the special rules to be applied in the TDC will be those concerning cross-border flow of data and protection of exported data. In other words, the special TDC rules are most likely those on data protection, cybersecurity, etc., as opposed to rules on tax, customs clearance or inspection, etc. that are applied in a SEZ or FTZ which is designed to support the traditional economy.

TDC archetypes

The TDC structure may present itself in different archetypes in ASEAN.

It can be a bilateral TDC that

- connects a designated area in AMS A and a designated area in AMS B to support the flow of data between those two designated areas;
- connects a designated area in AMS A and the entire territory of AMS B to support the flow of data between AMS A's designated area and anywhere in AMS B; or
- connects the entire territory of AMS A and the entire territory of AMS B to support the flow of data between these two AMSs.

---

51 For more detailed discussions of the Trusted Data Corridor, see *Establishing a Trusted Data Corridor in ASEAN* (Asian Business Law Institute, December 2024).

52 Anecdotally, such critique includes vagueness, lack of practical details, difficulty in enforcing compliance, etc.

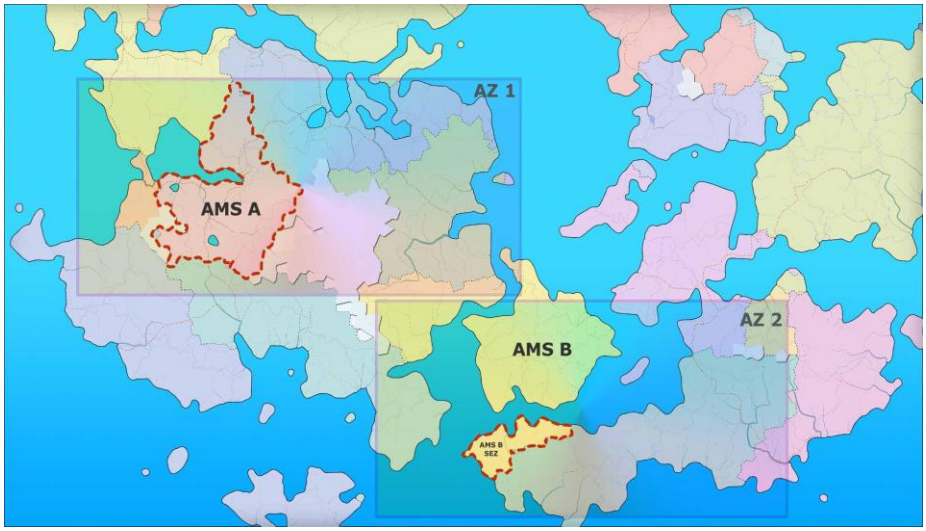
srahim@pdlegal.com.sg 23 Feb 2026

Further, a TDC can also be between more than two AMSs. This can be achieved either from the start (i.e., more than two AMSs participating in the TDC from the beginning) or over time (i.e., a bilateral TDC subsequently expanding to a multilateral one).

Each AMS decides *how* to join a TDC at its discretion, i.e., whether participation is more advantageous via a designated area (such as an existing or a new SEZ or FTZ) or for its entire territory. Since special rules need to be adopted in a TDC, it is administratively more conducive for an AMS with a larger land mass to join a TDC via a designated area. This is because modifications are always easier to make within a confined space than across the entire country, especially if the country is large or a federated state.

Likewise, each AMS has full discretion to decide *when* to join a TDC, taking into account its own development priorities and stage.

Figure 4: Illustration of a bilateral TDC in ASEAN[53]



Specific Principles

As special rules *may* need to be developed for a TDC, four Specific Principles are proposed under this Framework to provide AMSs with concrete guidance on how to develop those rules. The Specific Principles are all directed at the two key pillars of legal and regulatory governance for cloud computing.

The Specific Principles are:

Specific Principle 1	Subject to the assurance that participating ASEAN Member States of a Trusted Data Corridor (**TDC**) share comparable standards for the protection of personal data in the TDC, the transfer of personal data in the TDC may take place without the need for any further authorisation which may otherwise be required under the domestic legal framework of a participating ASEAN Member State.

53 The bilateral TDC illustrated in Figure 4 covers the entire territory of AMS A and a SEZ of AMS B. AMS A is in Cloud AZ 1 while AMS B is in Cloud AZ 2.

srahim@pdlegal.com.sg 23 Feb 2026

Specific Principle 2	Participating ASEAN Member States of a TDC agree not to impose any data localisation requirement on the transfer of personal data in the TDC except under the exceptional circumstance, and subject to the safeguards, stated in General Principle 4.
Specific Principle 3	Participating ASEAN Member States of a TDC affirm that access to data held by private sector entities in the TDC shall be provided for and regulated by their respective domestic legal framework. Such a legal framework shall be binding on the public authorities of a participating ASEAN Member State, be aligned with international principles or guidelines that operate under the rule of law, and set out the purposes, conditions, limitations and safeguards concerning access by public authorities to data held by private sector entities.[54]
Specific Principle 4	Participating ASEAN Member States of a TDC agree that when their respective public authorities need to seek access to data held by private sector entities that are hosted in the TDC, those public authorities shall a. seek access directly from the enterprise customers of the cloud services providers, wherever practicable; and b. where it is impracticable for them to seek access directly from the enterprise customers of cloud services providers, clarify the role of the cloud services providers in fulfilling such access requests, such as providing subscriber information of their enterprise customers.

Each of the four Specific Principles is explained in detail below.

54 Reference of wording is taken partially from the Declaration on Government Access to Personal Data Held by Private Sector Entities (Organisation for Economic Co-operation and Development, 14 December 2022) Article I.

srahim@pdlegal.com.sg 23 Feb 2026

Specific Principle 1

Subject to the assurance that participating ASEAN Member States of a Trusted Data Corridor (TDC) share comparable standards for the protection of personal data in the TDC, the transfer of personal data in the TDC may take place without the need for any further authorisation which may otherwise be required under the domestic legal framework of a participating ASEAN Member State.

Specific Principle 1 serves as a practical mechanism to bring into action the commitments AMSs made under General Principle 3 to further facilitate cross-border data flows in ASEAN.

As mentioned above, the stance towards cross-border data flow varies among AMSs. This legal fragmentation means data transferors have to navigate multiple sets of regulations with different standards while transferring the same set of data, making them resort to the "safe bet" of obtaining data subject consent, often at considerable operational and compliance cost.

A TDC thus aims to enable free movement of data between (designated areas of) participating AMSs by directly tackling such disparity and fragmentation. Under Specific Principle 1, data will be transferrable without restriction (i.e., without "further authorisation" in the form of transfer mechanisms such as consent) in the TDC provided that there is comparability between the standards on personal data protection of the participating AMSs for the purpose of the TDC. This is a direct response to the complexities brought about by "different standards" mentioned above. This assurance of comparability on standards reduces legal and regulatory friction and fragmentation and avoids legal and/or regulatory vacuum and arbitrage.

