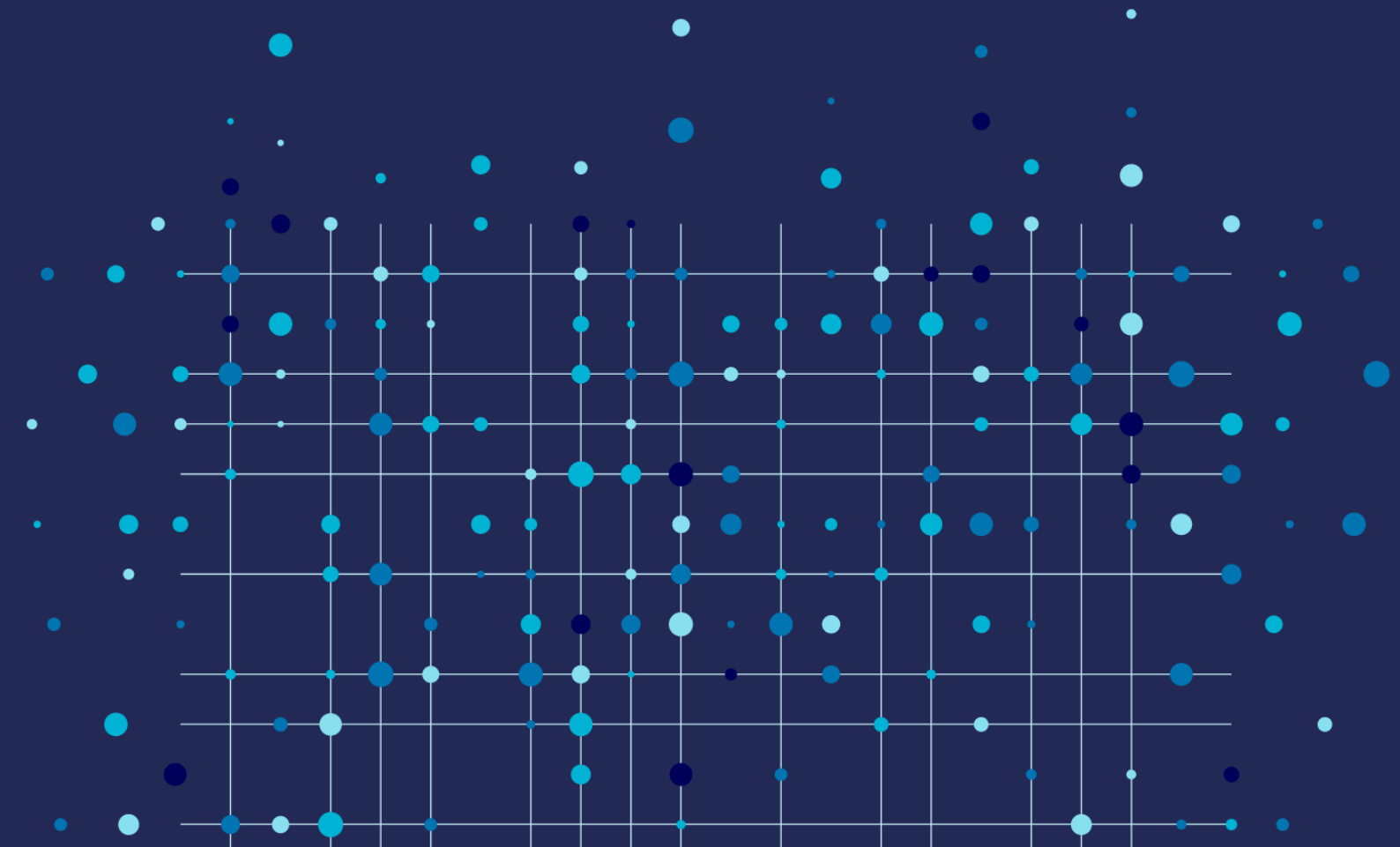
ASIA HOUSE

Mind the Gap:

How Southeast Asia's fragmented personal data rules impact digital finance

Poomthawat Wachirapornpruet



Executive Summary

This report examines the impacts of fragmented personal data regulations on digital financial services in Southeast Asia. It focuses on how the different regulations in the region work together, or more typically do not, and their effect on consumer financial services.

