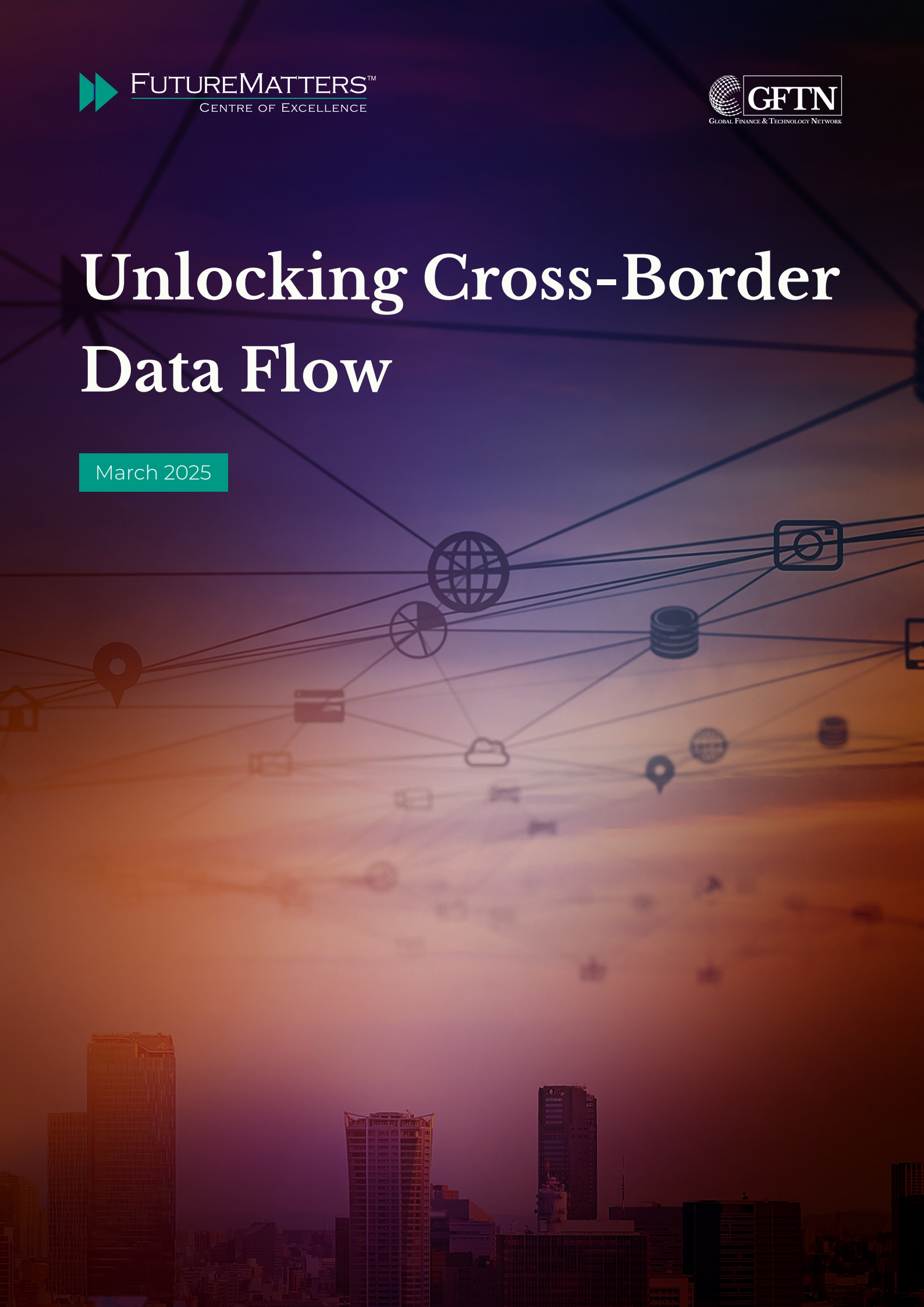
FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

Unlocking Cross-Border Data Flow

March 2025



Contents

About

The Global Finance & Technology Network (GFTN) (formerly known as Elevandi) is a not-for-profit organisation established by the Monetary Authority of Singapore (MAS) in 2024 to harness technology and foster innovation for more efficient, resilient, and inclusive financial ecosystems through global partnerships. GFTN organises convening forums, offers advisory services on innovation ecosystems, provides access to transformative digital platforms, and invests in technology startups with the potential for growth and positive social impact through its venture fund.

