

越境クラウドに関する ASEAN 枠組み： 戦略分析と企業への影響

ASEAN Framework on Cross-Border Cloud Computing: Strategic Analysis and Business Implications

【要約】

ASEAN における越境クラウドに関する枠組みは、ASEAN 加盟国間における信頼性と安全性の高いクラウド利用を促進するため、越境データ流通と国外移転データ保護に関する共通原則を示すものである。ASEAN 域内で広く参照される一般原則 6 項目に加え、「信頼データ回廊 (TDC)」を通じた具体的な原則と、金融・医療などの規制に向けた補足的指針を含む構成となっている。投資誘致、ビジネス円滑化、信頼構築を目的に、データ越境移転の予見可能性の向上とデータ保護基準の整合性確保を図る内容となっている。

TDC は参加する ASEAN 複数国間でデータの安全な流通を可能にする制度であり、共通基準の整備や法制度調整を通じて運用される。金融・医療分野にも配慮しつつ、ASEAN のデジタル経済基盤強化と市場拡大を支える枠組みとなっている。

【免責条項】

本レポートで提供している情報は、ご利用になる方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用になる方に不利益等が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承下さい。なお、本稿は 2025 年 11 月時点の情報に基づきます。

Title: ASEAN Framework on Cross-Border Cloud Computing: Strategic Analysis and Business Implications

Country/Region: ASEAN, Indonesia

Written Date: January 2026

Lead Paragraph

The ASEAN Framework on Cross-Border Cloud Computing ([ASEAN Cloud Computing Framework](#)) was developed to promote trusted and secure cloud adoption across ASEAN Member States. This framework addresses two critical pillars of cloud governance: cross-border data flows and protection of exported data. The framework introduces a tiered structure consisting of six General Principles for region-wide application, four Specific Principles operationalized through a policy innovation called the Trusted Data Corridor (TDC), and an addendum addressing application to regulated industries (finance and healthcare).

Vision and Strategic Objectives

Overall Vision:

To assist ASEAN policymakers in attracting cloud investment by enhancing trust in the region's cloud ecosystem through enabling institutional infrastructure aligned with internationally accepted principles, while encouraging private sector cloud adoption through guarantees of cross-border data flow and safeguards for transferred data.

Three Core Objectives:

- **Attract Investment** - Build institutional support that demonstrates ASEAN jurisdictions are trustworthy destinations for cloud infrastructure investment
 - **Enable Business** - Provide guarantees of cross-border data flow and assurances of safeguards for data transferred between Member States
 - **Build Confidence** - Enable businesses and individuals to participate in ASEAN's digital economy with confidence through demonstrated commitment to data protection
-

Framework Structure: Six General Principles

The framework establishes six General Principles for ASEAN-wide adoption:

1. **General Principle 1: Fostering Trusted Cloud Environment**
 - ASEAN Member States commit to supporting trusted and secure deployment and use of cloud computing by public and private sectors
 - Recognition that cloud computing must develop in a manner that serves public good
2. **General Principle 2: Rule of Law**
 - Provision and regulation of cloud computing must be in accordance with law
 - Emphasis on protection of personal data within legal frameworks
 - Recognition that rule of law provides predictable and transparent legal environment
3. **General Principle 3: Facilitating Cross-Border Data Flows**
 - Commitment to further facilitate cross-border data flows in manner aligned with international and regional principles
 - Reference to ASEAN Framework on Personal Data Protection (2016), ASEAN Framework on Digital Data Governance (2018), and ASEAN Data Management Framework (2021)

- Does not require sweeping changes but calls for continued efforts toward facilitation
4. **General Principle 4: Limiting Data Localization Requirements**
 - Prohibition on imposing requirements for onshore computing facilities as condition for conducting business
 - Exception allowed only for legitimate public policy objectives, with strict safeguards:
 - Must not constitute arbitrary/unjustifiable discrimination or disguised trade restriction
 - Must not impose restrictions greater than required to achieve objective
 - Consistent with positions in Digital Economy Partnership Agreement (DEPA) and other digital economy agreements
 5. **General Principle 5: Special Rules for Cloud Services**
 - Recognition that cloud computing brings unique circumstances requiring tailored approaches
 - Agreement that special rules may be developed where appropriate to provide legal clarity and regulatory coherence
 - Acknowledgment of cloud services providers (CSPs') unique role as intermediaries rather than data owners
 6. **General Principle 6: Promoting Cooperation to Reduce Regulatory Conflicts**
 - Commitment to cooperation among Member States to reduce regulatory conflicts
 - Particular focus on situations where data are held in or accessed from multiple Member States
 - Recognition that borderless nature of cloud computing requires heightened cooperation
-

Trusted Data Corridor (TDC)

TDC Overview:

A governance structure connecting data centers in two or more ASEAN Member States to support secure, seamless, and trusted flow, processing, and storage of data. Mirrors approach of Special Economic Zones (SEZs) and Free Trade Zones (FTZs) by applying special rules within designated areas.