Specific Principle 1 also makes it clear that in developing any special TDC rules (if necessary), participating AMSs must bear in mind the goal of achieving comparability of standards in the TDC. One way for them to achieve such comparability is to adopt mutually-agreed and neutral international and/or regional principles and standards as references to map their relevant domestic laws against. Examples of such international and/or regional principles and standards include, among others, the OECD Privacy Principles developed as part of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[55] the principles enumerated in the ASEAN Framework on Personal Data Protection (**ASEAN Principles of Personal Data Protection**), the *APEC Information Privacy Principles* stated in the *APEC Privacy Framework* (2015)[56] and the Global Cross-border Privacy Rules Framework (2023).[57] In addition, these international and regional principles and standards on data protection may be supplemented by relevant global and regional standards concerning digital trade,[58] as well as technical standards[59] and governance frameworks.[60]

---

55 Adopted on 23 September 1980, and as amended on 11 July 2013.

56 Published in August 2017.

57 Endorsed for adoption by the Joint Media Statement of the 5th ADGMIN and Related Meetings at Bangkok, Thailand on 16 and 17 January 2025, para 7.

58 For example, Article 14.11 and Article 14.13 in Chapter 14 Electronic Commerce of the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* and Article 12.14 and Article 12.15 in Chapter 12 Electronic Commerce of the *Regional Comprehensive Economic Partnership.*

59 For example, the ISO 27001 series of standards on information security management.

60 For example, the ASEAN Data Management Framework (final copy endorsed by the 1st ASEAN Digital Senior Officials' Meeting in January 2021).

srahim@pdlegal.com.sg 23 Feb 2026

If after undergoing the mapping exercise described above, a participating AMS finds areas of non-alignment between its applicable laws and the principles and/or standards mapped against, the participating AMS needs to make legal modifications such that the rules it applies in the TDC (i.e., the special rules) become aligned with those principles and/or standards. If the mapping exercise shows that relevant laws of the participating AMS are already in alignment with those principles and/or standards, it may not be necessary for the participating AMS to make legal modifications in the TDC.

Once comparability of standards is achieved in the TDC, Specific Principle 1 allows for free movement of data in the TDC between (designated areas of) participating AMSs.

The process by which a participating AMS conducts the mapping exercise is also *in itself* a rule-of-law exercise under General Principles 1 and 2.

Specific Principle 2

Participating ASEAN Member States of a TDC agree not to impose any data localisation requirement on the transfer of personal data in the TDC except under the exceptional circumstance, and subject to the safeguards, stated in General Principle 4.

Specific Principle 2 reinforces Specific Principle 1 in the same way as General Principle 4 reinforces General Principle 3.

As explained earlier, seamless flow of data across borders is of critical importance to the delivery and use of cloud services, and mandating the establishment or use of local computing facilities is detrimental to cloud development and adoption both at national and business levels. Continued application by an AMS of data localisation requirements, if any, in a TDC is anathema to the concept, design and construct of the TDC structure as well as the overall ASEAN Cloud Computing Framework. As such, Specific Principle 2 commits participating AMSs of a TDC to the default position of no data localisation in the TDC. It also addresses any gap or "loophole" of comparability in standards in the TDC should participating AMSs both have data localisation requirements.

At the same time, Specific Principle 2 acknowledges the existence of exceptional circumstances which may call for a limited degree of deviation from the default position, provided that any such deviation must be subject to stringent controls. This ensures consistency between Specific Principle 2 and General Principle 4 (as well as the positions taken by most digital economy agreements) while affording participating AMSs the flexibility to make adjustments where necessary.

Specific Principle 1 and Specific Principle 2 work together to enhance the appeal of the TDC as a use case to translate the ASEAN Cloud Computing Framework into action.

Specific Principle 3

Participating ASEAN Member States of a TDC affirm that access to data held by private sector entities in the TDC shall be provided for and regulated by their respective domestic legal framework.

Such a legal framework shall be binding on the public authorities of a participating ASEAN Member State, be aligned with international principles or guidelines that operate under the rule

srahim@pdlegal.com.sg 23 Feb 2026

of law, and set out the purposes, conditions, limitations and safeguards concerning access by public authorities to data held by private sector entities.

Specific Principles 1 and 2 are directed at cross-border data flow. Specific Principles 3 and 4, on the other hand, address the other key pillar of legal and regulatory governance for cloud computing which is the protection of exported data, specifically public authority access to private sector entity data. This is also an effort to fulfil the task of developing "access rules" laid out in the ASEAN Digital Master Plan 2025.

As mentioned earlier, the level of protection granted to exported data directly influences the perception of trust CSPs and other cloud ecosystem players have in a country's cloud and digital infrastructure, impacting their investment, business and operational decisions. It is therefore of utmost importance that in a TDC, participating AMSs explicitly commit to each adopting a binding legal framework aligned with international principles or guidelines to govern public authority access to private sector entity data. This provides CSPs with clarity as to *when* the public authorities of participating AMSs of the TDC may issue requests to access private sector entity data.

Specific Principle 3 also makes the hallmarks of such a binding legal framework clear. In other words, the binding legal framework applied by a participating AMS on public authority access to private sector entity data in the TDC must be aligned with relevant international principles or guidelines and set out relevant matters concerning such access, including purposes, conditions, limitations and safeguards. Examples of such principles and guidelines include, among others, the *Declaration on Government Access to Personal Data Held by Private Sector Entities*,[61] and the Trusted Cloud Principles.[62]

To develop and apply such a binding legal framework in a TDC, a participating AMS of the TDC may again adopt the mapping approach described under Specific Principle 1 so that cloud infrastructure investors, CSPs, cloud users and other cloud ecosystem players all have the assurance that the power of the public authorities of the participating AMS to access private sector entity data in the TDC is regulated by internationally accepted standards and norms. This assurance creates familiarity, builds trust and engenders confidence.

While it is not impossible to commit AMSs to align their overall domestic legal framework governing public authority access to private sector entity data with relevant international standards and norms at the General Principle level, an attempt to this effect is only made at the Specific Principle level because study[63] has shown that the legal and regulatory frameworks adopted by AMSs to govern such access vary greatly. Having a tiered approach in the form of Specific Principle 3 is thus a more achievable target and provides AMSs with a concrete roadmap to put into action their commitments under General Principles 1 and 2.

Specific Principle 3 only outlines the contours of a robust binding legal framework on public authority access to private sector entity data, and participating AMSs of a TDC are free to negotiate and agree on more specific obligations. For example, they may agree that their respective public authorities shall seek access to data held by private sector entities in the TDC only for the purpose of fulfilling

---

61 Organisation for Economic Co-operation and Development, 14 December 2022.

62 Produced under the Trusted Cloud Initiative, a shared initiative by eight major cloud services providers (**CSP**).

63 Landscape Study of ASEAN Framework on Cross-border Cloud Computing (Asian Business Law Institute, March 2025).

srahim@pdlegal.com.sg 23 Feb 2026

specified sovereign duties and obligations (e.g., investigation of alleged criminal offenses) and in accordance with their respective rules applicable in the TDC.