For more information, visit www.gftn.co

BowerGroupAsia (BGA) is a strategic advisory firm that specializes in the Indo-Pacific.

BGA applies unmatched expertise and experience to help clients navigate the world's most complex and dynamic markets. We do that by providing actionable intelligence to implement strategies, expand business, solve problems and do good work for the people of Asia, the countries they live in and our clients.

BGA is the first company to provide granular, exclusively Asia-focused strategic support in this space.

For more information, visit www.bowergroupasia.com

Executive Summary

Cross-border data flows are essential for the digital economy, enabling the seamless exchange of information across national boundaries, fostering innovation, economic growth and regional collaboration. According to research by the World Trade Organisation and OECD, global GDP could fall by 5% if countries restricted data flows – and conversely, if all countries were to enable data flows with trust, global GDP would grow by 1.77%.[1]

Yet, an uptick in data localisation policies, arising out of concerns for data protection and privacy, economic goals, and national security and sovereignty, have created a challenging environment for the flow of data across borders and impact economic growth. This report draws from the discussion that took place during the Insights Forum public-private roundtable on Unlocking Cross-Border Data Flows: Navigating Data Localisation Requirements in the Financial Sector at the Singapore FinTech Festival in November 2024. The report synthesises key themes and presents recommendations for industry and governments to consider on how to enable the full potential of cross-border data in fostering innovation, economic growth and regional collaboration.

Key themes included the impact of geopolitics on cross-border data flows, the increasing constraints on cross-border data flows by localisation policies and regulatory ambiguity, the need to align national priorities with regional data governance standards, and the role of technology in addressing cross-border data challenges. These themes underscore how industry and government can think about the challenges posed by today's dynamic and fast-paced social and economic interactions, which rely on the free flow of data across borders.

The discussion highlighted the need for governments to adopt balanced localisation approaches that account for both national interests and economic priorities, as well as to establish baseline standards to minimise inconsistencies and regulatory ambiguity. Governments in the Asia-Pacific region should also prioritise regional data governance agreements to harmonise data standards and enable regional data flows.

Additionally, companies should perform regular risk assessments to ensure compliance with relevant data protection regulations as they evolve and keep abreast of technological developments that can create new opportunities for overcoming cross-border data challenges.

Introduction

Cross-border data flows are essential for the digital economy. They enable the seamless exchange of information across national boundaries, fostering innovation, economic growth and regional collaboration. Research by the World Trade Organisation and OECD found that global GDP could fall by 5% if countries restricted data flows. Conversely, if all countries were to enable data flows with trust, global GDP would grow by 1.77%.[1]

Global and regional connectivity has enabled cross-border economic activity, allowing individuals, startups and small businesses to participate in global markets, with forecasts indicating that the value of cross-border payments will reach US$250 trillion in 2027.[2]

Despite the explosive growth in connectivity and data, the landscape for data governance in the Asia-Pacific is still taking shape. Leaders know that allowing data to flow across borders has wide-ranging benefits, but they are reluctant to give up control. In the current climate, reaching a consensus on agreements will be challenging, but it is critical for the private sector and governments to work together to find the appropriate balance.

Four key themes are explored in this report:

Theme 1:

The impact of geopolitics on cross-border data flows.

Cross-border data flows are critical for the digital economy. However, geopolitics — and domestic politics — significantly impact government policies towards data governance. Some countries have adopted restrictive data governance policies; others have more relaxed policies. The United States, which has traditionally placed fewer restrictions on data governance, has shifted towards more restrictive policies due to national security concerns. This complex landscape requires companies and countries to navigate varying data governance approaches influenced by geopolitical tensions.