The key findings of the research are:

- **The use and movement of personal data is increasingly being regulated in Southeast Asia but relevant regulatory frameworks remain fragmented across the region.** With different regulatory regimes being developed separately, Southeast Asia has interoperability problems affecting the flow of personal data across its borders.

- **Financial services in Southeast Asia are becoming more digitalised but face fragmented regulations when operating cross-border.** Digitalisation allows the financial sector to tap into the expanding consumer market more effectively, concurrently enhancing financial inclusivity. However, as digital financial service providers increasingly rely on personal data to innovate and tailor their services, the fragmented regulatory landscape can mean higher costs and complex work-arounds.

- **Despite this, digital financial service firms do not consider increasingly regulated use of personal data to necessarily be negative, nor constitute an insurmountable obstacle.** On the contrary, complying with strict regulations is seen as a viable approach to building consumer trust, even as fragmentation may lead to reduced efficiency. In addition, businesses have the capability to navigate this complex regulatory environment and extend their services beyond borders even in the absence of improved interoperability. Challenging existing regulatory frameworks is not, as a result, a top priority for businesses.

- **Nevertheless, interoperability would benefit digital financial services providers.** Even as firms may value trust, cost also remains a deciding factor for businesses to be viable. Personal data regulatory interoperability enables data sharing and the centralisation of operations, which are the key to efficient and effective services. However, this is difficult to achieve under a fragmented landscape. Moreover, compliance approaches taken in the current environment also create potential negative repercussions for businesses, including vulnerabilities to cyber-attacks.

- **Stakeholders are working together to create interoperable personal data governance framework across the region.** This needs to take into account the interests of different governments, businesses and societies. Efforts to increase regional regulatory interoperability of personal data are taking place at the ASEAN level. While earlier initiatives were hindered by limitations such as their non-binding nature, the forthcoming ASEAN Digital Economy Framework Agreement (DEFA) is expected to be legally binding and go further than previous initiatives.

- **How stakeholders respond to the issue of personal data regulations is key for Southeast Asia to position itself in the global digital economy and become a player in the debate over digital governance.** For the region to truly be a leader on the world stage, it would need to prove itself as a viable role model. As such, to match its ambitions to become a global leader in the digital economy, it needs effective and enabling digital governance at the regional level. Policymakers and regulators are already playing catch-up with the market, and the way they address current regional regulatory fragmentation should mark the first step in building digital governance for the future.

Table of contents

List of Figures

List of Tables

Acknowledgement

This research was made possible through the unwavering support of the Asia House team and their extensive network.

I am deeply grateful to Joanna Octavia for consistently mentoring me throughout the entire research. I would also like to extend my appreciation to Zhouchen Mao, Michael Lawrence OBE, and the other staff members at Asia House for their invaluable guidance, assistance, and the very opportunity to conduct this research. All have been instrumental in the successful completion of this report.

Additionally, I wish to express my profound gratitude to all the interviewees who generously shared their time and expertise, providing crucial insights that contributed significantly to this study. I also extend my sincere thanks to the editorial and design teams, whose efforts have ensured that this report would be able to effectively communicate its findings to a wide range of its intended audiences.

Lastly, I would like to express my deepest appreciation to my family for their endless encouragement, as this achievement would not have been possible otherwise.

Poomthawat Wachirapornpruet
Asia House Fellow 2023-24

Section One:

Introduction

Southeast Asia is in a period of rapid digital transformation, with growing internet connectivity, widespread smartphone adoption and an expansion of digital products and services. The growth of such services is driving extensive collection and use of personal data, a key component for conducting business through data-driven decision making (HSBC, 2022). As a result, concerns have arisen about the privacy and security of personal data across the region. Since countries in Southeast Asia adopt varying approaches to data governance, businesses looking to leverage this digitalisation trend can face both compliance and technical challenges, especially when operating across borders.

