WORLD ECONOMIC FORUM

Advancing Data Flow Governance in the Indo-Pacific:
Four Country Analyses and Dialogues

WHITE PAPER

APRIL 2021

Cover: Getty Images/Gremlin
Inside: Unsplash/Markus Spiske; Getty Images/XtockImages; Getty Images/Fevziie Ryman; Getty Images/Tero Vesalainen; Getty Images/DragonImages; Getty Images/Oatawa; Getty Images/Oatawa

Contents

Foreword

Data flow governance is challenging as it takes place at the domestic, regional and global levels. The World Economic Forum provides a platform for discussions on best practices.

Børge Brende
President,
World Economic Forum

The digital revolution was accelerating rapidly even before the COVID-19 pandemic. The difficult events of the past year have served to reinforce the importance of technology in people's lives. Data flows underpin the diffusion of advanced technologies, bringing economic benefits, innovation, societal advances and human connection.

Many countries are working to create or update data governance frameworks. The wide range of approaches taken is making it increasingly difficult to move data across borders. However, a number of best practices are beginning to emerge that ease data transfers, while maintaining governments' ability to regulate.

The World Economic Forum has been working to engage stakeholders on complex data flow governance questions for several years. Our community has provided insights in discussions on new global digital trade rules and regional initiatives, such as the development of an ASEAN cross-border data flow mechanism and inputs to World Trade Organization negotiations. Most recently, it has been our privilege to organize workshops on data transfer governance and digital growth in India, the Philippines, Thailand and Viet Nam. We have reviewed national data policy developments and identified avenues for facilitating data transfers.

We believe that by taking account of both international and domestic perspectives, a workable balance can be found for effective data governance. This White Paper summarizes the materials prepared for each workshop as well as highlights from the discussions. We hope that the material can be a useful reference for data flow governance debates, particularly from an economic development perspective.

The Forum is grateful to various government partners that collaborated in organizing the national workshops as well as to our group of global and regional experts for thought leadership. Policies to ensure that digital economy opportunities are widely shared are essential now, more than ever. As the digital world continues to rapidly evolve, getting these settings right will inevitably be a process of continuous exchange between and across nations.

Executive summary

Data governance has become increasingly important as digitalization accelerates. Countries must engage in a series of balancing acts and need to determine priorities for cooperation with each other to encourage trade and investment.

As part of its efforts to engage stakeholders on complex data flow governance questions, the World Economic Forum organized four workshops over a four-month period from December 2020 to March 2021 on data transfer governance and digital growth in India, the Philippines, Thailand and Viet Nam. Each nation has a different context for cross-border data flows in legislation and in practice.

India has pursued important public digitalization programmes, and the use of digital tools is growing. Data can drive industrial transformation and bring societal benefits. The business environment will benefit from a pending Personal Data Protection Bill (PDPB), although it includes provisions that present major barriers to international services trade and could possibly hamper the use of some digital transformation tools in-country.

Workshop leaders noted that Indian digital services exporters do not face significant challenges in accessing the US market, though that could change in the future. Firms also seem comfortable assuming compliance with European Union rules, but such self-determination leaves a degree of uncertainty. Several participants encouraged India to develop a strategy to engage with trade partners – perhaps initially via bilateral or regional routes. The establishment of a single data protection authority under the PDPB may facilitate India's global engagement on these issues.

The Philippines has a history of creating a balanced regulatory environment that allows data to flow while requiring accountability for controllers and processors regardless of location. New barriers to data transfers from the Philippines could nonetheless emerge in areas like government-related data and linked to cybersecurity concerns.

More capacity building is also needed in the country to ensure small businesses use data transfer mechanisms for digital services exports. For example, one or more accountability agents for Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) certification must be established, which will help compliance with privacy rules in large neighbouring regional markets. The Philippines also needs to build up data privacy, cybersecurity and related skill sets since these are currently hard to hire in-country.

Thailand has a vibrant digital economy, particularly in the area of e-commerce, and many new internet users who prioritize mobile usage over fixed-line internet use. Digital tools have enabled some resilience for business and consumers alike in the face of the coronavirus pandemic. Concerns over the costs of implementing the Data Protection Act caused its delay for a year, but moving ahead will be important to raise systemic trust.

The country has much to gain from joining international forums on privacy enforcement and cooperation as these will encourage digital trade in services. Thailand can apply best practices to strike a balance between protecting and securing data while encouraging investment and trade. Workshop participants encouraged the country to join the APEC Cross-border Privacy Enforcement Arrangement (CPEA) as a required precursor for offering CBPR certification.

Viet Nam is among the world's fastest growing economies. Global trade has been a part of its success, and digitalization will now be key to maintaining the country's competitiveness as a regional hub. The government is pursuing a National Digital Transformation Roadmap, and COVID-19 has accelerated the use of digital tools, many of which are underpinned by data. Viet Nam needs to finalize a cross-cutting data privacy law.

Workshop panellists commended the government for recognizing the importance of digitalization and taking action to support it, particularly for small businesses. Digital growth has been substantial, but there is room for more. Participants agreed cross-border data flows need to be facilitated to encourage further digitalization. Getting the regulatory landscape right is a challenging task. Several participants suggested the government has made good strides in areas like financial inclusion, whereas certain policies on e-commerce and data could benefit from insights from international best practices.

1 Introduction

Multistakeholder discussions took place in workshops in India, the Philippines, Thailand and Viet Nam on designing data transfer policies for growth and development.

Massive volumes of data move across borders daily to support economic activity, value chain functioning, research and human connection. Continuing to facilitate data flows must be a priority as digital economy regulation evolves, particularly now amid the COVID-19 pandemic, during which transacting online has become the new normal for many.

During the World Economic Forum Annual Meeting 2019 in Davos-Klosters, then Japanese Prime Minister Abe Shinzo shared a vision in which openness to data flows co-exists with confidence in data treatment, access and usage when it is abroad – a concept known as "data free flow with trust" (DFFT). The Forum subsequently convened 30 leading experts from business, academia and international organizations to map existing policies relevant to data governance and propose practical paths for collaboration.[1]

The Forum then moved into a process of (virtual) national dialogues on data flow policies, selecting economies at various stages of digital transformation and policy-making. These included the Philippines, Thailand, India and Viet Nam. The initiative also builds on engagement with ASEAN Member States on a new regional data transfer mechanism. The theory of impact creates a flow between national priorities and regional and global cooperation (see Figure 1). In total, the four dialogues involved over 250 participants, representing public, private, academic and civil society organizations. The Forum collaborated directly with government partners or local institutional partners for each workshop.

FIGURE 1 **Theory of impact**

Source:
World Economic Forum

This White Paper summarizes the briefing materials prepared for the workshops and provides discussion highlights. The briefing materials have been edited from the original versions, which can be requested from the World Economic Forum.

The Forum is grateful for and recognizes the contributions made by a group of global and regional experts as part of its data flows governance community alongside staff at its Centres for the Fourth Industrial Revolution Japan and India.

2

India

India has much digital potential, though stakeholders are concerned about the effects of new rules on data transfers. The country may wish to develop a strategy for international engagement on these topics, starting at the bilateral and regional levels.

2.1 Context

A growing digital market

India is the world's largest consumer market in terms of population, dominated by young people, and it is also steadily growing in economic importance. Although the digitalization of India's economy was initially slow, demand is now growing rapidly, and average mobile data usage is higher than in China and the Republic of Korea thanks to falling costs.[2] Yet, half the country remains unconnected, with full internet access not foreseen until beyond 2025. Rural and gender digital divides are manifest[3] and the average revenue per user is one of the lowest in Asia.[4]

Government of India initiatives are focused on building public service infrastructure for the domestic digital economy to thrive. The flagship Digital India government programme, started in 2015, aims to improve internet access, standardize identity and payments and generally improve digital literacy.[5] Aadhaar, biometrically enhanced digital government IDs, was launched in 2009 and underpins the growth of many new services from digital payments to delivery of public services.[6] Similarly, the government's mass financial-inclusion drive, Pradhan Mantri Jan-Dhan Yojana, has enabled millions to open Aadhaar-linked mobile banking accounts.[7]

Digital trade potentials

In certain parts of the economy, India is already a leader in digital exports. Business services and information and communications technology (ICT) represent the lion's share of India's services trade, equal to 45.1% of the total in 2019/2020, led by a strong information technology and business process management (IT-BPM) sector.[8] Revenues for the latter were $167 billion in 2017-2018 and could reach between $280-350 billion by 2025.[9] The sector directly employs 4.1 million people and indirectly supports 10 million jobs. India's top business and ICT services export markets are the United States, the United Kingdom, Singapore, Germany, the Netherlands and Switzerland.[10]

The IT-BPM boom has led to broader benefits. Telecommunications services providing interconnection for videoconferences, digital file sharing and data processing were estimated at around $50.6 billion in 2017.[11] It has also spurred investment, particularly as India has gradually opened up, now permitting 100% foreign equity in areas like telecommunications services and business-to-business electronic commerce activities.[12] The majority of India's foreign investment flows in 2019 went to the ICT and construction industries.[13] The Prime Minister's Atmanirbhar Bharat or self-reliant India campaign is designed to boost investment in India's IT sector through a production-linked incentive scheme for large-scale electronics manufacturing.