Theme 2:

Cross-border data flows are increasingly constrained by localisation policies and regulatory ambiguity.

Companies face several challenges when transferring data across borders. Two that are highlighted in this section are the growing trend of data localisation policies and compliance challenges arising from regulatory ambiguity. Multilateral cooperation and the development of regional standards can help address these challenges by providing a shared framework for national policies.

Theme 3:

Aligning national priorities with regional data governance standards

The Asia-Pacific's fragmented data governance policies highlight the tension between national priorities and the economic benefits of cross-border data flows. As excessive localisation and divergent regulations create inefficiencies, regional consensus for safe and trusted data flows becomes crucial.

The Association of Southeast Asian Nations' (ASEAN) Digital Masterplan 2025 and the upcoming ASEAN Digital Economic Framework Agreement aim to harmonise data governance frameworks and facilitate cross-border data flows.

Governments in the Asia-Pacific should prioritise the negotiation and implementation of these frameworks to harmonise standards and reduce inefficiencies. In parallel, countries could also explore bilateral digital trade agreements, which offer a pragmatic pathway to advance digital trade collaboration without the complexities of broader trade deals.

Theme 4:

The role of technology in addressing cross-border data challenges

Technological innovations offer significant potential to address cross-border data challenges and advance economic integration without compromising national priorities. Emerging technologies in this space include blockchain, tokenisation, artificial intelligence, synthetic data and privacy-enhancing technologies.

The successful deployment of these technologies will depend on collaboration between governments and the private sector, facilitating international cooperation and aligning solutions with global best practices.

Report

The impact of geopolitics on cross-border data flows

Cross-border data flows are essential to the digital economy. They enable the seamless exchange of information across borders, supporting real-time transactions, global communication and market expansion for a wide range of industries. Businesses rely on data flows to manage customer interactions, optimise supply chains and effectively analyse markets. By streamlining operations and coordinating activities across borders, companies can drive innovation, enhance customer connections and improve operational efficiency.

In the financial sector, cross-border data flows are essential for processing international transactions and preventing fraud. For instance, when a customer uses a credit card abroad, the transaction data is sent back to the home country for verification to detect and prevent fraud. In another example, a bank might use cloud services to store and process customer data in multiple locations worldwide. This allows the bank to scale up its computing resources, handle market stress events and access cutting-edge technologies like data analytics and artificial intelligence.

Although the benefits of cross-border data flows are evident, the impact of geopolitics on data markets is becoming more pronounced. There is no comprehensive international legal regime on data governance, much less a consistent position on the flow of data between countries. In today's fragmented world, politics and geopolitics are increasingly influencing how governments view data governance and their approach to regulating cross-border data flows, creating a complex landscape for companies and countries alike.

This tension is most evident in the U.S.-China rivalry for digital leadership, which casts a long shadow over the Asia-Pacific. China has one of the most restrictive regimes on cross-border data transfers in the world. It asserts the central role of the state in regulating the flow and use of data. The government has strict compliance requirements for companies transferring large amounts of data out of China, including passing official security assessments and obtaining personal information protection certifications. For example, in 2022, China released its Measures for the Security Assessment of Data Export, stressing that cross-border data transfers should not endanger national sovereignty and security.

On the other end of the spectrum, the United States has historically promoted the free flow of data across borders, led by a business-first approach. However, recent policy shifts indicate it is moving towards a more restrictive data regime, driven by national security concerns. In February 2024, the executive order "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" was introduced, empowering the Department of Justice to identify countries 'of concern' and regulate or prohibit bulk data transfers to them. Soon after, Congress passed the Protecting Americans' Data from Foreign Adversaries Act, which restricts the transfer of Americans' sensitive information to certain countries for national security reasons. More bills are under congressional consideration that, if passed, would further restrict data transfers to foreign entities or governments.