The financial sector is at the forefront of this digital transformation. Digital financial services are expanding the reach of providers and enabling them to access previously untapped customer segments by enhancing accessibility and driving the adoption of new and innovative solutions. However, firms seeking to use personal data for business across the region's borders face a complex and highly fragmented regulatory environment.

This report explores the interoperability of personal data regulations across Southeast Asia and examines how these regulations affect the ability of companies to provide digital financial services. It looks at how regulatory fragmentation impacts these services, and at ongoing region-wide efforts to enhance interoperability.

The first section of this report explores the digital finance landscape in Southeast Asia and how the financial sector may utilise personal data. The second section considers differences in personal data regulatory regimes across Southeast Asia and analyses how fragmentation may impact interoperability in digital financial services. The third section examines how businesses in the financial services industry navigate the fragmented regulations. In the fourth section, the report reviews regulatory harmonisation efforts at the multilateral level, and assesses the potential of other ongoing ASEAN initiatives to address the issue. Finally, the last section evaluates how ongoing developments in personal data regulations play a role in the trajectory of financial services, as well as caveats to consider.

1.1 Evolution of personal data governance in Southeast Asia

Within the last decade, governments across Southeast Asia have been taking an increasingly hands-on approach in regulating how businesses handle personal data. The rationale for this ranges from national security, consumer protection and economic reasons such as incentivising data centre business domestically (Li, 2022; Sangfor Technologies, 2023). There is also the issue of data sovereignty, the control of data and laws within given jurisdictions. This Southeast Asian approach stands in sharp contrast to that of the European Union, where the General Data Protection Regulation (GDPR) was predominantly driven by the rationale of individual rights and privacy.

Development in Southeast Asia has come in various forms, ranging from the creation of entirely new national regulatory frameworks on personal data to the introduction of relatively narrow regulatory requirements for specific sectors. Since the 2010s, six Southeast Asian countries – Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam – have introduced new personal data protection laws (with Vietnam's passing as recently as 2023) (DLA Piper, 2024a). Meanwhile, specific restrictions on the cross-border flow of personal data for banks and financial services have come into force, such as in Indonesia in 2022 (Long, 2023).

This development comes as the financial services sector eyes Southeast Asia's substantial consumer market with its high potential for digitalisation. For example, in 2023, up to 80 per cent of Indonesians remain underserved by traditional banking (Habir and Negara, 2023). The potential is enhanced further by the region's widespread adoption of digital devices, which enables a significant portion of underserved Southeast Asians to access financial services that may be difficult otherwise. Digitalisation also means financial service providers can serve a broader range of consumers at lower cost (additiv, 2024; Kim et al., 2022). But the increasing adoption of digital solutions such as mobile banking, e-payments, and other fintech innovations means the need for robust and harmonised data protection mechanisms has become increasingly critical.

In short, tightening regulations of personal data use across Southeast Asia can influence the future of digital finance in the region. It complicates the regional operations of businesses offering cross-border digital financial services and slows the adoption of digital innovations within the sector in general. Moreover, as financial digitalisation has been regarded as one of the main pillars supporting the development and integration of digital economy, any additional regulatory barriers also have a potential to undermine ongoing efforts to integrate the digital economy across the region (ASEAN and USAID, 2021).

1.2 Digital financial services in Southeast Asia

1.2.1 Defining digital financial services

For the purposes of this report, **digital financial services** will be defined as financial services that can be accessed and delivered via digital channels such as mobile devices (AFI, 2019). This can be in the form of the services or financial products provided by either traditional financial institutions such as banks, or alternative providers such non-bank financial technology (fintech) companies. Table 1 illustrates the distinction between banks and fintech firms being used in this report, and how they provide digital financial services in Southeast Asia.

Many people in the region lack access to conventional financial services due to geographical barriers, limited infrastructure and high costs associated with traditional banking. As a result, a substantial proportion of the population remains excluded from essential financial services such as banking and credit, with up to 50 per cent or 200 million people being "unbanked" or unable to access basic services such as bank accounts. Another 24 per cent, up to 98 million people, are "underbanked" with broader unmet financial needs such as access to credit or investment products (Google, Temasek, and Bain & Company, 2019).