India has other digital strengths too, such as a significant public cloud market estimated at $2.6 billion in 2018, and forecast to grow to $8 billion by 2023.[14] The country is likely to emerge as the world's sixth largest over-the-top streaming market by 2024, using digital distribution to leverage music and entertainment talent.[15] Online advertising revenues from foreign markets associated with India-based content were estimated at $99 million in 2017 and could grow ten-fold by 2030.[16] Some Indian businesses use e-commerce platforms to export goods, though the share is lower than elsewhere, in part due to fewer Indian businesses tapping trade opportunities. Nonetheless, today over 27% of Indian businesses receive orders via the internet, suggesting strong growth potential·

Deploying data benefits broadly

A headline government objective is to generate $1 trillion in economic value using digital technologies across sectors by 2025 – up from a digital economy worth around $200 billion currently, according to a report commissioned by the government.[17] India's thriving and strategically important agricultural sector is an important case for digitalization. Real-time data on crop prices from international and local sources combined with algorithm analytics can improve demand forecast and pricing. Highlighting another example, from the logistics sector, a joint venture between the Government of India and Japanese-IT firm NEC Corporation created a Logistics Data Bank System, providing export-import container visibility along the Western corridor of India.[18]

Nevertheless, the integration of digital technologies is still in its early stages in many manufacturing and industrial processes. An Ernst & Young study found that 60% of Indian manufacturers surveyed had a broad understanding of digital manufacturing, but only 20% had a clear digital strategy and defined budget.[19] A KPMG-CII report identified the lack of trained professionals and of high-quality data as well

as regulatory uncertainty as the main roadblocks for the industry's uptake of advanced technologies.[20]

Small businesses face particular constraints around investing in new technology and digitalization – a trend replicated across the region. According to one survey, only 16% of Indian small business respondents were making investments in cloud tech (compared to a 15% regional average), 13% in security (compared to a 12% regional average) and 12% in upgrading IT hardware (compared to a 12% regional average).[21]

Regulatory developments

Interest in privacy protection in India has increased as digitalization has spread. Discussions on privacy rights under existing laws,[22] global developments and insufficient cybersecurity measures have led to calls for more specific legislation. The Personal Data Protection Bill (PDPB 19), introduced in parliament in December 2019, is currently under consideration.[23] Under the proposal, data transfers abroad may take place under a tiered system whereby personal data can be transferred, while "sensitive data" for processing may be transferred with prior authorization by a Data Protection Authority (DPA) and with a mirror copy remaining on soil. "Critical personal data" with bearing on India's security interests (to be defined by the central government) must be stored and processed locally.

The prospect of a Personal Data Protection Bill has been much debated in India. Supporters of the bill point to the individual rights granted, such as for data to be deleted if improperly collected, and penalties for reidentification of de-identified data.[24] Critics of the bill have raised privacy concerns and risks of government control. The bill's limitations on data processing could result in productivity losses if compliance slows the use of big data or artificial intelligence (AI) services.[25] Several domestic and international industry groups have raised concerns around the localization requirements.

Exchanges around the PDPB 19 have also led to discussions on non-personal data governance. In December 2020, a government-appointed committee of experts proposed a framework for government access to non-personal data held by private entities.[26] Several of the recommendations in the latter may raise complications for businesses operating in India.

Reducing barriers abroad

According to a survey sample of 225 companies from a variety of sectors, all located in one of India's six major metropolitan cities, around 32% of the businesses reported being affected by data localization measures in export markets such as the United Kingdom, United States, China, the Republic of Korea, the European Union (EU), Canada and Australia.[27] Yet a significant number of firms indicated that foreign regulations demanding local storage but not restricting data transfers or restricting to countries with recognized privacy standards would not affect data management or ICT costs.

Another recent study models the impact on digital services exports of a rise in data transfer restrictions across the world.[28] Losses for India could be between $19 billion and $36 billion by 2025, spread across exports, investment, productivity and worker income. Increased or reciprocal data restrictions against Indian businesses by the EU and the US could result in a 10.6% drop in digital services exports, while restrictions present in all trading partners (excluding the EU) could result in an 18-19% drop.

Although much of the friction around data transfers and compliance with rules in foreign markets relates to personal information protection, policy evolutions could see a greater degree of restrictions arising related to non-personal data (including internet of things and machine-to-machine data), as may be the case in India itself. Further, an aspect less discussed is how data rules at home and abroad affect digital services imports used for industrial transformation or societal benefits. Imported digital services alone are estimated to add $3.3 billion to economic sectors in India.[29]

Options for collaboration

India has been an observer of the APEC CPEA since November 2011. India's bid to join APEC, however, is not moving forward at this stage. The PDPB 19 also does not envisage data transfers taking place on the basis of an approved certification scheme, though it is conceivable that a bilateral agreement could be justified under approval from the DPA.

In other cases, countries have used FTAs to align on parameters for privacy protection and interoperability. The India–Singapore Comprehensive Economic Cooperation Agreement highlights both the importance of privacy protection and that this not become a means of arbitrary discrimination or disguised restriction on trade. The

Japan–India Comprehensive Economic Partnership Agreement contains similar provisions and pledges not to restrict information transfers around financial services necessary to conduct business. For now, India is not participating in the recently signed RCEP between ASEAN and its trading partners that includes an e-commerce chapter.

Some countries offer data transfer templates that operate on a business-to-government basis. The prevalence of the EU's standard contractual clauses (SCCs) has created a degree of interoperability for multinationals that use these across their networks.[30] The new ASEAN MCCs offer another template, but are different from the SCCs since the latter are set out as a transfer option in EU laws while and ASEAN Member States are at varying stages of data policy development.[31] Under PDPB 19, sensitive personal data may be transferred for processing where a contract makes provisions for effective protection and liability in the case of non-compliance. Further, intra-corporate transfers of sensitive personal data could be made subject to a scheme approved by the new Indian DPA, that may be analogous to Binding Corporate Rules, another EU transfer option.

The possible development of a DPA could see India more readily equipped to participate in international forums such as the GPA (where India is currently an observer) or the GPEN. Exchanges in these regulatory cooperation forums could provide a stepping stone for interoperability on privacy, though not on other policy areas and questions. India may also wish to explore data transfer cooperation within the ASEAN–India strategic partnership dialogues that see senior officials meet on a regular basis.

2.2 Highlights

Panellists described the uptake of digital tools by Indian businesses and society, and policy strategies to encourage further adoption. Digital tools from the private sector have complemented government-led initiatives in education, agriculture and health that "create wealth at the bottom of the pyramid". The participants identified use cases where India can benefit from data, including in the manufacturing sector, where growth has slowed.

The discussion then shifted to the dynamics between domestic rules and international regulatory cooperation. One panellist stated that India is "ready" for a data privacy protection regulation, noting that large firms already comply with the General Data Protection Regulation (GDPR), and SMEs are working towards compliance. The participant also said that India should take positions based on its own interest and develop a strategy for engagement with international negotiations, although it need not immediately come to agreement with partners. Potential strategic partnerships for data sharing with Japan and Africa were raised.