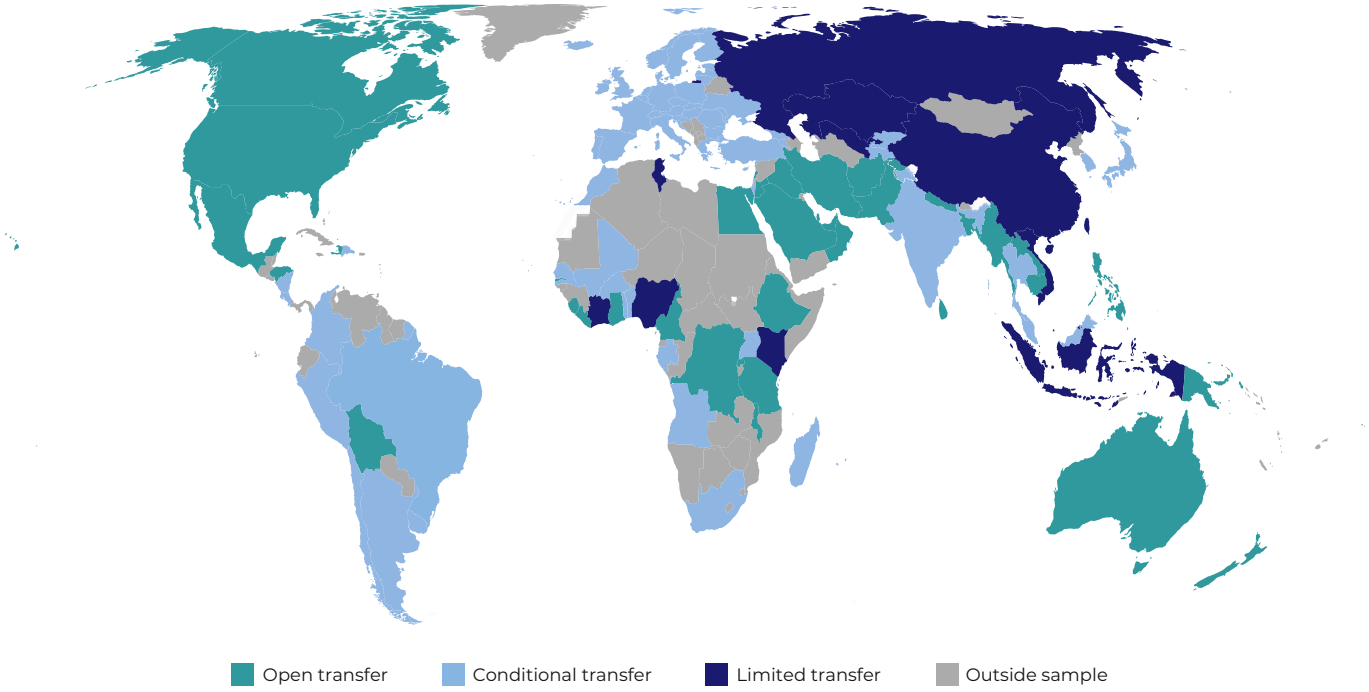
The 2023-2030 Australian Cybersecurity Strategy outlines measures to uplift data security, with a focus on protecting Australia's most critical and sensitive datasets. Reforms to the Security of Critical Infrastructure Act passed in November 2024 aim to ensure that critical infrastructure entities are protecting "business-critical" data storage systems. Reforms to the Privacy Act passed in November 2024 allows government to prescribe a "white list" of countries that provide substantially similar privacy protections to the Australian Privacy Principles. The intent is to enhance the free flow of information across national borders while protecting privacy of individuals. Additionally, entities are required to include additional information relating to automated decisions in an entity's privacy policy.

ASEAN finds itself in a delicate position amid escalating competition between China and the United States. Within the ASEAN regional grouping, a unified approach to data governance has not yet emerged, and individual countries have taken inspiration from the governance frameworks offered by Beijing and Washington. A few ASEAN countries have established mechanisms to encourage cross-border data flows; others have enacted laws protecting personal data and regulations, including data localisation requirments.

Numerous factors will feed into the future global framework for cross-border data. For one, it is evident that governments are increasingly prepared to intervene in data markets with data localisation laws or other regulations. This trend shows no signs of abating. Furthermore, diverging approaches to data governance highlight its fragmented and political nature. Countries and companies must now navigate a landscape where geopolitics and technology are intertwined and inseparable.