Digital solutions are in a perfect position to fill this financial inclusivity gap (Macquarie Capital, 2022). Despite having limited or no access to traditional financial services, there is a very large potential customer base that increasingly owns digital devices, such as smartphones, and benefits from affordable mobile data (Kapron, 2024; Macquarie Capital, 2022). Smartphone users are expected to have comprised nearly 90 per cent of internet users in Southeast Asia in 2023 (Cheung, 2023). This significant penetration of digital services and devices in the region further supports the development of digital financial services, with 78 per cent of consumers conducting transactions online in 2021 (Bain & Company and Facebook, 2021).

Table 1: Digital financial services in Southeast Asia

Traditional banks	Fintech companies
In this report, "traditional banks" mean established financial institutions licensed by regulators to provide banking services. These banks have been providing an increasing number of digital products and services within Southeast Asia and are major players in digital finance. Banks may also rely on partnership with, or outsourcing to, non-bank technology vendors to jointly provide digital products or services. In Southeast Asia, there has also been a trend among banks to establish in-house fintech arms.	Fintechs are first and foremost technology vendors serving the financial sector. They are not holders of banking licenses like established players but have become major alternative providers of digital finance. To provide digital financial services in Southeast Asia, fintech players may obtain limited permits from the regulator for specific activities short of a full banking license, such as payment service. Alternatively, fintech companies also acquire firms or banks with operating licenses.

(Adapted from AFI, 2019)

Moreover, the expansion of a tech-savvy middle class in Southeast Asia is also driving demand for more sophisticated financial products with potential in wealth and investment services, especially those offered via digital platforms (AAA Global, 2024; additiv, 2024; Bender, 2023).

The introduction of digital innovations to the sector is a promising response to the financial inclusivity gap (Kim et al., 2022). Increasing digital penetration, coupled with continuous interests from governments in the region to provide enabling policy as part of developments in the wider digital economy, creates a promising environment for the expansion of digital financial services (Kapron, 2024).

1.2.2 Major types of digital financial services in Southeast Asia

Digital financial services encompass a broad range of products and services. The focus here is on consumer finance, a segment of financial services where the use of personal data is crucial. Personal data is being used for a wide variety of purposes in these services and plays important roles in both business operations and user experience. This ranges from the verification of customer identity to the use of data analytics for due diligence or the personalisation of service offerings.

In Southeast Asia, the consumer financial services market has been steadily gaining traction, making up 42 per cent of fintech solutions in 2019 (CCAF, ADBI and FinTechSpace, 2019). Among these products, some have been receiving significant attention from businesses and governments, such as digital payments, digital lending, and digital wealth. These services appeal to the growing tech-savvy population, thereby broadening financial inclusion, and are looking to increasingly apply personal data-driven insights in their emerging innovations. They are also increasingly looking to operate cross-border in the region.

Digital Payments

Digital or e-payment products encompass a wide variety of ways to handle money digitally, examples of which can be found in Table 2. These include eWallet and associated person-to-merchant (P2M) and peer-to-peer (P2P) transaction solutions, digital international remittance and transfer services, and other types of e-payment gateways (CCAF, ADBI and FinTechSpace, 2019). Among them, digital wallet and digital remittance are core consumer market products and are being offered by multiple regional players, including fintechs such as GrabPay and Dana. Similarly, traditional banks such as Krungthai (KTB) and CIMB also provide payment solutions as part of their mobile banking platforms.

Table 2: Examples of digital payment solutions found in Southeast Asia

Digital wallet (eWallet)	Digital solutions to transfer and manage money, can be peer-to-peer (P2P) or person-to-merchant (P2M)
Digital international remittance	Digital solutions designed to send money to companies or people abroad
Payment gateways	Systems for accepting, authorising, and processing payments at businesses
POS technologies	Point-of-sale solutions for mobile and businesses

(Adapted from: CCAF, ADBI and FinTechSpace, 2019)

In addition, QR code payments have now become one of the most notable innovations in the region, regularly used in combination with digital wallets. The system relies on the generation of unique QR codes – machine-readable codes consisting of an array of black and white squares – that can be scanned by digital devices such as smartphones to complete transactions without requiring customers to input all data manually. Depending on how the system was set up, these codes can be generated and presented by either the payer or the payee (World Bank, 2021).

