NEW GLOBAL ORDER

The missing link in Asean's AI economy: trusted cross-border data flows

The region's AI future depends on bridging differences and scaling what works. BY LIU JINGTING AND JESSLENE LEE

ARTIFICIAL intelligence could add nearly US$1 trillion to Asean's economy by 2030, equivalent to between 10 and 18 per cent of the region's gross domestic product. But unlocking that growth hinges on one thing: data.

"Data is the lifeblood of AI," said Singapore's Minister for Digital Development and Information Josephine Teo at the Asia Economic Summit in Indonesia on Jun 17. As Asean seeks to capture AI-powered growth, common rules and frameworks are key to enabling data to flow seamlessly and securely across borders.

Yet, countries in the region differ in their approaches to data governance. Some place greater emphasis on national security and more arduous data controls, while others favour more open data flows with safeguards.

Fragmentation in the region's data governance regime hinders smooth cross-border flow of data and imposes an estimated US$15 billion to US$20 billion in annual compliance costs on businesses, noted the Information Technology Industry Council.

The answer is not to force a single set of data rules across Asean, but to build bridges between existing ones. Those bridges are what a common framework can realistically look like.

The Asean Model Contractual Clauses (MCCs) and the joint guides mapping them to extra-regional frameworks provide a practical mechanism for businesses to move data lawfully across jurisdictions with different data regimes without the need for full regulatory convergence.

Scaling such mechanisms is how Asean can fully capture the economies of scale of the AI economy.

Asean members pull in different directions on data: sovereignty versus openness, and chasing the data economy versus keeping value at home.

Until data moves freely and securely across Asean, the region might not fully realise the benefits of the AI economy. PHOTO: BT FILE

Patchwork of rules

Most countries in the region now lean towards conditional liberalisation of data governance similar to that adopted in the EU, indicated the Asia Competitiveness Institute's book, *Data Governance and the Digital Economy in Asia.*

Adequate data protection by data-receiving regions, binding corporate rules or standard contractual clauses are common mechanisms for transferring private data across borders, as set out in their implementing regulations or in frameworks under development. Countries such as Singapore, Malaysia and Thailand fall into this camp.

Some other countries, driven by national security and cybersecurity concerns, adopt a regulatory framework closer to China's – classifying data by sensitivity and imposing stricter rules on "important" or "core" data, with state approval required, in some cases, before data can be transferred abroad. Vietnam is one such example.

Sitting at the other end of the data regulatory spectrum is the Philippines, the region's most liberal on cross-border flows. Rather than channelling transfers through prescriptive gateways, it places primary responsibility on businesses, which must take reasonable measures to ensure comparable protection abroad.

Gaps in data regulations across the region hinder smooth cross-border data transfer. The fix is not to seek complete regulatory uniformity. Imposing a single rulebook across 11 countries is neither feasible nor realistic; each guards its own balance of sovereignty, security and openness.

The smarter path is to build bridges between regimes that already exist – bilaterally or regionwide.

A few examples already point the way. In 2023, Asean and the EU released a joint guide mapping the Asean Model Contractual Clauses onto the EU's Standard Contractual Clauses, easing data transfers between the region and Europe.

In 2025, a second guide mapped the Asean clauses onto that of the Ibero-American Data Protection Network, opening the same pathway to Latin America, Spain and Portugal.

Wider trade pacts offer another model. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), whose 12 members include four Asean member states, is hailed as the "gold standard" for digital trade – in principle, cross-border data transfers must be allowed and data localisation barred.

Crucially, it does not impose regulatory uniformity. It carves out exceptions and allows deviation from both requirements for legitimate public policy objectives, but subjects such measures to scrutiny through a dispute settlement mechanism.

This mechanism ensures any such deviations are not more trade-restrictive than necessary. The UK cited this flexibility when assuring its citizens that it would not have to give up its relatively stringent personal data protection standards when it acceded to the CPTPP.

This combination of open data flows by default and a shared process for adjudicating exceptions functions as a bridge in its own right, reconciling national regulatory autonomy with digital integration.

The challenge for Asean is to realise this bridging logic at the regional level.

The Digital Economy Framework Agreement (Defa), due to be signed at the Asean Summit this November, has at its core the development "streamlined, robust and shared digital rules" for trusted data flows, as noted by the Singapore Ministry of Trade and Industry.

Provisions that allow replicating and scaling up bridging mechanisms would allow it to live up its name as a "landmark" deal for regional digital trade.

A relatively low-hanging fruit might be to formalise endorsement of Asean MCCs as a legitimate cross-border data transfer mechanism, and potentially leave room for exceptions or transition periods where needed.

That, more than any single rulebook, will determine whether Defa can set a new benchmark for digital integration standards and help the region plug into the global digital economy.

Cyber resilience

Robust cybersecurity infrastructure should also complement efforts to bridge data regimes. As cross-border connectivity deepens, the region faces heightened exposure to risks such as data breaches and coordinated cyberattacks.

Asean is already strengthening cyber resilience through mechanisms such as the Asean Regional Computer Emergency Response Team, which facilitates incident response coordination and intelligence sharing. The Asean Data Management Framework also provides a guide for businesses to implement data governance safeguards.

Seamless data flows should not come at the expense of security, nor should safeguarding security become a barrier to data flows. The two objectives can – and must – reinforce rather than constrain each other.

Countries could negotiate a shared list of "safe" data categories, assessed as relatively low-risk, that move with lighter scrutiny. This builds another bridge that keeps data flowing while preserving sufficient policy space for countries to protect their unique national priorities.

In Asean's push to realise the benefits of the AI economy, trusted cross-border data flows are the crucial missing link. Until data moves freely and securely, those returns will stay out of reach.

The writers are researchers at the Asia Competitiveness Institute, Lee Kuan Yew School of Public Policy at the National University of Singapore. Liu is also a senior lecturer with James Cook University Singapore.

This essay is part of New Global Order, a series which explores how the changing world landscape is reshaping business, politics and beyond.