Specific Principle 4

Participating ASEAN Member States of a TDC agree that when their respective public authorities need to seek access to data held by private sector entities that are hosted in the TDC, those public authorities shall

a. seek access directly from the enterprise customers of the cloud services providers, wherever practicable; and

b. where it is impracticable for them to seek access directly from the enterprise customers of the cloud services providers, clarify the role of the cloud services providers in fulfilling such access requests, such as providing subscriber information of their enterprise customers.

Specific Principle 4 is a concrete way for AMSs to implement their commitments under General Principles 5 and 6.

As explained earlier, circumstances unique to cloud computing often make it challenging for CSPs who are intermediaries to confidently comply with laws and regulations that are not developed with cloud computing in mind while protecting the rights and interests of cloud users, often resulting in conflict of laws dilemmas.

Taking such issues into account, Specific Principle 4 is designed to provide CSPs with clarity on *how* the access requests issued by public authorities of participating AMSs of a TDC are governed procedurally. For example, acknowledging the role of CSPs as intermediaries rather than as owners or controllers of customer data, Specific Principle 4 commits public authorities of participating AMSs of the TDC to seek access directly from the CSPs' enterprise customers as long as it is practicable to do so. Where doing so is not practicable, Specific Principle 4 provides for the clarification of the role of CSPs in fulfilling access requests, again taking into account that they are "custodians" rather than owners of customer data. As this default rule may differ from the rules that a participating AMS ordinarily applies in its territory outside of the TDC, the participating AMS may need to develop and apply special rules in the TDC, provided that those special rules must also meet the requirements under Specific Principle 3.

Specific Principles 3 and 4 work in tandem to reduce conflict of laws incidents in a TDC, enabling CSPs to facilitate access requests from public authorities for private sector entity data with greater confidence and clarity. They balance the need for legitimate public authority access (e.g., for investigation of alleged crimes) with the protection of data, standardise the level of protection granted to exported data at an internationally accepted level, and instil greater trust in ASEAN's cloud ecosystem.

TDC advantages

The TDC use case under this Framework has two key advantages.

First, it is jurisdictionally scalable.

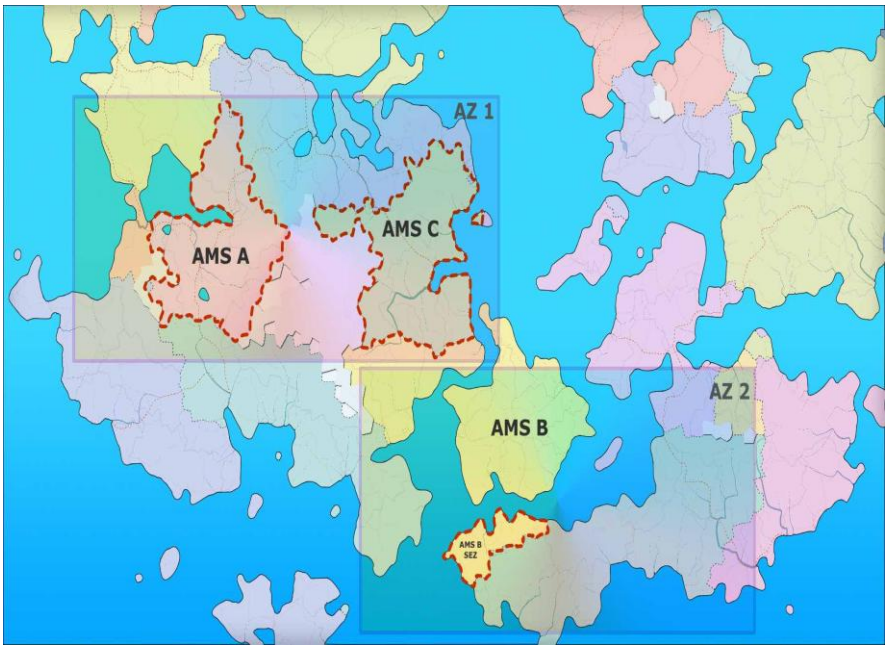
A TDC is not restricted to two participating AMSs. Instead, it is open to any AMS which commits to the standards of personal data protection practiced in the TDC. Since those standards are mapped

srahim@pdlegal.com.sg 23 Feb 2026

against agreed, neutral international and/or regional principles, guidelines and standards, an AMS interested in joining the TDC has clear signposts to follow in benchmarking its own legal and regulatory framework and in developing new rules or modifying existing ones for the TDC where necessary.

Having jurisdictional scalability is a critical feature of the TDC structure because CSPs and their enterprise customers come from all over the world; restricting a TDC to only two AMSs diminishes its marketability and utility, and is not conducive to promoting greater cloud adoption in ASEAN.

Figure 5: Illustration of a multilateral TDC in ASEAN[64]



Second, it is flexible in terms of data type.

An ASEAN TDC does not prescribe the types of data it covers. It can be utilised for personal data, the most heavily regulated data type. It can also be employed for only a specific category of data if the participating AMSs so wish. For example, participating AMSs of a TDC are free to agree that the TDC will only apply to data held by covered financial institutions, with a focus on facilitating the flow of financial data and managing public authority access requests to financial data.[65] Alternatively, participating AMSs may adopt a "negative list" approach whereby the TDC can be used for all data types other than those specifically excluded (e.g., financial data), in which case the excluded data will continue to be subject to the ordinary laws and regulations of the participating AMSs instead of their respective special rules in the TDC.

Having this data type flexibility allows participating AMSs to tailor the TDC use case to their respective economic and regulatory priorities as well as the shared objectives to maximise benefits and effectiveness.

---

64 The multilateral TDC illustrated in Figure 5 covers the entire territory of AMS A and AMS C, and a SEZ of AMS B. AMS A and AMS C share the same cloud AZ (AZ 1). AMS B is in a different cloud AZ (AZ 2).

65 Where necessary, the "legitimate public policy objective" exception provided for in General Principle 4 and Specific Principle 3 can accommodate exceptional circumstances if a TDC is utilised for a specific category of data.

srahim@pdlegal.com.sg 23 Feb 2026

How to set up a TDC in ASEAN

The TDC use case and the accompanying Specific Principles are put forward under the ASEAN Cloud Computing Framework with a view to "giving teeth" to the General Principles and to providing AMSs with an actionable roadmap to operationalise this Framework. It is therefore imperative to provide further guidance for any AMS which is interested in implementing the TDC use case.

In essence, an AMS keen to implement a TDC needs to take two key steps.