Recommendation: Companies should perform regular risk assessments to identify operational and geopolitical risks to their business. This process should include a thorough review of IT systems, business processes, business continuity plans, personnel and physical environments as well as compliance with all relevant data protection laws, regulations and standards applicable to their specific industry and jurisdiction. Risk assessments should be forward-looking, with the aim of understanding and being able to effectively respond to political and geopolitical developments that have an impact on data governance regimes.

Figure 1: The state of data transfer policies globally.[3]



Countries around the world broadly pursue three different approaches to cross border data: (1) open transfers of data; (2) conditional transfers; and (3) limited transfers.

Cross-border data flows are increasingly constrained by localisation policies and regulatory ambiguity

Companies face several challenges when transferring cross-border data to support their operations. The roundtable discussion touched on two salient issues:

1. The growing trend of data localisation policies.
2. Compliance challenges due to regulatory ambiguity.

There has been a strong trend towards data localisation policies in recent years, requiring data to be stored, processed and handled domestically. Although personal data regulations diverge widely, countries around the world are pursuing three broad approaches: open transfers of data, conditional transfers and limited transfers.

By early 2023, around 100 data localisation measures had been implemented across 40 countries, with over half introduced in the past decade. These measures are growing stricter, with more than two-thirds now combining storage mandates with restrictions on data transfers.[1]

Data localisation regimes are driven by both economic and non-economic reasons. The non-economic drivers are generally political and security in nature, such as concerns about safeguarding national security, digital sovereignty, cybersecurity, data privacy and assisting law enforcement (domestic surveillance). The economic driver is a form of protectionism which aims to provide an enabling environment for local players free from outside competition. However, while limiting competition, data localisation also limits citizens' access to foreign services that may be cheaper or whose equivalents are not available in the domestic market.

Although governments justify localisation measures to protect national security and support local industries, the measures impose significant costs. Multinational corporations face up to 30 percent higher operational expenses due to compliance burdens and redundant infrastructure.[4] One roundtable participant described data localisation policies as crippling the backbone of the digital economy. Furthermore, according to the World Bank, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services."[5] Small and medium-sized enterprises (SMEs), in particular, which lack the resources to comply with these rules, are effectively excluded from global markets.

Localisation can impair or actively undermine national security objectives. For instance, data localisation can increase the risk of data breaches and impact privacy because the data is more accessible and centrally stored, making it easier for hackers to locate and access sensitive data.

India has implemented data localisation rules, such as the Reserve Bank of India's mandate requiring all payments data, except for the foreign leg of transactions, to be stored domestically. Framed as a national security measure, this

approach also serves to promote the local technology infrastructure. However, these policies risk isolating India from global digital ecosystems, limiting its access to international markets and innovation.

For its part, Indonesia is shifting from strict localisation to a more pragmatic stance. The country initially enforced data localisation laws to ensure national control but has begun easing restrictions to attract investment in cloud computing and digital services. This approach reflects an effort to balance economic growth with sovereignty, signalling the potential for greater regulatory flexibility.

Regulatory ambiguity is another significant challenge for companies. This may occur for various reasons, such as differing interpretations of standards and definitions or deliberate ambiguity by the regulating authority. As stated by a forum participant, two different lawyers could have very different interpretations of data regulations. One person might take a more conservative approach, while another adopts a more risk-tolerant stance. An established baseline understanding of principles and good practices between industry and regulators is needed. Improving the compatibility of cross-border data transfer frameworks would enhance legal certainty and give greater confidence to the industry.

Regulatory ambiguity may also be a result of conflicting guidance provided by regulatory authorities. This can occur for several reasons. It can be in part a byproduct of the "law lag" and the rapid pace of developments in the technology sector. When new disruptive technologies are introduced, a period of adjustment is needed as regulators play catch-up. Because multiple government agencies may be involved in the management of cross-border data, an overlap in responsibilities and a lack of coordination can lead to inconsistent and ambiguous policy positions towards cross-border data. Also, governments may often lack the necessary human resources to design, implement and monitor data policies. Multilateral cooperation and the development of regional standards can help to address these challenges by providing a shared framework to guide national policies.