A participant commented that any privacy regulation should distinguish between non-sensitive data and sensitive data (financial, healthcare) and should provide for a degree of flexibility, which COVID-19 has shown to be useful. Panellists emphasized the centrality of data flows to services exports and noted that stricter regulations on data flows abroad could negatively impact exports. Indian firms have not to date faced significant challenges in exporting digital services to the United States. Panellists also noted that firms seem comfortable in assuming compliance with the EU GDPR, although such self-determinations leave a degree of uncertainty.

India's international engagement with privacy forums and data transfers is expected to evolve once the PDPB 19 is in place. Some participants said they view bilateral and regional frameworks as more realistic than global ones, while one identified the WTO as an appropriate place for multilateral negotiations.

3 Philippines

The Philippines has a relatively open approach to data transfers, but greater capacity building for small business could help encourage digital exports.

3.1 Context

Consumer opportunities, digital services trade

The Philippines' digital economy is on track to significantly expand, by as much as 30% between 2020 and 2025, according to one survey.[32] It is seen as among those with the most room for growth among South-East Asian economies, accounting for 2.1% of GDP in 2019[33] and expected to hit 5.3% in 2025. COVID-19 has expanded the user base of online services by around 76%, driven by e-commerce and food delivery services.[34]

More generally, the digital services trade has been a growth engine for the country, backed by data flows. The Philippines is one of the top global locations for IT-business process outsourcing (IT-BPO) and is particularly dominant in high-end segments such as legal process outsources. The sector generates approximately $25.5 billion annually and employs 1.4 million people.[35] Data flows also underpin remittances – the country's largest source of foreign exchange income. The broader digital transformation of economic activity, meanwhile, could add up to $8 billion to the Philippines' GDP and increase the growth rate by 0.4% annually.[36]

A regional front-runner in privacy rules

Privacy rules are an important part of data transfer governance discussions since they are typically where most compliance efforts are required or where like approaches are sought. The Philippines enacted a Data Privacy Act (DPA) in 2012 that is enforced by the National Privacy Commission (NPC). The NPC issued Implementing Rules and Regulations of the DPA in 2016 (DPA IRR). The government recently launched a major campaign to increase awareness and improve rule enforcement on how data is collected and used and the corresponding risks.

The DPA allows international data transfers out of the Philippines, provided the controllers of personal information ensure compliance with the law.[37] The DPA, however, was primarily designed to boost the country's competitiveness as a business processing outsourcing hub by providing a legal framework offering assurance to trading partners of personal information treatment within the country.

Regulatory cooperation, trade commitments

One of the NPC's roles is to ensure coordination with privacy regulators in other countries and to participate in regional and international initiatives for data privacy protection.[38] The NPC signed its first cooperation agreement with another privacy enforcement authority (PEA) in September 2019 through a Memorandum of Understanding with Singapore's Personal Data Protection Commission (PDPC).[39] It involves sharing information and best practices on data protection as well as mutual assistance on privacy enforcement. Separately, Bangko Sentral ng Pilipinas (BSP) and the Monetary Authority of Singapore (MAS) recently issued a statement of intent to promote data connectivity in the area of financial services.[40]

The DPA does not explicitly outline other types of transfer mechanisms. Implicitly, the use of a data subject's consent for transfer is not required, but it could be used as an option. The use of contractual safeguards is likely another possibility. The DPA and the IRRs specify data protection requirements for outsourcing agreements, whether for commercial data sharing or for processing. The use of binding corporate rules, for transfers within a company across borders, is a conceivable transfer option to assure comparable protection, but is also not explicitly mentioned. Codes of conduct are mentioned but with no indication of how they might apply in the context of transfers. No reference is made to adequacy or white lists.

The Philippines is a member of the ASEAN Economic Community that has agreed to develop a regional cross-border data transfer mechanism as part of its Digital Data Governance Framework. The mechanism will include model contractual clauses (MCCs) and ASEAN certification (of compliance) and thus offers a couple of other types of data policy transfer mechanisms. These were adopted by ASEAN Member States in January 2021.

The country participates in the Regional Comprehensive Economic Partnership (RCEP), a major initiative between ASEAN and its six free trade agreement (FTA) partners. That includes an e-commerce chapter that requires parties to adopt or maintain a framework to ensure the protection of e-commerce users' personal information and pledges to cooperate in these areas.[41] The chapter equally commits to not requiring data localization as a condition of business, and similarly to not preventing

cross-border information transfers for business purposes, with both provisions accompanied by exception clauses for legitimate public policy objectives. Several RCEP parties have been given more time to implement these commitments.

The Philippines is also participating in plurilateral negotiations on e-commerce at a global level via the World Trade Organization (WTO). Several proposals on data flows, personal information protection and related areas have been tabled. The Philippines is not part of, but has expressed interest in, the 11-nation Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) that includes commitments on privacy protection, data flow for business purposes and other digital policies.

Data flow policy challenges

Digital tools have a lot of room for growth in the Philippine economy and the impact could be transformational. Yet, a number of sources align on key challenges to be solved in the next decade, including improving internet infrastructure; increasing (and maintaining) consumer trust; attracting talented digital economy professionals; developing efficient and innovative logistics networks to support e-commerce across thousands of islands; developing policies to support the wider use of digital payments; strengthening policies related to cybercrime; and securing sufficient venture capital investments to fund the internet economy. The way that data is handled and processed, in and out of the country, will affect many of these objectives.

The DPA IRRs require a number of compliance actions when controlling personal data in the Philippines[42] or in cases significantly related to the country. When initially rolled out, some domestic firms were not clear on the requirements, not having previous experience with such laws. Consumers in the Philippines are also growing wary of transacting online despite the engagement.

The Philippines' application to join the APEC CBPR system was approved on 9 March 2020. CBPRs allow for multi-country certification of compliance with privacy requirements and thus streamline the movement of data. Nine APEC economies currently participate in the system.[43] The NPC must identify an accountability agent, who can independently assess and certify compliance to CBPRs by Philippine companies. For the handling of Philippine data, the NPC has recognized APEC CBPRs as a mechanism whereby a controller can demonstrate comparable levels of protection when information is processed by a third party abroad.

3.2 Highlights

Workshop participants highlighted the importance of data flows. For its part, the IT-BPO industry has faced challenges since 2016 due to geopolitical tensions as well as a complex legal and regulatory landscape. The shift towards data localization in some markets is perceived as a barrier for Philippine services growth.

Participants also flagged the attention paid to cyberthreats by policy-makers and business. Digital services have surged during the COVID-19 pandemic, but so too have consumer complaints and risks. There was broad agreement among participants that effective public-private sector collaboration could increase cybersecurity readiness and build small business capacity. Small and medium-sized enterprises (SMEs) need help to implement data best practices and to understand the consequences of not being data compliant. There is insufficient cybersecurity expertise within the Philippines, making it a difficult hiring area.

One of the breakout groups focused on potential data localization requirements for certain types of government data. Some participants expressed surprise since the Philippines has to date had a relatively open approach to data transfers. Several participants suggested clarifying when data localization should take place, if at all, and with what impacts. They agreed that the intertwined relationship between cybersecurity and data protection affects consumer-to-business and government-to-government trust. Other participants raised issues regarding transferring sensitive financial data and called for greater efforts to reassure regulators so as to deliver important financial inclusion goals.

Some participants described the different ways transfer mechanisms could play out for Philippine businesses of varying sizes, focusing on ASEAN MCCs, APEC CBPR for data controllers and the APEC Privacy Recognition for Processors (PRP). The PRP system has 18 requirements compared to the CBPR system that has around 50. Several participants suggested that the Philippines submit a letter of intent to join the PRP, as has been done with the CBPRs, because these more directly benefit and are accessible to smaller IT-BPO firms.

One panellist recommended following a private-sector approach for CBPR accountability agents as has been done by the United States to meet demand. Using a private-sector model could create

competition and reduce the cost of certification, which would be very helpful for smaller businesses.