Ongoing developments indicate that cross- border payment systems are becoming increasingly integrated through QR payments. In recent years, QR payment is becoming the primary digital cross-border payment method sanctioned by central banks of the countries of the Association of Southeast Asian Nations (ASEAN) – an intergovernmental organisation of 10 Southeast Asian countries (Inoue, 2024). Bilateral "linkages" that have already been or are being launched between members are expected to help "position ASEAN at the forefront of QR payment integration globally" (Monetary Authority of Singapore, 2024).

A multilateral memorandum of understanding on payment connectivity has also been signed between Indonesia, Malaysia, the Philippines, Singapore, and Thailand. For example, Malaysian users of the CIMB mobile banking app would be able to transfer money to KTB app users in Thailand by scanning a QR code they generated and vice versa (Bank of Thailand, 2024). Meanwhile, an Indonesian tourist may scan a merchant's QR code in Malaysia, with Rupiah-Ringgit conversion being instantly processed (Kominfo, 2023; BCA, 2023). Such interoperability between banking apps across borders can create a more integrated and accessible financial ecosystem in the region.

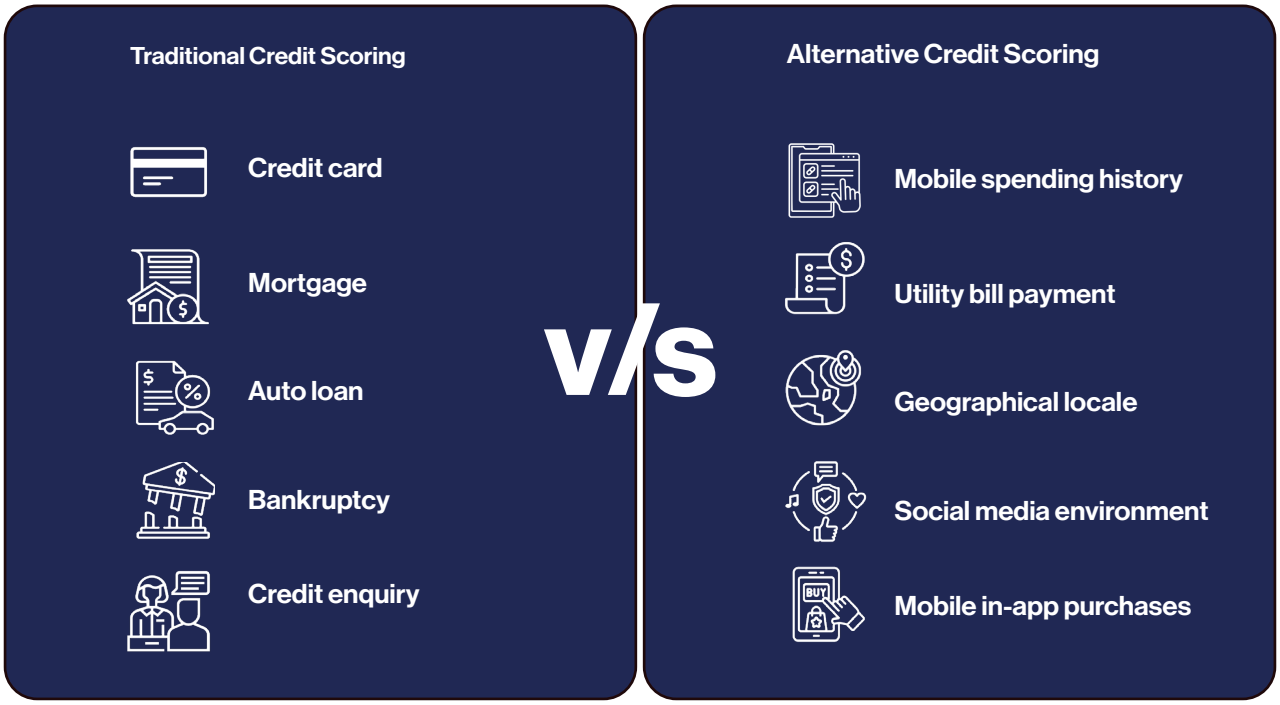
Efforts to facilitate cross-border transactions using QR codes are in part supported by governments' desire to increase the use of local currency transactions and to drive better regional payment connectivity (Medina, 2023). Such linkages will not only deepen regional economic integration but will also facilitate tourism, consumer spending, and remittance flows (BCA, 2023). However, as integrated payment systems often require the exchange of personal data between countries, these developments raise questions over how individuals' data is transferred, stored and protected across borders.