Figure 6: Actionable roadmap to implement a TDC in ASEAN

The first step is to conclude a G2G agreement. Specifically, AMSs interested in setting up a TDC between or among themselves should enter into a G2G agreement on the establishment, operation and administration of the TDC. Such an agreement needs to take a legally binding form to give the principles under this Framework the legal enforceability that is otherwise lacking in soft law instruments. This legal enforceability gives cloud investors, CSPs, cloud users and other cloud ecosystem players assurance and certainty in making investment, business and operational decisions. Through negotiation, AMSs to such a G2G agreement can detail the specific obligations to action upon the principles under this Framework so that their TDC is better tailored to the specific economic, regulatory and policy priorities of the signatory AMSs.

Although voluntary and non-binding in nature, this Framework encourages AMSs to enter into separate agreements to further strengthen collaboration as long as such agreements serve to further its objectives. In other words, this Framework empowers AMSs to negotiate and conclude separate binding G2G agreements to establish TDCs to further promote cloud adoption in ASEAN. A suggested template for such an agreement is provided in the Annexure which AMSs may use as a baseline for negotiation and customisation.

Once such a G2G agreement is in place, the second step is for signatory AMSs to ensure their respective domestic laws and regulations as applicable to the TDC give effect to the commitments they have made under the G2G agreement. This requires those AMSs to conduct the mapping exercise described above to benchmark their relevant laws and regulations against agreed, neutral international and/or regional principles, guidelines and standards,[66] and where necessary, make

66 As mentioned earlier, examples of such principles, guidelines and standards include the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the *ASEAN Principles of Personal Data Protection*, the *APEC Information Privacy Principles*, the *Global Cross-border Privacy Rules Framework*, the *Declaration on Government Access to Personal Data Held by Private Sector Entities*, the *Trusted Cloud Principles*, etc.

srahim@pdlegal.com.sg 23 Feb 2026

modifications by amending relevant existing laws and regulations and/or by passing new ones for application in the TDC.

Administratively speaking, it is more practicable for a TDC to take off with two participating AMSs in the initial phase. Any third and subsequent AMS which is interested in joining the TDC can apply to join the G2G agreement as long as it undertakes to abide by the same commitments made in that agreement by the two initial participants and achieves comparable standards of protection in the TDC through a similar mapping exercise. This is how the jurisdictional scalability feature of the TDC structure is achieved.

Photo by fabio on Unsplash

CONCLUSION

srahim@pdlegal.com.sg 23 Feb 2026

Conclusion

To encourage and support greater cloud adoption in ASEAN, the region needs huge investment[67] in infrastructure such as broadband technology and data centres as *hardware support* for CSPs to deploy and deliver, and for users to access, cloud computing services. To attract such investment, AMSs need to have in place *institutional support* to demonstrate they are jurisdictions that investors can trust their financial resources with and have the confidence to gain returns from.

Targeting cross-border data flow and protection of exported data as two key pillars of legal and regulatory governance for cloud computing, the ASEAN Cloud Computing Framework serves to assist AMSs in building out the desired institutional support in a practical and hands-on manner. It empowers AMSs to decide on the most suitable form of adoption based on their respective national circumstances through the tiering of General Principles, the TDC use case and the Specific Principles. The TDC use case also presents a clear pathway for AMSs to translate the General Principles into practice. AMSs can opt for high-level General Principles as the "North Star" to set the tone of their overall cloud development strategies before exploring the TDC use case and its Specific Principles. Alternatively, AMSs can directly pursue bilateral or multilateral cooperation on the TDC structure under this Framework.

It is hoped that the ASEAN Cloud Computing Framework provides AMSs with not only governance guidance but also a practical route in furtherance of cloud development to benefit individuals and businesses alike in ASEAN and beyond.

---

67 One study puts the investment need for the data centre sector in Asia Pacific, including ASEAN, at approximately US $116 billion in the next five to seven years. See Amy Kathleen Kelly, "Over US $100 billion needed to fund Asia Pacific data centre pipeline in the coming five to seven years", *Cushman & Wakefield*, 27 February 2025, citing the Cushman & Wakefield H2 2024 Asia Pacific Data Centre Market Update.

srahim@pdlegal.com.sg 23 Feb 2026

References

Primary sources

- APEC Privacy Framework, Asia-Pacific Economic Cooperation, 2015.
- ASEAN Data Management Framework, final copy endorsed by the 1st ASEAN Digital Senior Officials' Meeting in January 2021.
- ASEAN Digital Master Plan 2025, adopted at the 1st ASEAN Digital Ministers Meeting on 21 to 22 January 2021.
- ASEAN Framework on Digital Data Governance, adopted at Bali, Indonesia, on 6 December 2018.
- ASEAN Framework on Personal Data Protection, adopted at Bandar Seri Begawan, Brunei Darussalam, on 25 November 2016.
- The ASEAN ICT Master Plan 2020, ASEAN Secretariat, 2021.
- AITI Strategic Plan 2020 to 2025, Authority for Info-communications Technology Industry of Brunei Darussalam, undated.
- Amendments to Department Circular No. 2017- 002 Re: Prescribing the Philippine Government's Cloud First Policy, Department of Information and Communications Technology, 2 June 2020.
- Agreement between the United States of America and Japan Concerning Digital Trade (signed 7 October 2019).
- Australia-Singapore Digital Economy Agreement (signed 6 August 2020).
- Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership (signed 23 October 2020).
- Agreement on Digital Trade between the European Union and the Republic of Singapore (signed 7 May 2025).
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (signed on 8 March 2018).
- Declaration on Government Access to Personal Data Held by Private Sector Entities, Organisation for Economic Co-operation and Development, 14 December 2022.
- Digital Economy Partnership Agreement (signed 11 June 2020).
- Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore (signed 25 February 2022).
- Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore (signed 21 November 2022).
- Framework for Negotiating ASEAN Digital Economy Framework Agreement endorsed by the ASEAN Economic Community Council on 3 September 2023 in Jakarta, Indonesia.
- Guidance for Use of ASEAN Model Contractual Clauses for Cross-border Data Flows in Singapore, Personal Data Protection Commission of Singapore, 22 January 2021.

srahim@pdlegal.com.sg 23 Feb 2026

- Joint Media Statement of the 5th ADGMIN and Related Meetings at Bangkok, Thailand on 16 and 17 January 2025.
- Leaders' Statement on the Development of the ASEAN Digital Economy Framework Agreement (DEFA), adopted at Jakarta, Indonesia on 5 September 2023.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted on 23 September 1980, and as amended on 11 July 2013).
- Regional Comprehensive Economic Partnership (15 November 2020).
- Standards for the Maintenance of Cybersecurity in Cloud Computing Systems B.E. 2566 (2023), National Cyber Security Committee, adopted 3 September 2024.