> **Recommendation:** To address these challenges, governments should adopt balanced localisation approaches that account for both national interests and economic priorities. Policies should be designed to minimize unnecessary compliance burdens, particularly for economies driven by small and medium-sized enterprises, and avoid isolating countries from regional or global innovation ecosystems

For businesses, collaborating with regulators to establish baseline standards and good practices is critical to navigating inconsistencies or conflicting rules. Clearer regulatory frameworks, supported by regular dialogue between stakeholders, will help ensure that data governance promotes economic growth without compromising security.

Aligning national priorities with regional data governance standards

The Asia-Pacific's fragmented data governance policies reflect a tension between national priorities and the economic benefits of cross-border data flows. Although countries in the region seek to maintain control and protect domestic interests, excessive localisation and divergent regulations and standards are creating inefficiencies. Leaders need to strike a balance between promoting economic development, protecting public policy interests and integrating into the global and regional digital ecosystem. As a first step, a regional consensus is critical for all to benefit from cross-border data flows.

At the regional level, ASEAN's Digital Masterplan 2025 provides a roadmap for harmonising data governance frameworks among member states. In addition to the masterplan, ASEAN member states are currently negotiating the ASEAN Digital Economic Framework Agreement (DEFA), of which a key pillar is cross-border data flows and data protection. DEFA aims to create a unified regulatory regime that facilitates cross-border data flows and addresses various aspects of digital trade, including cross-border e-commerce, cybersecurity, digital ID, digital payments and cross-border data flows.

ASEAN member states have agreed that DEFA will be legally binding, requiring each country to adjust and implement domestic policies accordingly. The challenges are in finding common ground and in reaching an agreement among domestic agencies to implement DEFA commitments effectively. Tailored support and assistance from developed economies will be necessary to address the different levels of digital economy readiness among the ASEAN countries.

ASEAN's DEFA represents a promising step towards regional alignment. Broader frameworks like the Asia-Pacific Economic Cooperation (APEC) forum's Cross-Border Privacy Rules (CBPR) extend its efforts by promoting trust and reducing compliance burdens across a wider region. While DEFA focuses on harmonising cross-border data flows within ASEAN, CBPR, as a neutral framework, complements these

efforts by enabling mutual recognition of privacy standards among APEC economies. For instance, economies like Japan and Singapore, which are part of both frameworks, can act as bridges to facilitate greater integration between ASEAN and APEC. Both frameworks could help ASEAN economies participate more effectively in data ecosystems while upholding stringent privacy standards.

Governments could also explore engaging in "stand-alone" digital trade agreements, which are typically simpler and more focused on negotiating compared to broader, comprehensive trade deals. For instance, the 2020 Australia-Singapore Digital Economy Agreement (DEA) prevents unnecessary restrictions on the transfer and location of data to support businesses operating between Australia and Singapore, including in the financial sector, to transfer data and to not be required to store it in either jurisdiction. None of the provisions in the DEA affect the ability of Australia to enforce regulations on privacy.