Digital Lending

Digital lending applications and other tech help provide loans to consumers through digital means. However, the process is not limited to the conversion of traditional paper-based, in-branch bank loan applications into digital ones. In recent years, fully digital lenders have emerged, operating exclusively online via mobile apps and offering quick credit services without the need for physical branches. These "alternative finance" channels enhance financial inclusivity and enable underbanked and unbanked individuals to access funds beyond what the traditional financial institutions offer (CCAF and ADBI, 2022). Peer-to-peer lending became the most funded fintech sector in ASEAN-6 markets (Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam) in 2023, making up 32 per cent of fintech startup investment at US$408 million (UOB, 2023).

People underserved by traditional banking systems, however, may lack formal credit history, which hinders their ability to use conventional credit scoring methods to obtain loans from financial institutions. This has prompted the development of alternative credit data sources-something that involves intensive processing of personal data. As shown in Figure 1, alternative credit scoring relies on other means for credit underwriting, such as payment behaviour and personal spending habits through various means including social media activities (Goh, 2023). The issue that arises then, however, is that although leveraging personal data can enhance financial inclusion by providing lenders the means to assess the creditworthiness of individuals even without formal credit histories, such extensive processing of personal data can also raise significant privacy and data security concerns. This is particularly true if this wide range of data is transferred across national borders.

Figure 1: Differences between traditional and alternative credit data



It is worth noting that existing plans for regional cross-border connectivity in digital lending are focused on micro-, small- and medium-sized enterprises (MSMEs) rather than on individuals. This is the current case between Singapore and Cambodia as part of the Financial Transparency Corridor (Sarat, 2024). MSMEs do indeed account for between 97 to 99 per cent of total business establishments in Southeast Asia and play an important role in the economy of these countries (ASEAN, no date). But this focus is new, diverging from the primary regional market for P2P lending, which traditionally targets consumer lending underserved by the banking system (UOB, 2024). The trend also runs contrary to the popularity of cross-border consumer P2P lending in other regions, notably the more mature markets of Europe, America, and China since 2005 (ADB, 2023). Nevertheless, as many MSMEs across the region are run by single operators, they can also benefit from the use of these alternative data to determine their credit worthiness (Sarah, 2024; Yulius et al., 2023b; Konsyg, 2023).

Digital Wealth

Digital wealth solutions have started gaining traction in Southeast Asia, not only with digitalisation of traditional wealth services in developed financial markets such as Singapore, but also as a response to the growing wealth of the rapidly expanding yet underserved middle class in developing markets (additiv, 2024; KPMG, 2021).

Notably, despite the increasing wealth across the region, the use of traditional wealth management services remains low and primarily serves relatively niche demands such as Islamic financing, and in turn has left a significant portion of population in Southeast Asia underbanked (additiv, 2024; KPMG, 2021). At the same time, it is also a part of wider trend of "embedded finance" or "orchestrated finance", where investment products are offered digitally in conjunction with other financial products (Zylstra, 2023). For example, on their mobile banking platforms, banks may include wealth features like investment portfolios, offering additional services such as virtual investment options and insights, real-time remote portfolio monitoring and digital financial advice.

Since personalisation is a key of wealth management services, personal data can form the backbone of digital wealth management products that may provide both personalised investment portfolios and other tailored advisory solutions digitally (Ghanem, 2020; Nanayakkara et al., 2023). This includes the use of analytics tools such as a 'robo-advisor' that relies on machine learning and artificial intelligence to tailor wealth management offerings to customer needs, based on personal information they choose to share, not only relying on their financial information (Wong, 2024).