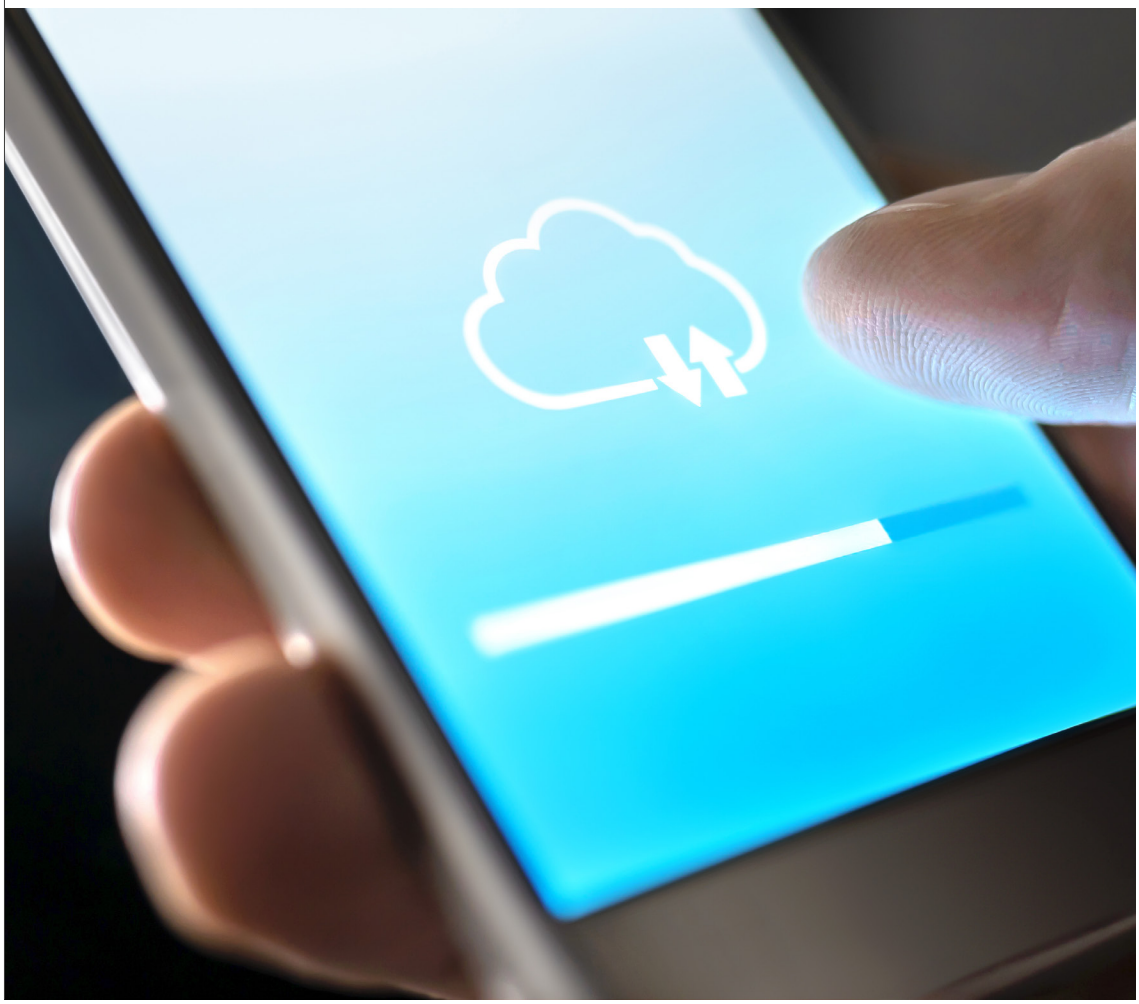
Some participants suggested that ASEAN MCCs would be important for growing regional business for the Philippines. The MCCs are designed to simplify data protection arrangements and reduce lengthy contract negotiations for companies trading overseas. During the breakout group discussions, however, some participants questioned how much MCCs would streamline business contract negotiations since ASEAN countries' privacy regulatory frameworks still vary greatly.

New bilateral and plurilateral agreements were perceived as good opportunities for additional cooperation. The Philippines could, for example, consider joining a Digital Economic Partnership Agreement led by Singapore, Chile and New Zealand.

4

Thailand

The implementation of Thailand's privacy law could support its participation in regional and international forums to learn best practices on data transfer mechanisms. This would help accelerate digital trade and investment.



4.1 Context

Rapid digitalization

Internet penetration in Thailand is one of the highest in South-East Asia at 75% in January 2020,[44] while partnerships between Thai authorities and tech companies are seeking to further reduce disparities in digital literacy, skills and connectivity by providing training programmes and free Wi-Fi hotspots.[45] A digital divide persists, though, between urban centres and rural areas. Bangkok has the highest proportion of households with computers at 42%, more than double that of other regions.[46] Thailand does not have major home-grown tech unicorns, yet it is deeply integrated into the region's internet economy.

Thai users are "mobile-first"; in other words, the mobile usage outstrips fixed-line internet usage.[47] Mobile internet has empowered users to access new products, markets, information and services. Since 2014, sales through online retail channels in Thailand have grown by approximately 10% in value each year, and in 2018 totalled $103.6 billion.[48] The online travel sector is the largest in the region, valued at $7 billion in 2019, and expanding at a 17% annualized growth rate.[49] E-payments have expanded in tandem.

The Bank of Thailand (BoT) recently announced plans for cross-border digital payments via QR code by working with regulators in the ASEAN region.[50] At a more macro-level, the Bank of Thailand has also partnered with the Hong Monetary Authority and 10 participating banks to pilot a distributed ledger technology solution for cross-border funds transfers (dubbed Project Inthanon-LionRock). The project's aim was to reduce pain points in cross-border transfer and settlement that can slow commercial efficiency and raise costs of doing international business.

The uptake of digital technologies and online services by business is also steadily improving. In a Deloitte survey in 2020, 59% of respondents indicated cloud technologies are already implemented in their business, while 29% said they have plans to do so within one year.[51] According to another survey of 1,000 regional small businesses before and during the COVID-19 pandemic, 73% of those in Thailand prioritized technology investment over other investments, such as factories and machinery, more than any other country in the region (by comparison, 65% did so in Malaysia and 63% in Singapore).[52]

Thailand is prominent in business process outsourcing (BPO) and offshoring services that are heavily dependent on data flows. According to the Kearney Global Services Location Index, in 2019 Thailand was the seventh most attractive service offshore location out of 50 ranked countries.[53] It targets BPO offshoring mainly from Australia and has competition from Indonesia, Vietnam and the Philippines. Online media and the creativity industries have grown, too, with the entry of foreign production companies into the Thai market.[54]

Pending privacy rules

Thailand enacted a Personal Data Protection Act (PDPA) in 2019 after consideration for around 15 years. That is an important step forward. The law was scheduled to enter into force in May 2020, but the application of key parts relevant to data controllers has been postponed for about a year, with the government citing the need to avoid extra legal costs during the pandemic period.[55] The PDPA will allow data transfers to take place to a jurisdiction abroad that has adequate data protection standards, and in accordance with rules set out by a Personal Data Protection Committee (PDPC), which is yet to be established. The Committee is also expected to play an important role in providing rules and guidelines to implement the law.

The PDPA will join a suite of other legislative acts that are cornerstones for the functioning of the digital economy, including the criminalization of cybercrime, laws to ensure equivalence between digital and traditional legal documents and consumer protection. Further, in 2016, a new vision for "Thailand 4.0" was launched to accelerate digital technology adoption across government, business and society.[56] A number of public policy initiatives are now in place to deliver these objectives.

Other policy considerations

Certain policy developments may affect the appetite for delivering digital services and introducing new technologies in Thailand, and dampen investment in related activities. For example, Thailand's Cyber Security Act (CSA) came into effect on 28 May 2019. Some experts have said that the CSA adds a number of hurdles to digital services provision and has prompted concerns over government

intervention impacting intellectual property rights and individual privacy.[57]

Thailand requires local presence to register a website under a national domain. The 2007 Computer Crimes Act (CCA) was amended in 2017 to bring it into line with world practices regarding Intermediary Service Providers' liability for the breach of intellectual property rights. The Copyright Act is planned to be amended similarly. The CCA eventually led to the creation of a Computer Data Filtering Committee with the power to block a range of websites that the Committee finds disseminate information violating public order.[58]

Meanwhile, the Computer-Related Offences Act does not provide a safe harbour for intermediaries and does not distinguish between different types of intermediaries, with a short time window for redress (24 hours in the case of some content).[59] Non-compliance can imply both financial sanctions and up to five years of imprisonment.