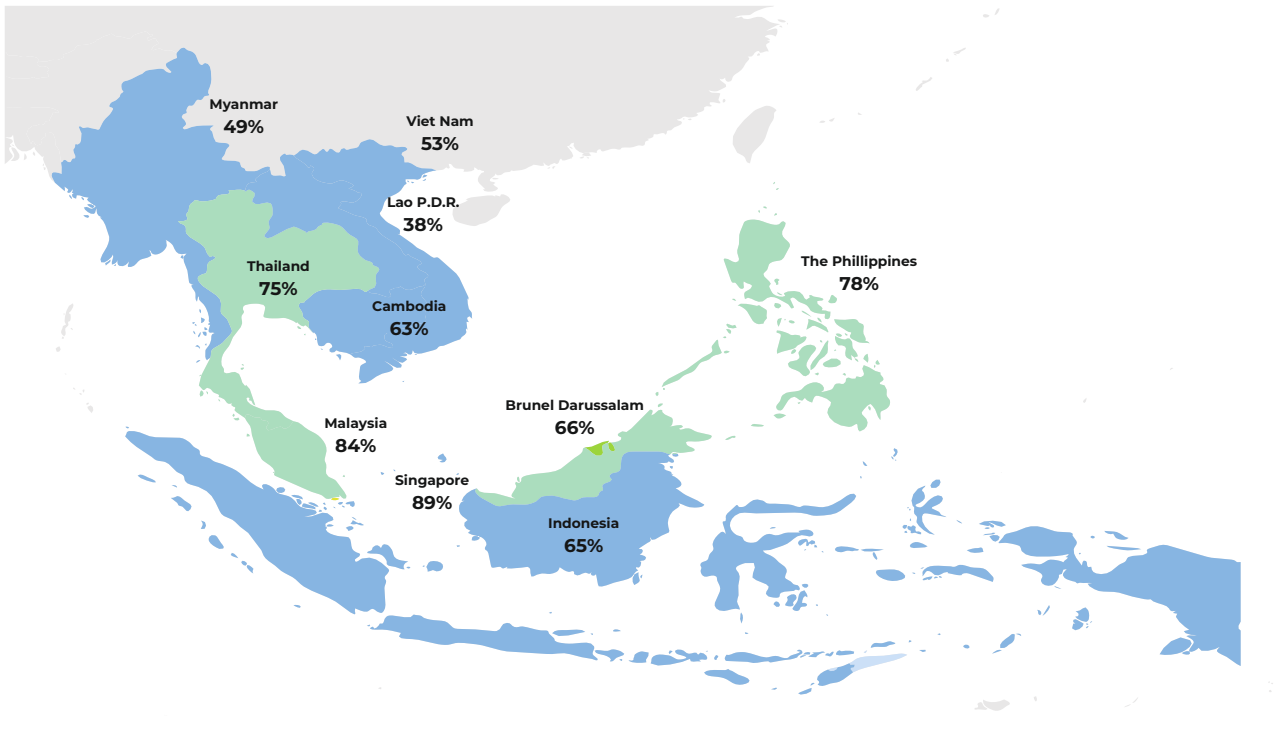
Another such agreement is the Digital Economy Partnership Agreement (DEPA), originally signed by Chile, New Zealand and Singapore, with South Korea joining as the fourth member in May 2024. DEPA serves as a forward-thinking platform that fosters international collaboration on digital trade and innovation. One of DEPA's key initiatives includes the development of data regulatory sandboxes, which create controlled and secure environments where companies can test and refine innovative technologies and business models. These sandboxes allow for close collaboration between businesses and governments, ensuring that innovation occurs within a framework of trust, compliance and shared learning. This targeted approach to digital trade agreements not only accelerates progress in the digital economy but also provides a foundation for more complex and comprehensive trade negotiations in the future.

> **Recommendation:** Governments in the Asia-Pacific should prioritise the implementation of regional frameworks like DEFA and CBPR to harmonise data governance standards and reduce inefficiencies caused by divergent and fragmented policies. In parallel, countries could also explore bilateral digital trade agreements, which offer a pragmatic pathway to advance digital trade collaboration without the complexities of broader trade deals.

For ASEAN member states, ensuring that DEFA commitments are upheld requires robust domestic implementation complemented by regional enforcement mechanisms. This dual approach can strengthen trust in cross-border data flows while fostering an environment conducive to innovation and growth.

To achieve these goals, digitally advanced economies should take a leadership role in supporting less digitally mature nations. This includes providing technical expertise, capacity-building programs and guidance on establishing resilient data governance frameworks and best practices. By empowering all economies to participate effectively in multilateral frameworks and agreements, including stand-alone digital trade pacts, the region can advance towards a cohesive, inclusive and dynamic digital economy that balances innovation with regulatory alignment.