Secondary sources

- Asyran Zarizi Bin Abdullah, Wan Isni Sofiah Wan Din, Zalili Binti Musa and Razulaimi Bin Razali, "A Review of Cloud Computing Implementation in ASEAN Countries", at The 6th International Conference on Software Engineering & Computer Systems, *IOP Publishing*.
- Danial Azhar and Rozanna Latiff, "*Malaysia plans national cloud policy, AI regulations*", *Reuters*, 1 October 2024.
- Frances Alyssa Briñas, "The State of Outsourcing in the Philippines: Key Statistics for 2025", *KDCI*, 7 March 2025.
- Sapna Chadha, "How Southeast Asia can become a $1 trillion digital economy", *World Economic Forum*, 12 December 2023.
- Corrado, C. et al. (2022), "The value of data in digital-based business models: Measurement and economic policy implications", *OECD Economics Department Working Papers*, No. 1723, OECD Publishing, Paris.
- Paul Estrach, "Scalability in Cloud Computing: A Deep Dive", *MEGA*, 18 August 2023.
- Mark Freeman, "Distributed Data Centre Architecture: Ensuring Scalability", *Gable*, 5 March 2024.
- Don Hall, "Cost Savings & Benefits of Cloud Computing", *TechnologyAdvice*, last updated 18 June 2024.
- Zia Hayat, "Digital trust: how to unleash the trillion-dollar opportunity for our global economy", *World Economic Forum*, 17 August 2022.
- Kang Wan Chern, "South-east Asia emerges as global data centre hot spot as AI usage rises", *The Straits Times*, 14 October 2024.
- Amy Kathleen Kelly, "Over US $100 billion needed to fund Asia Pacific data centre pipeline in the coming five to seven years", *Cushman & Wakefield*, 27 February 2025, citing the Cushman & Wakefield H2 2024 Asia Pacific Data Centre Market Update.
- Liza Mark and Maisy Chang, "China's Data as a Fifth Market Production Factor – an Asset on Your Balance Sheet", *Haynes Boone*, 23 September 2024.
- Kavita Panda, "Switch to cloud: ASEAN takes the lead", *ASEAN Business Partners*, undated.
- Rapid Sun, Cambodia Digital Transformation (Ministry of Post and Telecommunications, 16

srahim@pdlegal.com.sg 23 Feb 2026

January 2025).

- Yeong Zee Kin, Cross-border Data Flows in the Digital Economy, 2025 SAL Prac 14.
- Mary Zhang, "How Much Does it Cost to Build a Data Center?", *Dgtl Infra LLC*, 5 November 2023.
- "Harnessing ASEAN's Data Center Boom: Opportunities for Operators, Investors & Tech Providers", *ARC Group*, 21 March 2025.
- "The Structure of ASEAN Economy", *ASEAN Statistical Brief Volume IV*, ASEANstats, January 2024.
- Establishing a Trusted Data Corridor in ASEAN (Asian Business Law Institute, December 2024).
- Landscape Study of ASEAN Framework on Cross-border Cloud Computing (Asian Business Law Institute, March 2025).
- "Vietnam: New telecom decree clarifies rules on data center, cloud computing and OTT communications services", *Baker McKenzie*, 7 January 2025.
- "What is a Public Cloud", *Google*, undated.
- "Global data centre market is projected to reach US$4 trillion by 2030", *Knight Frank*, 13 April 2025.
- "Cloud Computing and Services", *Infocomm Media Development Authority*, last updated 23 May 2024.
- Datacentre architecture and infrastructure, *Microsoft*, 8 May 2024.
- "ASEAN Cloud Computing Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)", *Mordor Intelligence*, last updated 7 July 2025.
- Business Process Outsourcing – Malaysia", *Statista*, undated.
- "Spending on public cloud services in ASEAN countries in 2016 and 2021 with a forecast for 2026", *Statista*, 18 September 2024.
- "We take a look at Southeast Asia's rising popularity as a data centre hub", *Tech Collective*, 29 August 2024.
- "e-Conomy SEA 2024 report: Profitability push in Southeast Asia's digital economy delivers 2.5X profits in two years as businesses focus on monetisation", *Temasek*, 5 November 2024.
- "IT outsourcing fetches nearly US$700 million", *Viet Nam News*, 3 January 2025.
- Trusted Cloud Principles.

srahim@pdlegal.com.sg 23 Feb 2026

Annexure: Suggested key contents of an Agreement between AMS A and AMS B on the Establishment of a Trusted Data Corridor[68]

1. General definitions

1.1. In this Agreement, the following definitions apply:

a. Personal information or personal data means any data about an identified or identifiable natural person.

b. Trusted Data Corridor (**TDC**) means a designated geographical area that encompasses [**insert designated geographical area, if applicable**] AMS A and [**insert designated geographical area, if applicable**] AMS B.

c. Party means either AMS for which this Agreement is in force.

d. Subscriber information has the same meaning ascribed to it under the Convention on Cybercrime signed at Budapest, Hungary on 23 November 2001.

2. Module: Personal Data Protection and Transfer

2.1. The Parties recognise the economic and social benefits of protecting personal information in the TDC and the importance of such protection in enhancing confidence in the TDC.[69]

2.2. To this end, each Party shall adopt or maintain legal and regulatory frameworks that provide for the protection of personal information in the TDC. In the development and maintenance of its legal and regulatory frameworks for the protection of personal information in the TDC, each Party shall take into account principles, guidelines and standards of relevant international and regional bodies, including but not limited to the principles stated in the ASEAN Framework on Personal Data Protection adopted at Bandar Seri Begawan, Brunei Darussalam on 25 November 2016, the ASEAN Framework on Digital Data Governance adopted at Bali, Indonesia on 6 December 2018 and the ASEAN Data Management Framework endorsed in January 2021.

2.3. The Parties also recognise that facilitating cross-border data flows through the TDC is necessary for the expansion of cross-border cooperation and international trade.[70]

2.4. Under the premise that the Parties assure each other that their respective national legal and regulatory frameworks for the protection of personal information in the TDC align with international and regional principles that underpin robust legal and regulatory frameworks for the protection of personal information, the Parties agree that the transfer of personal information in the TDC may take place without the need to obtain any further

---

68 This Annexure sets out select key clauses of a template agreement between two AMSs in negotiating a bilateral TDC. It is intended as a starting point for negotiations between AMS A and AMS B, and *not* intended to provide the exact wording of any clause that may be included in such an agreement. For the avoidance of doubt, there is no obligation for any AMS to include any of the suggested clauses in this Annexure in any eventual formal agreement. Reference of wording is made to existing international and regional instruments to promote greater consistency.

69 Reference of wording is taken partially from DEPA Article 4.2.1: Personal Information Protection.

70 Reference of wording is taken partially from Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information.

srahim@pdlegal.com.sg 23 Feb 2026

authorisation.[71] For the avoidance of doubt, transfer of personal information in the TDC means the transfer of personal information between [**insert designated geographical area, if applicable**] AMS A and [**insert designated geographical area, if applicable**] AMS B.