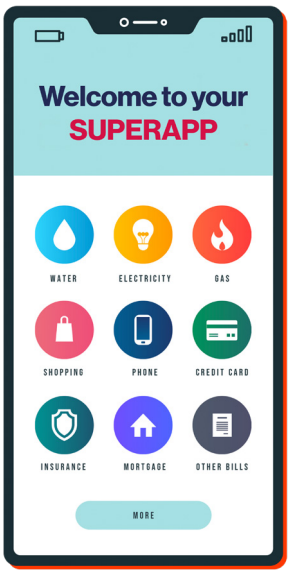
As for cross-border connectivity of wealth technologies, regional financial centre Singapore is experiencing increasing flows beyond Southeast Asia, including Hong Kong (Banerjee et al.,2023). At the same time, customers within the region, such as in Malaysia, currently seek out Singaporean traditional wealth management providers for their needs, since these services are not widely available at home (APIB, 2021). Digital wealth services such as Singapore-based StashAway offer retail wealth management and investment solutions to retail investors. However, depending on the service, they may only be available for Singapore citizens and foreigners residing in the country (StashAway, no date). The deployment to other countries can face personal data restrictions.

For example, Indonesia has strict rules on the transfer of personal data across borders, so firms may need to establish their ecosystem onshore to use fully utilise personal data in innovations like robo-advisors. Currently, companies like StashAway rely on partnership with traditional players such as Citi to use their existing infrastructure (Citi, 2020).

1.2.3 Features supporting digital financial services in Southeast Asia

Digital financial services in Southeast Asia, ranging from digital payments to digital lending and digital wealth management, are increasingly using online platforms such as mobile banking apps and 'super-apps', front end apps that open the way to a wide variety of digital services – the latter being a key trend in the region's digital finance industry (Asian Banking & Finance, 2022).

Figure 2: Super-apps bundle multiple services



Companies are developing their digital platforms to provide a one-stop service that integrates financial products into a range of digital services as shown in Figure 2. This includes "embedded finance" solutions such as digital payments, digital lending, and digital wealth management. For example, GoTo's super-app Gojek has GoPay, GoPayLater, and GoInvestasi, which are payment, consumer credit, and investment solutions respectively. Grab's platform offers payment and insurance products in addition to their primary ride-sharing function.

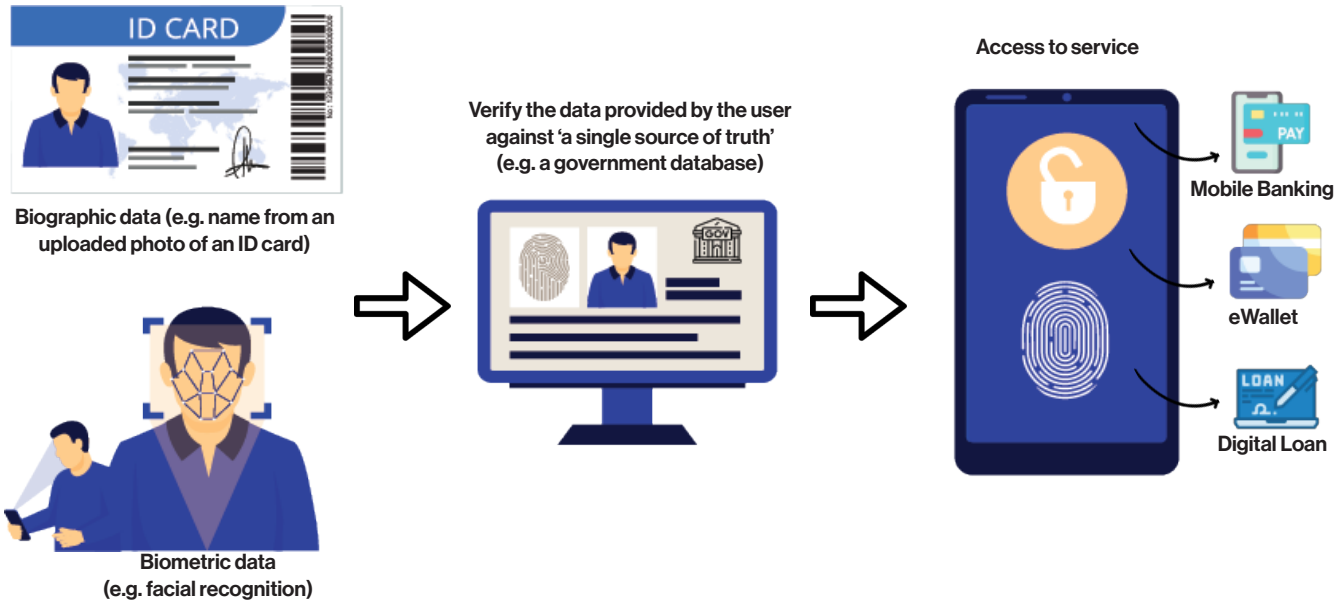
Another feature supporting Southeast Asian digital financial services is an **electronic Know Your Customer (eKYC) process.** This enterprise solution underpins digital financial services, particularly because it involves extensive use of personal data to provide secure ways of verifying customer identities.