Transfer mechanisms, cooperation and trade

The PDPC may choose to list certain jurisdictions as adequate for data transfers or, if not, to clarify how this approach is to be enforced. Four exceptions to the adequacy requirement exist in the law:

1. A data subject's consent to transfer has been obtained
2. Specific statutory exemptions apply[60]
3. The receiving organization provides suitable protection measures that enable the enforcement of the data subject's rights
4. The receiving organization has put in place a "personal data protection policy" applicable to overseas data transfers.

These exceptions suggest that entities transferring data out of Thailand may be able to avail themselves of several transfer mechanisms beyond adequacy. The PDPC will have the authority to cooperate with PEAs abroad. Without a PEA, Thailand could not become a member of the Global Privacy Assembly (GPA), Global Privacy Enforcement Network (GPEN) or Asia Pacific Privacy Authorities (APPA) Forum. Thailand is part of APEC but has not joined the CBPR system. CBPRs could conceivably be among the solutions for demonstrating suitable protection measures when transferring Thailand data. Thailand may also wish to consider joining the APEC PRP. As the country is an ASEAN Member State, its companies could have recourse to the new MCCs.[61]

Thailand has assumed some international commitments related to personal data protection through trade agreements, such as the Thailand–Chile FTA, Article 11, where parties pledge to consider international standards when protecting the personal data of e-commerce users and when developing their own approaches. Although the country has over a dozen other trade agreements in force, many of these are older and do not cover the topic. Thailand has had debates on joining the CPTPP and it is part of the RCEP. It is also participating in plurilateral negotiations via the WTO Joint Statement Initiative on e-commerce involving some 85 WTO members where several data flow proposals have been tabled.

4.2 Highlights

Panellists highlighted the importance of "creating certainty and collaboration" for data governance. Across the region, business surveys indicate the main challenge to managing data flows is a lack of certainty on compliance, even if transfers are permitted in the letter of the law. A lack of collaboration between regulators on data governance principles also creates a patchwork effect and risks introducing gaps in personal information protection.

A public consultation on the foreign jurisdiction adequacy principles for freely transferring data ran from January to March 2021. Additional consultations will also take place on other types of transfer mechanisms. The PDPC's participation in global and regional forums will help build up its expertise and knowledge. Participants suggested that the PDPC does not need to "reinvent the wheel" but can deploy best practices used by neighbours. Doing so will be important to harness the opportunities of the Fourth Industrial Revolution and to avoid overly prescriptive or burdensome approaches.

During the breakout groups, participants noted that implementing guidelines must account for various types of business capacity. Larger firms can absorb and spread costs among many consumers while the same is not true for smaller businesses. Participants highlighted that compliance "cannot be faked" and thus capacity is critical for a sustainable system. The PDPC could equally clarify how the enforcement of extraterritoriality application will take place, as data controllers and data processors both in and outside the country could be subject to

the PDPA. Participants considered that a narrower approach where the link with Thailand is stronger could be the way forward.

Panellists emphasized that Thai businesses face a variety of legal requirements for data compliance abroad in addition to data localization issues. Participants encouraged Thailand to join the CPEA, a precursor for implementing CBPRs. They suggested Thailand need not wait until the PDPC is fully established to do so. The Thai Ministry of Digital Economy and Society could take on that role. Thailand may wish to eventually consider joining digital economy trade agreements that facilitate deeper regulatory cooperation on data transfer related areas like privacy, artificial intelligence, digital payments and so on. These are "customizable" depending on topics of interest between partners.

Whichever approach is taken, panellists stressed that it would be important for the PDPC to be as clear as possible. Issuing guidelines in advance, including those relevant to common services use such as cloud providers, can avoid confusion. It may also avoid smaller firms building their own services that may be less secure. Participants underscored that SMEs benefit from outsourcing the accountability of data compliance to other parties in the supply chain (for example platforms and cloud service providers).

5

Viet Nam

Trade plays an important role in Viet Nam's development and digital tools now need to be integrated into modes of operation. A new privacy law could bring coherence but may contain provisions that slow digital activities and investment.

5.1 Context

Pursuing digital transformation

Viet Nam has a dynamic economy that has developed remarkably over the past 30 years, in a large part thanks to trade. Yet Viet Nam's position in global value chains is vulnerable to competition from automation as well as new market entrants and cheaper labour in least-developed countries.[62] As such, Viet Nam is looking to transition from the traditional assembly and processing of trade to becoming a regional innovation centre, particularly using emerging technologies.[63] Viet Nam's National Program for Digital Transformation expects digital tools, some of which rely on the cross-border flow of data, to contribute 10% value add to every sector, resulting in annual productivity increases of 7%.[64]

One survey conducted in 2019 indicated that a quarter of manufacturing enterprises and 35% of formalized agricultural enterprises in Viet Nam were planning to invest in advanced technologies within the year.[65] These investments can pay off in multiple ways, notably lowering operational costs and improving efficiency, among other factors. For example, a wireless sensor network set up in 2016 on a fish farm in Dong Thap Province next to the Mekong River is controlling water quality and preventing disease. According to a recent technical report, "If implemented more widely, real-time monitoring on fish farms" (using internet of things and cloud technologies) "could help cut production losses by 40-50%, equating to a difference in turnover for each farm of at least $12,000 every six months".[66]

Viet Nam's e-commerce market, meanwhile, continues to grow. Ha Noi, as one of the two leading cities in e-commerce development, estimates a 20% increase in online retail sales by 2025 assuming 55% of the population will move to online shopping and 50% of SMEs will conduct business through e-commerce.[67] It is proving a vector for international expansion. In 2019, some 600 Vietnamese businesses were exporting through Alibaba and 140 through Amazon, thanks to a partnership with the Viet Nam E-commerce Association.[68] World Bank field studies suggest that e-commerce is essential to improve turnover among Vietnamese SMEs.[69]

Digital payments are growing, though from a low starting point. Vietnamese fintech start-ups Fvndit, Kim An Group, Timo and NextPay have recently secured new capital injections from domestic and foreign investors.[70] Foreign direct investment in financial services has been made easier after the Central Bank removed the 49% ownership limit for fintech in intermediary payment services.[71] Nonetheless, challenges to cross-border payments persist. Examples include the lack of access to international payments cards and payments methods, foreign exchange controls and fraud.[72]

For other types of services trade that build on data flows, Viet Nam ranks fifth worldwide as an offshore service location in the Kearney Global Services Location Index, competing with established offshore locations such as India, China, Malaysia and Indonesia.[73] Yet, the country comes in 37th out of 50 countries in the Index's digital resonance category, a new metric that incorporates variables around digital skills, legal adaptability, corporate activity and digital outputs, highlighting the importance of digital upgrading. Further, Viet Nam ranks last out of 24 nations in the readiness of adoption and growth of cloud computing services, according to a BSA Global Cloud Scorecard, hampered by the legal and regulatory environment, the level of cybersecurity and an absence of rigorous enforcement of intellectual property rights that impede cloud research.[74]

Digital policies

The National Digital Transformation Roadmap is the Government of Viet Nam's long-term digital support strategy. The country is also promoting digital growth in specific sectors. The plan for the IT sector, for instance, includes creating 10 IT unicorns with revenue surpassing $1 billion each and having 60% of the social networks used in Viet Nam developed locally by 2025.[75] The government is working to promote digital services that have been created, designed and produced in Viet Nam. Similarly, a National E-commerce Development Strategy sets goals of getting 55% of the population shopping online by 2025, non-cash payments accounting for 50% of transactions, 50% of small business using e-commerce platforms, and 40% of business using mobile apps for exchange.[76]

These policies are flanked by a suite of digital economy laws. New developments are under way on cybersecurity and the regulation of data privacy that is currently scattered across different ministerial bodies. A Law on Cybersecurity has been in effect since January 2019 with the aim of protecting national security and ensuring social order in cyberspace. It also includes data storage provisions requiring foreign and domestic enterprises providing telecom, internet and other value-added digital services to locate any servers on which Vietnamese users' data are administered within the country. Foreign enterprises

must have representative offices in Viet Nam. Personal data originated in Viet Nam may not be transferred overseas even if the data subject offers consent.[77]

Further, in February 2020, the Ministry of Public Security announced the completion of a Draft Decree on Personal Data Protection (DPDP).[78] The official draft of the DPDP, released early February 2021, is now open for public consultation. The proposed effective date is 1 December 2021. Article 21 sets four conditions that must be met to transfer Vietnamese personal data outside the country: 1) the data owner's permission has been given;[79] 2) the original data is stored in Viet Nam; 3) official documentation shows the data to be transferred goes to a jurisdiction that has an equivalent or higher data protection regulation than Viet Nam; and 4) written approval is received from the Personal Data Protection Committee (which will be established to oversee and ensure compliance).