2.5. Recognising that the Parties may have different legal provisions on cross-border data flows, each Party shall pursue, at its discretion, the development of its own mechanisms to achieve the transfer of personal information in the TDC without the need to obtain any further authorisation.[72]

2.6. Acknowledging that the application of data localisation requirements in the TDC will hinder the free flow of data in the TDC, the Parties agree not to impose data localisation requirements on the transfer of personal information in the TDC, unless such a requirement is adopted to achieve a legitimate public policy objective, provided that the requirement

a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised restriction on trade; and

b. does not impose restrictions on the transfer of personal information in the TDC that are greater than are required to achieve the objective.[73]

2.7. The Parties agree to engage in enforcement cooperation in the TDC via their respective competent regulatory authorities, including but not limited to sharing information and providing assistance for investigations and enforcement of regulatory outcomes. The Parties shall decide on the specific areas and forms of enforcement cooperation through consultation.

3. Module: Access by public authorities of the Parties to data held by private sector entities in the TDC

3.1. The Parties affirm that access to data held by private sector entities in the TDC shall be provided for and regulated by their respective domestic legal framework. Such a legal framework shall be binding on the public authorities of a Party, be aligned with international principles or guidelines that operate under the rule of law, including but not limited to the Declaration on Government Access to Personal Data Held by Private Sector Entities adopted on 14 December 2022 by the Organisation for Economic Co-operation and Development, and set out the purposes, conditions, limitations and safeguards concerning access by public authorities to data held by private sector entities.[74]

3.2. Recognising the sovereign duties and obligations of a Party to protect the safety of its citizens by preventing, detecting and confronting criminal activities and threats to public order and national security, and acknowledging that access by public authorities to data held by private

---

71 Reference of wording is taken partially from DEPA Article 4.2.3: Personal Information Protection.

72 Reference of wording is taken partially from DEPA Article 4.2.6: Personal Information Protection.

73 Reference of wording is taken partially from DEPA Article 4.3.3: Cross-Border Transfer of Information by Electronic Means.

74 Reference of wording is taken partially from Declaration on Government Access to Personal Data Held by Private Sector Entities (**OECD Declaration**) (Organisation for Economic Co-operation and Development, 14 December 2022) Article I.

srahim@pdlegal.com.sg 23 Feb 2026

sector entities in the TDC is recognised in a Party's domestic legal framework as essential to meeting those sovereign duties and obligations, the Parties affirm that their respective public authorities shall seek access to data held by private sector entities in the TDC

a. only for the purpose of fulfilling such sovereign duties and obligations;

b. pursuant to their respective domestic legal framework; and

c. in accordance with their respective rules applicable in the TDC.[75]

3.3. Each Party shall adopt or maintain a domestic legal framework where data acquired from private sector entities through public authority access in the TDC are processed and handled only by authorised personnel pursuant to requirements that ensure

a. privacy, security, confidentiality and integrity of such processing and handling;

b. such data are processed lawfully;

c. such data are retained only for as long as authorised under its domestic legal framework in view of the purpose and taking into account the sensitivity of the data; and

d. such data are kept accurate and up to date to the extent appropriate having regard to the context.[76]

3.4. Each Party shall implement or maintain internal controls to detect, prevent and remedy loss, unauthorised or accidental access, destruction, use, modification, or disclosure of data acquired from private sector entities through public authority access, and to report such instances to oversight bodies.[77]

3.5. Each Party shall implement or maintain domestic regulations to clarify that in the TDC, the role of service providers, other than cloud services providers (**CSP**), in fulfilling public authority access requests shall be limited to conveying such requests to their enterprise customers or informing their enterprise customers of the receipt of such requests.

3.6. Acknowledging the unique nature of cloud services and the role of CSPs in providing cloud services, the Parties agree that when their respective public authorities seek access to data held by private sector entities that are hosted in the TDC, those public authorities shall

a. seek access directly from the enterprise customers of CSPs, wherever practicable; and

b. where it is impracticable for them to seek access directly from the enterprise customers of CSPs, clarify the role of the CSPs in fulfilling such access requests, such as providing subscriber information of their enterprise customers.

3.7. [**Optional, aspirational element**] Recognising that one Party may wish to facilitate the requests by the public authorities of the other Party to, for legitimate purposes, access data

---

75 Reference of wording is taken partially from OECD Declaration preamble and Article III.

76 Reference of wording is taken partially from OECD Declaration preamble and Article IV.

77 Reference of wording is taken partially from OECD Declaration preamble and Article IV.

srahim@pdlegal.com.sg 23 Feb 2026

held by private sector entities that are hosted in the geographical areas of the TDC that are within the first Party's territory, the Parties agree to clarify that

a. a private sector entity constituted, domiciled or established, or having business operations, in one Party should be compellable by that Party to retrieve data stored in data centres located in the TDC, including in data centres located in the territory of the other Party, for legitimate purposes in the first-mentioned Party, subject to the domestic legal framework of the first-mentioned Party that applies to the TDC; and

b. a CSP providing services in or for the TDC may provide public authorities of the Parties with subscriber information of its enterprise customers for legitimate purposes, subject to the Parties' respective domestic legal framework that applies to the TDC.

3.8. The Parties shall not impede private sector entities from publishing aggregate statistical reports regarding requests by their respective public authorities to access data held by the private sector entities that are hosted in the TDC, provided that such aggregate statistical reporting is not in contravention of the Parties' respective domestic legal framework that applies to the TDC.

srahim@pdlegal.com.sg 23 Feb 2026

srahim@pdlegal.com.sg 23 Feb 2026

Addendum: Application of the ASEAN Cloud Computing Framework to financial and health industries

Building upon earlier ASEAN data governance efforts such as the ASEAN Principles of Personal Data Protection, the ASEAN Framework on Digital Data Governance and the ASEAN Data Management Framework, the ASEAN Cloud Computing Framework is designed to be industry-agnostic but with a specific focus on cloud computing and its unique characteristics.

Accordingly, the ASEAN Cloud Computing Framework introduces several innovations, such as the tiering structure and the TDC use case, to reflect the evolving needs of data and digital governance. It may be referenced to as an intermediary layer between high-level principles for data and digital governance and granular regulatory and technical measures for cloud computing.

As mentioned earlier, cloud computing is already an essential enabler for a wide range of industries, and among the beneficiaries include regulated industries such as finance and health which have increasingly integrated cloud solutions into routine operations. Regulated industries, however, are usually subject to more stringent requirements on cloud use for a variety of reasons. First, these industries usually operate under a complex web of legal and regulatory requirements as well as industry-specific standards. Those requirements and standards are often more stringent than, and apply on top of, universal, baseline laws and regulations, in areas such as cross-border data transfer, data security, confidentiality, etc. Second, regulated industries often deal with data that are sensitive in nature, the compromise of which will likely result in significant harm. As a result, regulators of those industries tend to impose higher standards on matters such as access control in cloud deployment, as well as on how to manage third-party vendor risks, such as outsourcing to CSPs.

In light of the additional complexity faced by regulated industries in cloud adoption, this Addendum discusses how the financial industry and the health industry, two typical regulated industries, may make use of the ASEAN Cloud Computing Framework.

Special circumstances of financial and health industries

Several special circumstances can be observed with regard to data and the use of cloud computing in financial and health industries in ASEAN.