TDC Archetypes:

- Bilateral TDC connecting designated areas or entire territories of two Member States
- Multilateral TDC involving more than two Member States
- Flexibility for Member States to participate via designated areas (e.g., existing SEZs) or entire territory
- Full discretion for each Member State on timing and method of participation

Four Specific Principles for TDCs:

1. **Specific Principle 1: Comparable Protection Standards**
 - Personal data transfer in TDC may occur without further authorization if participating Member States share comparable protection standards
 - Member States conduct mapping exercise against neutral international/regional principles (OECD Privacy Principles, ASEAN Principles, APEC Privacy Framework, Global CBPR Framework)

- Legal modifications required only where mapping reveals non-alignment
2. **Specific Principle 2: No Data Localization in TDC**
 - Participating Member States agree not to impose data localization requirements on personal data transfers in TDC
 - Exception only under circumstances stated in General Principle 4 (legitimate public policy objectives with strict safeguards)
 3. **Specific Principle 3: Regulated Public Authority Access**
 - Access to data held by private sector entities in TDC must be provided for and regulated by domestic legal framework
 - Legal framework must be:
 - Binding on public authorities
 - Aligned with international principles operating under rule of law
 - Clear on purposes, conditions, limitations, and safeguards
 - Reference to OECD Declaration on Government Access to Personal Data Held by Private Sector Entities
 4. **Specific Principle 4: Direct Access from Enterprise Customers**
 - When public authorities seek access to data in TDC, they shall:
 - Seek access directly from enterprise customers of CSPs wherever practicable
 - Where impracticable, clarify role of CSPs in fulfilling requests (e.g., providing subscriber information)
 - Recognition of CSPs' role as intermediaries rather than data owners

Two-Step Process for TDC Establishment:

1. **Step 1: Government-to-Government Agreement**
 - Interested Member States enter binding G2G agreement on TDC establishment, operation, and administration
 - Agreement details specific obligations tailored to signatory Member States' priorities
 - Suggested template provided in framework Annexure
 2. **Step 2: Domestic Legal Alignment**
 - Signatory Member States conduct mapping exercise to benchmark laws against agreed international/regional standards
 - Legal modifications made where necessary through:
 - Amendment of existing laws/regulations for TDC application
 - Passage of new laws/regulations for TDC
 - Subsequent Member States can join by undertaking same commitments and achieving comparable standards
-

Application to Regulated Industries: Finance and Healthcare

The framework includes specific guidance for financial and healthcare industries, which face more stringent requirements due to:

- Sensitive nature of financial and health data
- Complex regulatory requirements and industry-specific standards
- Higher standards for access control and third-party vendor risk management

Key Positions:

- **Computing Facilities/Data Localization:** Member States encouraged to revisit existing regulations requiring onshore facilities or data localization in finance/healthcare to assess compatibility with framework principles
 - **Public Authority Access:** Framework does not restrict regulators' ability to access data but introduces new rules to facilitate efficient, lawful processing while respecting CSPs' operational realities
 - **Special Considerations:** Recognition that financial regulators often require "immediate, direct, complete and ongoing access" to data, with framework accommodating through clarified CSP roles
-

Market Context

ASEAN Cloud Market Projections:

- Market size: \$24.91 billion (2026) projected to reach \$48.74 billion (2031) (Source: [Mordor Intelligence, "ASEAN Cloud Computing Market Size, Share & Industry Analysis, 2031"](#))
- CAGR: 14.35% during forecast period (2026-2031)
- Public cloud spending: \$5.4 billion (2021) forecasted to exceed \$11 billion (2026) (Source: [IDC](#))
- Cloud infrastructure revenue: \$2.18 billion (2022), up 25% year-on-year (Source: [CARI](#))

Data Center Landscape:

- Over 350 data centers across eight of ten ASEAN Member States (as of August 2024) (Source: [Tech Collective Asia](#))
- ASEAN emerging as major global data center market
- Estimated \$116 billion investment needed for Asia Pacific data center pipeline over next 5-7 years (Source: [Cushman & Wakefield](#))