Figure 2: The state of digital transformation in ASEAN.[6]



Role of technology in addressing cross-border data challenges

Technological innovations, driven by public and private sector efforts, offer significant potential to address cross-border data challenges. Combining the technical expertise of industry leaders with the vision and direction of government policies offers an opportunity to deliver solutions that enhance privacy, improve regulatory compliance and advance economic integration without compromising national priorities.

Blockchain, for example, shows potential for improving transparency and security in cross-border data sharing by creating verifiable, tamper-proof systems for trade, payments and logistics.

The use of tokenization in digital payments — a security measure that replaces sensitive payment information, such as credit card numbers, with an algorithmically generated set of numbers and characters called a "token" — has led to a 28 percent reduction in fraud for Visa.[7]

Artificial intelligence-driven tools are being used to automate compliance with complex regulatory requirements and reduce operational inefficiencies for businesses managing data across multiple jurisdictions.

There is also potential in the use of synthetic data — artificially generated data that mimics the characteristics and patterns of real-world data without containing any personally identifiable information. Companies can gain valuable insights by analysing the data without the limitations and risks associated with using real data.

Privacy-enhancing technologies (PETs) complement these solutions by enabling secure data processing without violating privacy regulations. In July 2022, Singapore's Infocomm Media Development Authority launched a sandbox for businesses to trial PETs in a real-world environment. PETs enable secure analysis of financial data across jurisdictions to detect fraud while complying with strict privacy laws. This highlights how advanced technology can support critical cross-border data usage while ensuring compliance with national data protection regulations.

Technology can provide tools to address cross-border data challenges, but its successful deployment depends on collaboration and sustained dialogue between governments and the private sector. By pooling resources and sharing expertise, these partnerships can accelerate the adoption of technologies that align with regulatory requirements, enabling secure cross-border data flows.

Public and private sector collaboration facilitates international cooperation by aligning technological solutions with global best practices. Governments can establish interoperable standards that reduce compliance burdens, while the private sector can provide the technical expertise needed to implement these standards securely. This partnership model not only addresses immediate regulatory challenges but also enables free and secure cross-border data flows that might otherwise exclude many businesses and economies from global markets.

Recommendation: As an initial step, governments and industries should establish a framework for regular, structured dialogues to discuss emerging technologies, their potential benefits, associated risks and strategies for mitigating those risks. These discussions will foster mutual understanding, build trust and create opportunities for collaboration in navigating the rapidly evolving technological landscape.

References

1. Cross-border data flows. OECD. Accessed January 31, 2025. https://www.oecd.org/en/topics/sub-issues/cross-border-data-flows.html

2. Diburga LS, Yan Xiao. Unlocking Interoperability: Overcoming Regulatory Frictions in Cross-Border Payments. The World Economic Forum; 2023. Accessed January 31, 2025. https://www3.weforum.org/docs/WEF_Unlocking_Interoperability_2023.pdf

3. Ferracane, MF, van der Marel, E. "Regulations on Personal Data: Differing Data Realms and Digital Services Trade." World Bank; 2021. Accessed January 31, 2025. https://wdr2021.worldbank.org/stories/crossing-borders/

4. Wu E. Sovereignty and Data Localization. Belfer Center for Science and International Affairs. Belfer Centre; June 2021. Accessed January 31, 2025. https://www.belfercenter.org/publication/sovereignty-and-data-localization

5. World Bank. World Development Report 2020: Trading for Development in the Age of Global Value Chains. World Bank; 2020. Accessed January 31, 2025. https://www.worldbank.org/en/publication/wdr2020

6. Digital policy action areas for a connected ASEAN. ITU Publications; 2024. Available from: https://asean.org/wp-content/uploads/2024/03/Digital-Policy-Action-Areas-for-a-Connected-ASEAN.pdf Accessed January 31, 2025.

7. Visa Tokens Surpass Physical Visa Cards in Circulation. Visa. Published August 24, 2022. Accessed January 31 2025. https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.19116.html

Global Finance &
Technology Network (GFTN)

89 Neil Road, #02-04, Singapore 088849
gftn.co | hello@gftn.com