First, individuals' financial and health data are generally considered to be of a sensitive nature, and this characterisation often subjects such data to more stringent protection requirements than non-sensitive data. Among AMSs with omnibus personal data protection legislation, some have a distinct category of sensitive personal data which often captures data on individuals' financial and/or health conditions. Others, although not explicitly regulating sensitive personal data by legislation, have indicated through advisory or other guidance that financial and health data of individuals are considered to be sensitive and ought to be protected to a higher standard.[78] Where AMSs impose more stringent requirements on the processing of sensitive personal data, the cross-border transfer of financial and health data of individuals in those AMSs will accordingly be subject to additional safeguards. If not managed properly, these more stringent requirements can disrupt business operations, such as the centralised outsourcing operations by MNCs described earlier.

Second, some AMSs impose special requirements on the financial and/or health industry in terms of data storage and the use of offshore cloud computing services. For example, Indonesia requires health information system providers to only process data and health information locally, apart from

78 See Table 1 for more details.

srahim@pdlegal.com.sg 23 Feb 2026

limited exceptions,[79] and all electronic medical records must be stored in onshore data centres.[80] In the financial industry, banks are allowed to use cloud services from offshore providers but only with prior regulatory approval, and they must place electronic systems in data centres and disaster recovery centres in Indonesia.[81] Thailand mandates the processing of credit information be done domestically.[82] Banks in Thailand are also required to notify or seek approval from the central bank before using cloud services, depending on service type.[83] Vietnam has general data localisation requirements, which covers financial and health data.[84]

Relatedly, financial and health regulators often have greater power to request access to financial and health data held by private sector entities such as CSPs. Special rules in this regard can be found across AMSs, regardless of whether general or industry-specific data localisation requirements are in place. For example, the financial regulators of Malaysia[85] and Singapore[86] both demand the right of access to regulators in third-party provider management or outsourcing agreements. The joint statement between the central banks of the Philippines and Singapore allow financial institutions to store and process data in any location provided that both regulators have full and timely access to the data necessary to fulfill their regulatory and supervisory mandate.[87]

These more stringent, industry-specific requirements stem out of broader considerations for financial stability, patient privacy, national security, legal supervision and investigation, etc.

Application of the ASEAN Cloud Computing Framework to financial and health industries

The special considerations above mean that the application of the ASEAN Cloud Computing Framework to the financial and health industries may require industry-specific adjustments.

Location of computing facilities and data localisation

The default position in General Principle 4 prohibits the imposition of any requirement on the use or location of computing facilities onshore as a condition for conducting business. This default rule can only be varied by the strictly-circumscribed legitimate public policy objective exception. Importantly,

FOR ASEAN CONSULTATION

---

79 See Irene Djalim and Annisa Syaharani, "*Personal Data Protection and Healthcare Services in Indonesia*", *Tilleke & Gibbins International Ltd*, 25 October 2023, citing Law No. 17 of 2023 concerning Health.

80 Cahyani Endahayu, Reagen Mokodompit and Nadia Andika, "*Indonesia: New medical records regulation — what's new?*", Baker McKenzie, 20 December 2022, citing MOH Regulation No. 24 of 2022 on Medical Records.

81 ASEAN Banking Interoperable Data Framework (IDF), ASEAN Bankers Association, November 2022, at p 14, citing OJK Regulation No. 13/POJK.03/2020.

82 Credit Information Business Operation Act, B.E. 2545 (2002), section 12.

83 Notification of the Bank of Thailand No. FPG. 19/2559 Re: Regulations on IT Outsourcing for Business Operations of Financial Institutions (1 September 2017), 1(1).

84 Decree No. 13/2023/ND-CP on Personal Data Protection (**Decree No. 13**) read together with Decree No. 53/2022/ND-CP guiding the Law on Cybersecurity 2018. On 26 June 2025, Vietnam passed the Law No. 91/2025/QH15 on Personal Data Protection (**Personal Data Protection Law**) which will supersede Decree No. 13 once it comes into effect on 1 January 2026. The Personal Data Protection Law has retained the requirements on cross-border transfer of personal data currently found in Decree No. 13.

85 *Risk Management in Technology (RMiT) Exposure Draft*, Bank Negara Malaysia, issued 7 November 2024, 10.48(a).

86 *Guidelines on Outsourcing*, Monetary Authority of Singapore, effective 8 October 2018, 5.10.2(b).

87 Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore, 16 November 2020, 2(b) and 2(c).

srahim@pdlegal.com.sg 23 Feb 2026

by not providing any industry-specific carve-out,[88] General Principle 4 signals to AMSs that they should continue to adhere to the default position even when applying this Principle to finance, health and other regulated industries. In fact, AMSs may take the application of General Principle 4 as an opportunity to revisit any existing regulations and/or policies that mandate the use or location of onshore computing facilities as a condition for doing business in the financial and/or health industry to assess whether those regulations and/or policies are justifiable under the legitimate public policy objective exception. If after assessment, an AMS considers such regulations and/or policies to fall under the legitimate public policy objective exception, the AMS should further ensure that any deviation of the financial and/or health industry from the default position is not unbridled and is instead within the confines of the additional safeguards adopted under General Principle 4.

Similarly, where AMSs pursue further cooperation under the ASEAN Cloud Computing Framework by entering into a G2G agreement to set up a bilateral or multilateral TDC, Specific Principle 2 requires the participating AMSs to lift the application of any existing data localisation requirements in the TDC and that requirement applies across industries. The only exception to this default rule is the legitimate public policy objective exception under General Principle 4. Participating AMSs of a TDC must assess whether any continued application of industry-specific data localisation requirements in the TDC is justifiable under this exception. Alternatively, participating AMSs may, in negotiating the G2G TDC agreement, agree that the TDC will, or will not, be utilised for specific types of data, such as data of a certain regulated industry.

In summary, to foster broader, industry-neutral cloud adoption across ASEAN, AMSs are encouraged to treat the implementation of the ASEAN Cloud Computing Framework as an opportunity to revisit existing regulations, policies or requirements on data localisation and the location of computing facilities in financial and health industries. During such review, AMSs should assess whether such regulations, policies or requirements remain consistent with the General and Specific Principles outlined in this Framework, and consider removing or easing those that do not serve any legitimate public policy objective and are thus incompatible with this Framework.

Public authority access to private sector entity data

Relevant General Principles and Specific Principles outlined in this Framework set to balance the legitimate needs of public authorities to access private sector entity data and the protection of exported data in cloud delivery, taking into account the operational realities of CSPs and their role as intermediaries. Working together, the principles require that public authority access be based on a binding legal framework aligned with internationally accepted standards, that AMSs collaborate to reduce conflict of laws incidents relating to such access, and that participating AMSs of a TDC adopt special rules so that public authority requests to access private sector entity data in the TDC are directly issued to the enterprise customers of CSPs whenever practicable. These requirements apply to all industries without exception.