Other requirements include keeping a history of cross-border transfers for a minimum of three years and following specifications on procedures to register cross-border personal data transfers with a new Personal Data Protection Committee, which will process the application within 20 working days from the date of receipt.

Trade commitments to consider

Viet Nam has over a dozen trade agreements in force, and while older ones do not cover data flow rules, the more recent ones do. The country is part of the CPTPP with its relevant commitments since January 2019 and has a two-year grace period for their enforcement. To date, CPTPP signatories have not challenged Viet Nam's Cybersecurity Law. Any potential legal questions would lie not in the legitimacy of the public policy goals but on whether Viet Nam's measures are proportionate to the objective sought.

An EU–Viet Nam FTA, signed in 2019, stipulates that both parties will allow financial services suppliers to transfer information, in electronic or other form, into and out of their territories, for the "ordinary course of business" no later than two years after the entry into force of the agreement. What is "ordinary" in financial services has been subject to debate in other FTAs in which identical language was incorporated. The text also stipulates that both parties must maintain proper safeguards to protect personal data and "nothing in this Article restricts the right of a Party to protect personal data and privacy, so long as such right is not used to circumvent this Agreement".[80]

Room to pursue regulatory cooperation

Serving foreign markets will require compliance with their data requirements. Viet Nam's draft and current regulations, however, do not for the most part envision data transfer mechanisms. Article 21 of the DPDP allows data transfers if a document is furnished that demonstrates the data will be relayed where the regulations are at the same level or higher than those the Decree stipulates. That could create room for Viet Nam to join regional certification mechanisms or create adequacy lists, but the document does not go into further detail.

Viet Nam is not part of the APEC CBPR system. It could consider joining the CPEA once the Personal Data Protection Committee is established to share information with counterparts and learn from best practices. It could also offer its businesses recourse to the ASEAN MCCs. Viet Nam is also not a member of the GPA, GPEN or APPA Forum.

The more data transfer mechanisms are available, the more attractive Viet Nam will be from an investment perspective and the less regulatory friction domestic providers will face when trying to reach other markets. Capacity building especially for SMEs, transparency and information on available mechanisms for transferring entities will be key to facilitate the operationalization of these trade opportunities.

5.2 Highlights

Panellists noted the rapid growth and potential of Viet Nam's digital economy. In the last decade alone, 20 million consumers made their first e-commerce purchase. More than 1 million sellers have joined the digital economy. Businesses are using cloud services and other advanced technologies. Many new start-ups are appearing, and companies have used digital tools in imaginative ways during the COVID-19 pandemic.

The Government of Viet Nam should be commended for facilitating this momentum. Actions such as the National Digital Transformation Roadmap are helpful, as is the just recently released national AI masterplan. It would be useful for Viet Nam to have one unifying privacy law in order to increase trust in the system. However, participants flagged the importance of "getting the balance right" between enabling data flows across borders and ensuring domestic objectives. Several panellists suggested regional and international best practices could be studied.

Participants noted that the current proposed DPDP has elements that are more demanding for transferring entities than the approach taken in other jurisdictions. Clarification will be needed on which transfers would be approved as many businesses are not clear on this matter. For example, questions remain regarding whether data "mirroring" should be undertaken, where data can be transferred but a copy is stored in-country.

Deviation from international norms will make it more difficult for Vietnamese companies to participate in the digital economy at the regional and global levels as business processes will need to be adapted and limited collaboration may reduce the number of mutual compliance mechanisms available. Some participants highlighted that Viet Nam does have international obligations – such as in the CPTPP – and ongoing WTO negotiations on e-commerce could be a useful forum for exchange. The country could consider joining these talks.

Digital payments and digital investment were highlighted as important areas to advance. Currently, only a small portion of the population has a bank account, and an even smaller portion has credit cards. Digital solutions can plug the gap, but regulations on e-wallets and efforts to improve public confidence, among others, are needed, while data transfer policies could affect the supply of international services. Digital policies will also impact investor appetite. One suggestion was that policy-makers think about how their actions impact domestic investment in digital transformation and foreign investment in the digital economy.

6 Conclusion

The insights from the country dialogues on data flow governance and digitalization aim to generate insights for improved regional and global cooperation.

The conversations on data flow governance and digital growth across the four diverse economies underscored the topics' critical importance and complexity. Many of the discussions took on a new meaning amid the COVID-19 health crisis, during which turning to digital solutions has been a lifeline for business and consumers alike. An overarching insight is that while governments and national stakeholders are not monolithic as regards data transfer policies, regional and global cooperation to pursue interoperability where possible is key for future growth opportunities.

The World Economic Forum will continue to work with stakeholders on the evolving policy landscape, remaining active in ASEAN digital economy integration processes and ready to support other regions in a similar capacity. The Forum seeks to leverage the Centre for the Fourth Industrial Revolution Network to help share perspectives between economies. Going forward, it will be important to continue to share national and regional developments within international negotiations and norm-setting, and to evaluate where cooperation between nations can best advance. Public-private dialogue remains essential to evaluate the impact of policy decisions.

Contributors

World Economic Forum

Kimberley Botwright
Community Lead, Global Trade and Investment, World Economic Forum

Rosa Esi Ennison
Specialist, International Trade and Investment, World Economic Forum

Yuiko Noda
Project Lead, Centre for the Fourth Industrial Revolution Japan

Jimena Sotelo
Project Lead, Digital Trade, World Economic Forum LLC

ECIPE

Hosuk Lee-Makiyama
Director, European Centre for International Political Economy, Belgium

Claudia Lozano
Research Associate, European Centre for International Political Economy, Belgium