As stated above, financial regulators often have stronger demands when it comes to accessing the financial data held by private sector entities including CSPs. This position is echoed in some digital economy agreements. In one instance, although the use or location of onshore computing facilities is

88 Some digital economy agreements have specific carve-outs for the financial industry by excluding "computer servers or storage devices of or used to access financial market infrastructures" from the definition of "computing facilities". See for example, Australia-Singapore Digital Economy Agreement (signed 6 August 2020) Chapter 14 Digital Economy, Article 1(b) and Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore (signed 21 November 2022) Chapter 14 Digital Economy, Article 14.1.

PUBLIC CONSULTATION

srahim@pdlegal.com.sg 23 Feb 2026

not mandated as a condition for conducting financial business, the regulator's "immediate, direct, complete and ongoing access" to financial data processed or stored on offshore computing facilities must be guaranteed.[89] In another instance, signatories only agree to share experiences and views relating to the development, adoption, and implementation of policies and rules that can allow such immediate, direct, complete and ongoing access without the need to mandate the use or location of onshore computing facilities.[90]

If the financial industry is included in the coverage of a TDC, in practice, the public authorities of the participating AMSs are likely to still turn to CSPs for access to the financial data owned by financial institutions which use cloud services provided by the CSPs. This is because the CSPs are in the best position to facilitate "immediate, direct, complete and ongoing access". This Framework caters to such scenarios by stating that where a public authority (in this case a financial regulator) must seek access from a CSP due to it being impracticable to seek access directly from the CSP's enterprise customer (in this case likely a financial institution), the requesting public authority will clarify the role of the CSP in fulfilling this access request, such as providing subscriber information.

In summary, this Framework does not restrict or diminish the ability of public authorities to access data held by private sector entities, whether in regulated industries or otherwise. On the contrary, it introduces new rules in a confined space that are aimed at both facilitating the efficient and lawful processing of legitimate public authority access requests and safeguarding exported data in a manner that respects the operational realities of CSPs. This is a balanced approach intended to build trust among stakeholders, promote regulatory clarity, and create a more attractive environment for cloud investment in ASEAN.

For ASEAN CIRCULATION

89 Australia-Singapore Digital Economy Agreement (signed 6 August 2020) Article 25.2.

90 Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore (signed 21 November 2022) Article 14.16(4)(a).

srahim@pdlegal.com.sg 23 Feb 2026

Table 1: Treatment of financial and health data of individuals as sensitive personal data[91]

Brunei	**Indonesia**	**Malaysia**	**Philippines**	**Singapore**	**Thailand**	**Vietnam**
The Protection Data Protection Order does not distinguish between sensitive and non-sensitive personal data. However, the regulator has stated that if the potential adverse effects or harm to an individual is high when the data concerned are misused or subject to unauthorised access or disclosure, such	The Personal Data Protection Law has the concept of specific personal data. These are personal data the processing of which may have a greater impact on data subjects. Individuals' **health information and information on personal financial status** are among examples of specific personal data.[93]	The Personal Data Protection Act (**Act**) defines sensitive personal data as, among others, information about **an individual's health or physical or mental condition**, political opinions, religious beliefs and other beliefs of a similar nature.[95] An individual's financial information is not specifically listed as	The Data Privacy Act and its Implementing Rules and Regulations include personal information about an individual's **health** and **tax returns** in the definition of sensitive personal information.[97] In general, the processing of sensitive personal information is prohibited unless such processing	The Protection Data Protection Act does not distinguish between sensitive and non-sensitive personal data. However, the Personal Data Protection Commission (**PDPC**) does take a stricter view when considering a case where the personal data compromised are of a sensitive nature. For instance, a person's	Sensitive personal data include, among others, personal data pertaining to a natural person's **health and disability data**, genetic data, and biometric data and any other data which may affect the individual in the same manner, as prescribed by the Personal Data Protection Committee.[100]	Sensitive personal data include, among others, a person's **health conditions**, physical and biological characteristics, and **banking information.**[102] A party that handles sensitive personal data has extra obligations, including to designate a department/person in charge of personal data

91 This table only covers AMSs with omnibus personal data protection legislation.

93 Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection Law, Article 4(2).

95 "What is personal data sensitive?", FAQ Personal Data Protection, Personal Data Protection Commissioner, undated.

97 Implementing Rules and Regulations of Republic Act no. 10173, also known as the "Data Privacy Act of 2012", Rule I Section 3(t).

100 Personal Data Protection Act B.E. 2562 of Thailand (2019), Section 26.

102 Decree No. 13, Article 2.4. Under Article 2.3 of the Personal Data Protection Law, sensitive personal data refer to "personal data associated with the privacy of an individual that, once infringed upon, will directly affect the lawful rights and interests of agencies, organizations or individual, as prescribed in the list issued by the Government". This definition makes it likely that an individual's financial and health data will fall within the category of sensitive personal data.

For ASEAN CIRCULATION

srahim@pdlegal.com.sg 23 Feb 2026

Brunei	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
data may be considered to be "sensitive" and that more stringent measures may be required to ensure appropriate protection of such data.[92] It is thus reasonable to infer that financial and health data of individuals may be considered sensitive.	Where data are classified as specific personal data, a data controller must conduct an assessment on the impact of the protection of such data.[94]	sensitive personal data. The Act does not allow the processing of sensitive personal data except for the purposes specified in the Act and such processing must be with the express consent of the data subject.[96]	falls under prescribed exceptions, such as where the data subject has given consent specific to the purpose prior to the processing.[98]	financial information, together with other identifying information, can constitute "sensitive" personal data. As the PDPC has noted, personal data of a sensitive nature should be subjected to a higher standard of protection.[99]	An individual's financial information is not specifically listed as sensitive personal data. Sensitive personal data may only be processed pursuant to a prescribed lawful basis, such as data subject consent and protection of the vital interest of an individual.[101]	protection, and exchange information about that department/person with the relevant government authority.[103]

92 "Response to Feedback on Public Consultation Paper on Personal Data Protection for the Private Sector", *Authority for Info-communications Technology Industry of Brunei Darussalam*, 3 December 2021, at para 3.3 and para 3.4.

94 Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection Law, Article 34.

96 "What are the conditions for processing sensitive personal data?", FAQ Personal Data Protection, Personal Data Protection Commissioner, undated.

98 Implementing Rules and Regulations of Republic Act no. 10173, also known as the "Data Privacy Act of 2012", Rule V Section 22.

99 "*Being Accountable to Stakeholders*", DPO Connect, Personal Data Protection Commission, September 2019.

101 Personal Data Protection Act B.E. 2562 of Thailand (2019), Section 26.

103 Decree No. 13, Article 28. The Personal Data Protection Law contains specific provisions on the protection of personal data related to health information (Article 26) and the protection of personal data in financial, banking and credit information activities (Article 27).

For ASEAN Circulation

ASIAN BUSINESS LAW INSTITUTE