Endnotes

1. World Economic Forum, "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows", White Paper, 2020.
2. Government of India, Press Information Bureau, "Report on India's Trillion Dollar Digital Opportunity Released", Press Release, 20 February 2019, https://pib.gov.in/PressReleasePage.aspx?PRID=1565669#:~:text=The%20report%20finds%20that%20India,diverse%20sectors%20of%20the%20economy (accessed 24 March 2021).
3. Krishnan, Murali, "India's digital divide grows among rural women", DW, 15 December 2020, https://www.dw.com/en/indias-digital-divide-grows-among-rural-women/a-55949074 (accessed 24 March 2021).
4. Osio, Julber, "Snapshot of Asia-Pacific's Mobile Markets, 2019", S&P Global Market Intelligence, 13 February 2020, https://www.spglobal.com/marketintelligence/en/news-insights/research/snapshot-of-asia-pacifics-mobile-markets-2019 (accessed 24 March 2021).
5. Initiatives under Digital India are organized into three categories: 1) digital infrastructure as a utility to every citizen; 2) governance and services on demand; and 3) the digital empowerment of citizens. Specific targets include delivering high-speed internet to all, ensuring digital identity, enabling mobile and digital bank account access, creating Common Service Centres for public connectivity, upgrading government services and availability, and promoting universal digital literacy and universally accessible digital resources, among others. See Government of India, Ministry of Electronics & IT, Digital India, "Vision and Vision Areas", https://digitalindia.gov.in/content/vision-and-vision-areas (accessed 24 March 2021).
6. Government of India, Unique Identification Authority of India, "Welcome to UIDAI", 2019, https://www.uidai.gov.in/16-english-uk/aapka-aadhaar/14-what-is-aadhaar.html (accessed 24 March 2021).
7. Kaka, Noshir, et al., "Digital India: Technology to transform a connected nation", McKinsey Digital, 27 March 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation (accessed 24 March 2021).
8. Key services exports include other business services, travel, transportation and financial services.
9. Consumer Unity & Trust Society (CUTS International), *Data Localisation: India's Double-Edged Sword?*, 2020.
10. OECD-WTO Balanced Trade in Services (BaTIS) statistics, http://www.oecd.org/sdd/its/balanced-trade-statistics.htm (accessed 24 March 2021)
11. Hinrich Foundation, AlphaBeta and All India Management Association (AIMA), *The Data Opportunity: The promise of digital trade for India*, 2019.
12. World Trade Organization, "Trade Policy Review: India", 6 and 8 January 2021, https://www.wto.org/english/tratop_e/tpr_e/tp503_e.htm (accessed 24 March 2021).
13. United Nations Conference on Trade and Development (UNCTAD), "Investment flows to developing countries in Asia could fall up to 45% in 2020", 16 June 2020, https://unctad.org/news/investment-flows-developing-countries-asia-could-fall-45-2020 (accessed 24 March 2021).
14. Boston Consulting Group, "India's Market Report", 2019, https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/india (accessed 24 March 2021).
15. India Brand Equity Foundation (IBEF), "Media and Entertainment industry", 28 February 2021, https://www.ibef.org/industry/media-entertainment-india.aspx (accessed 24 March 2021).
16. Hinrich Foundation, AlphaBeta and All India Management Association (AIMA), *The Data Opportunity: The promise of digital trade for India*, op. cit.
17. Government of India, Ministry of Electronics & Information Technology (MeitY), *India's Trillion-Dollar Digital Opportunity*, 2019.
18. NICDC Logistics Data Services (NLDS), "India's Logistics Redefined", 2020.
19. Nanda, Ashish, "Will the next transformation in manufacturing be led by digital?", EY, 21 February 2020, https://www.ey.com/en_in/supply-chain/will-the-next-transformation-in-manufacturing-be-led-by-digital (accessed 24 March 2021).
20. KPMG and Confederation of Indian Industry (CII), *Convergence towards inclusive digital growth*, 2018.
21. Cisco, "IDC-Cisco 2020 Asia Pacific SMB Digital Maturity Study", 2020, https://www.cisco.com/c/dam/global/en_sg/solutions/small-business/pdfs/ebookciscosmbdigitalmaturity-withcountries.pdf (accessed 24 March 2021).
22. The governance of electronic personal and sensitive personal data is partially addressed under the Information Technology Act, as amended in 2008, and the associated Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Under these rules, data may be transferred abroad so long as the same level of data protection is adhered to, for the performance of a lawful contract, and with personal consent. Other laws touching on data transfers include the National Data Sharing and Accessibility Policy (NDSAP, 2012); the Companies (Accounts) Rules, Ministry of Corporate Affairs (MCA, 2014); the Unified License Agreement (2012); the Aadhaar Regulations (2016); and the Guidelines for Procurement of Cloud Services (2019).
23. There is a degree of uncertainty on the next steps for the PDPB 19. According to some sources, it may not be passed in its current form, although it is currently under examination by a Joint Parliamentary Committee.

24. Bryant, Jennifer, "What you should know about India's forward-moving privacy bill", International Association of Privacy Professionals (IAPP), 17 December 2019, https://iapp.org/news/a/indias-data-privacy-bill-under-committee-review (accessed 24 March 2021).

25. Burman, Anirudh, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?", Carnegie India, 9 March 2020, https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217 (accessed 24 March 2021).

26. See the *Report by the Committee of Experts on Non-Personal Data Governance Framework* (available at https://www.mondaq.com/india/privacy-protection/1024312/revised-report-by-the-committee-of-experts-on-non-personal-data-governance-framework). Key recommendations include defining non-personal data (three suggested categories: public non-personal data, community non-personal data and private non-personal data; a concept of "sensitive non-personal data" is suggested where this relates to national security interests, business confidential information or anonymized data that could be reidentified); articulating a legal basis for rights over non-personal data; defining a data business that would be subject to the law; elaborating data-sharing mechanisms; and defining a non-personal data authority. Creating a new taxonomy to identify a "data business" that collects, processes, stores and manages data above certain threshold criteria is suggested. Data businesses will provide, within India, open access to metadata and regulated access to underlying data.

27. Kathuria, Rajat, et al., *Economic Implications of Cross-Border Data Flows*, Internet and Mobile Association of India (IAMAI) and Indian Council for Research on International Economic Relations (ICRIER), 2019.

28. Consumer Unity & Trust Society (CUTS International), *Data Localisation: India's Double-Edged Sword?*, op. cit.

29. Hinrich Foundation, AlphaBeta and All India Management Association (AIMA), *The Data Opportunity: The promise of digital trade for India*, op. cit.

30. It should be noted, of course, that an SCC does require recognition by the host jurisdiction. The EU–US Privacy Shield was another model for business-to-government compliance and interoperability, but was invalidated by the European Court of Justice in July 2020, which also added caveats to the use of SCCs.

31. EU SCCs are included as a transfer compliance option in Chapter 5 of the General Data Protection Regulation on transfers of personal data to countries outside the EU or international organizations.

32. Google, Temasek and Bain & Company, "e-Conomy SEA 2020", https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/e-Conomy_SEA_2020_Report.pdf (accessed 23 March 2021).

33. Temasek, "Google, Temasek, Bain & Company e-Conomy SEA 2019 Report", 2019.

34. Google, Temasek and Bain & Company, "e-Conomy SEA 2020", op. cit.

35. GSMA, *Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC Can Protect Data and Drive Innovation*, 2018, https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf (accessed 23 March 2021).

36. Microsoft Philippines Communications Team, "Digital Transformation to Contribute US$8 Billion to The Philippines GDP by 2021", Microsoft, 14 February 2018.

37. The Philippines ranks mid-way on the European Centre for International Political Economy (ECIPE) Digital Trade Restrictiveness Index (available at https://ecipe.org/dte/dte-report). The policy areas where restrictions are most severe in the Philippines compared to other countries are in horizontal (non-data) issues that affect the digital economy, such as foreign investment, business mobility and tariffs. The overall effect of these also needs to be considered but is not the direct focus of this paper and subsequent dialogue.

38. The NPC is an accredited member of the Global Privacy Assembly (GPA), the Global Privacy Enforcement Network (GPEN) and the Asia Pacific Privacy Authorities (APPA) Forum. Philippines' Privacy Commissioner Raymund Enriquez Liboro is serving as the head of the GPA's COVID-19 task force.

39. Cahiles-Magkilat, Bernie, "PH, Singapore sign MoU to protect personal data", *Manila Bulletin*, 10 September 2019.

40. The text highlights the importance of data flows in the financial sector to improve risk management and compliance programmes, detect cross-border money laundering and terrorist financing patterns, and defend against cyberattacks. The BSP and MAS intend to promote the adoption of policies encouraging data transfer and not restricting the location of data storage. These provisions, while non-binding, send a positive signal to industry on the direction of regulatory principles. See Monetary Authority of Singapore, "Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and the Monetary Authority of Singapore", Media Release, 16 November 2020.

41. Australian Government, Department of Foreign Affairs and Trade, "Consolidated RCEP Agreement (31Aug'20), Chapter 12, Electronic Commerce", 2020.

42. Lexology, "Company compliance with the Philippines' Data Privacy Act", 8 September 2017, https://www.lexology.com/library/detail.aspx?g=74b69284-898e-4294-a122-7d7bdbf6618d (accessed 24 March 2021).

43. Cross Border Privacy Rules System (CBPRs), "Participation in the APEC Cross-Border Privacy Rules (CBPR) System affords Asia-Pacific Economic Cooperation members a unique opportunity to work", 2021.

44. Kemp, Simon, "Digital 2020: Thailand", DataReportal, 18 February 2020, https://datareportal.com/reports/digital-2020-thailand (accessed 24 March 2021).

45. Christopher, Michell, "Leave No Thai Behind: Promoting equality of digital access in Thailand", OpenGov Asia, 19 July 2018, https://opengovasia.com/leave-no-thai-behind-promoting-equality-of-digital-access-in-thailand (accessed 24 March 2021).

46. Rattanakhamfu, Saowaruj, “Covid-19 emphasizes the need to bridge the digital divide and reduce online educational inequality”, Thailand Development Research Institute (TDRI), 6 May 2020, https://tdri.or.th/en/2020/05/covid-19-emphasizes-the-need-to-bridge-the-digital-divide-and-reduce-online-educational-inequality/ (accessed 24 March 2021).
47. J.P.Morgan, “E-commerce Payments Trends: Thailand”, 2019, https://www.jpmorgan.com/europe/merchant-services/insights/reports/thailand (accessed 24 March 2021).
48. Thailand Board of Investment, “Digital, Creative, and Startup Ecosystem”, September 2019, https://www.boi.go.th/upload/content/BOI_Digital_Economy_Brochure.pdf (accessed 24 March 2021).
49. Temasek, “Google, Temasek, Bain & Company e-Conomy SEA 2019 Report”, op. cit.
50. Banchongduang, Somruedi, “Thai banks spread QR code in Asean”, *Bangkok Post*, 10 February 2020, https://www.bangkokpost.com/business/1854194/thai-banks-spread-qr-code-in-asean#:~:text=Thailand%20is%20set%20to%20kick,digital%20platform%20across%20the%20region.&text=Regional%20interoperability%20of%20standardised%20QR,to%20make%20strides%2C%20she%20said (accessed 24 March 2021).
51. Deloitte, *The Thailand Digital Transformation Survey Report 2020*, 2020.
52. Dun & Bradstreet, “ASEAN SME Transformation Study 2020”, 2020.
53. Suman, Vidisha, “Digital resonance: the new factor influencing location attractiveness: The 2019 Kearney Global Services Location Index”, Kearney, 2019.
54. Thailand Board of Investment, “Digital, Creative, and Startup Ecosystem”, op. cit.
55. The Royal Decree declaring the delay was silent on whether data processors were also exempt. That may relate to the legal options for exemptions included in the PDPA itself and it is expected that the exemption applies given that a data processors’ main duty is to adhere to a data controller’s instructions.
56. Reuters Plus, “Digitalizing Thailand”, https://www.reuters.com/brandfeatures/thailand-advancing-into-the-future/digitalizing-thailand (accessed 24 March 2021).
57. ASEAN Today, “Thailand’s new cybersecurity law lets authorities violate privacy”, 8 March 2019, https://www.aseantoday.com/2019/03/thailands-new-cybersecurity-law-lets-authorities-violate-privacy (accessed 24 March 2021).
58. There has never been a successful appeal or reversal of the Committee’s decisions. In addition, lese-majeste laws affect platforms as for all media.
59. Ferracane, Martina Francesca, Hosuk Lee-Makiyama and Erik van der Marel, *Digital Trade Restrictiveness Index*, European Centre for International Political Economy (ECIPE) and Digital Trade Estimates (DTE), 2018, https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf (accessed 22 March 2021).
60. Statutory exemptions to the adequacy requirement include transfers made for compliance with the law, if necessary to perform a contract to which the data subject is party; for compliance with a contract between the controller and other persons for the interests of the data subject; to prevent danger to the data subject; or if necessary to carry out activities in relation to substantial public interest. See United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) and Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT), “Resource Materials on Data Privacy Laws in the Asia and the Pacific”, Webinar on Data Privacy Laws in ASEAN, 2021, https://www.unapcict.org/sites/default/files/2021-01/Resource%20Materials%20on%20Data%20Privacy%20Laws%20in%20Asia%20and%20the%20Pacific.pdf (accessed 22 March 2021).
61. Exporting companies in Thailand currently seem to rely on standard contractual clauses for data protection that are often based on EU standard contractual clauses. Such practices are not always well-suited for small businesses given the lack of regulatory infrastructure.
62. Hallward-Driemeier, Mary, and Gaurav Nayyar, *Trouble in the Making? The Future of Manufacturing-Led Development*, World Bank Group, 2018.
63. Ly, To Trieu Hai (Tracy), “Vietnam in the Post-COVID Era: Realizing a ‘Digital Country’”, Asia Pacific Foundation of Canada, 28 July 2020, https://www.asiapacific.ca/publication/vietnam-post-covid-era-realizing-digital-country (accessed 25 March 2021).
64. vanbanphapluat.co, Viet Nam legal document database system, “Decision No. 749/QD-TTg dated June 03, 2020 on introducing program for national digital transformation by 2025 with orientations towards 2030”, https://vanbanphapluat.co/decision-749-qd-ttg-2020-introducing-program-for-national-digital-transformation (accessed 25 March 2021).
65. Cameron, Alicia, et al., *Vietnam’s Future Digital Economy - Towards 2030 and 2045*, Technical Report, 2019, https://www.researchgate.net/publication/343180107_Vietnam%27s_Future_Digital_Economy_-_Towards_2030_and_2045 (accessed 22 March 2021).
66. Ibid.
67. Viet Nam News, Biz Hub, “E-commerce to continue growing this year”, 27 January 2021, http://bizhub.vn/tech/e-commerce-to-continue-growing-this-year_321885.html (accessed 25 March 2021).
68. Cameron, et al., *Vietnam’s Future Digital Economy - Towards 2030 and 2045*, op. cit.
69. World Bank Group, *Vietnam Development Report 2019: Connecting Vietnam for Growth and Shared Prosperity*, Final Report, 2019.
70. Deshmukh, Atharva, “Why Vietnam’s Expanding Digital Economy Presents Opportunities for Investors”, Dezan Shira & Associates Vietnam Briefing, 4 December 2020, https://www.vietnam-briefing.com/news/why-vietnams-expanding-digital-economy-presents-opportunities-for-investors.html (accessed 25 March 2021).

71. Yen, Hai, "Vietnam c.bank drops foreign ownership limit requirement for fintech", *Hanoi Times*, 12 February 2020, http://hanoitimes.vn/vietnam-cbank-discards-foreign-ownership-limit-requirement-for-fintech-301028.html (accessed 25 March 2021).

72. Anh, Lan, "Cross-border e-commerce opens door to global market", *Vietnam Economic News*, 23 September 2020, http://ven.vn/cross-border-e-commerce-opens-door-to-global-market-43805.html (accessed 25 March 2021).

73. Suman, "Digital resonance: the new factor influencing location attractiveness: The 2019 Kearney Global Services Location Index", op. cit.

74. BSA - the Software Alliance, "2018 BSA Global Cloud Computing Scorecard", 2018, https://cloudscorecard.bsa.org/2018 (accessed 25 March 2021).

75. Socialist Republic of Vietnam, Ministry of Information and Communications, "Vietnam sets ambitious plan for IT sector development", 5 June 2020, https://english.mic.gov.vn/Pages/TinTuc/142429/Vietnam-sets-ambitious-plan-for-IT-sector-development.html (accessed 25 March 2021).

76. Giang, Long, "National master plan on e-commerce development in a period of 2021-2025", ASEMconnectVietnam, Vietnam Industry and Trade Information Center (VITIC) - Ministry of Industry and Trade, 29 May 2020, http://asemconnectvietnam.gov.vn/default.aspx?ID1=2&ZID1=14&ID8=97603 (accessed 25 March 2021).

77. Article 26.3 of the Law on Cybersecurity states that any "domestic and foreign service providers on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service providers] carrying activities of collecting, exploiting [using], analysing and processing data [being] personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a [specified] period [to be] stipulated by the Government", so pending further guidance from the government. See Socialist Republic of Viet Nam, National Assembly, "Law on Cybersecurity", No. 24/2018/QH14, 12 June 2018, https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf (accessed 22 March 2021).

78. Data Guidance, "Vietnam: MPS seeks comments on draft data protection decree", 19 February 2020, https://www.dataguidance.com/news/vietnam-mps-seeks-comments-draft-data-protection-decree (accessed 25 March 2021).

79. The default position in current Vietnamese law is that the data owner or subject needs to provide consent for the collection, processing and use of personal information. The use of the information should not exceed the purposes for which consent was given. The data subject is entitled to request changes to the storage or use of their data, for example, by requesting their data be corrected or removed or that it stop being supplied to a third party. It has not always been clear in previous legislation, however, how consent should be expressed: whether consent needs to be explicit (opt-in) or whether notice and lack of objection is enough. Express consent is required by e-commerce websites. Article 8 of the Draft Decree does describe conditions of validity regarding consent to the processing of personal data, which creates business certainty on that aspect.

80. Center for WTO and International Trade, Vietnam Chamber of Commerce and Industry, EU-Vietnam trade and investment agreements, "Chapter 8: Liberalisation of Investment, Trade in Services and Electronic Commerce, Section A, General Provisions", 2019, p. 71.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org