The adoption of eKYC has been a major element of Southeast Asia's digital financial services market. Whether digital services are offered by traditional banks or fintech startups, they all rely heavily on the ability to authenticate and verify users. Providers are usually required by regulators to verify that a user is the person they claim to be, to efficiently prevent fraud and money laundering.

As eKYC processes often rely on national ID systems and are generally designed to comply with local regulations, they typically need to be performed within the country where the financial services are being offered.

For example, service providers may verify customer identity with the government's electronic databases such as civil registries as their "single source of truth" as shown in Figure 3.

Figure 3: electronic Know Your Customer (eKYC)



Furthermore, businesses' ability to "know their customers" forms the backbone of consumer trust, as both scrutiny and susceptibility to fraud can also contribute to the provider's positive or negative reputation. It can also serve as basis for future innovations that rely on customer profiling, including data analytics.

1.3 Relationship between personal data regulations and digital financial services

Consumer-focused digital financial services such as digital payments, digital lending and digital wealth management rely heavily on the processing of personal data. Data protection regulations, while essential for safeguarding consumer safety and privacy, can pose regulatory hurdles to digital financial service providers' cross-border operations. This is especially so when personal data regulations are fragmented across different countries, as in Southeast Asia.

Data protection regulations reassure consumers that their sensitive information is secure, because digital services are "critically premised on trust, underpinned by robust personal data protection and security of systems across the region" (ASEAN and USAID, 2021, p. 24). These regulations also alleviate concerns over the risks of storing personal information digitally (World Bank, 2019). This "digital trust" plays a significant role in filling the financial inclusivity gap, as rejection by consumers would mean a setback to enabling unbanked and underbanked populations to access financial services digitally.

However, inconsistent data protection standards between countries can cause significant challenges for business compliance and operational efficiency. Unlike the EU, which has adopted GDPR standards as a bloc, Southeast Asia has a fragmented landscape of personal data protection regulations arising from the diverse approaches and varying levels of regulatory development across the countries. This inconsistency complicates efforts to establish a cohesive digital economy in Southeast Asia and poses regulatory complexity for businesses operating in different countries within the region.

The next section will assess how the lack of interoperability in data protection regulations in Southeast Asia can hamper the seamless operation of consumer digital financial services. It will discuss the four primary characteristics which hamper the interoperability of personal data regulations in the region: the level of maturity of data regulations, bespoke rules specific to industries, unaligned data transfer requirements and differences in the legal terminology adopted by each country.

Section Two:

Southeast Asia's fragmented personal data regulatory framework

With personal data becoming increasingly regulated in Southeast Asia, one of the primary concerns is the lack of interoperability of the regulations across different jurisdictions. This fragmentation of regulations can obstruct both the use and integration ofdigital financial services within the region, creating hurdles to seamless cross border operations of businesses that rely heavily on the handling of personal data. It risks creating operational inefficiencies and barriers for businesses operating or seeking to operate in the region by adding up compliance costs, as they seek to meet different rules in each country (Goodman and Risberg, 2021; Parekh et al., 2022).

As it stands, Southeast Asia's regulatory regimes consist of diverse and often incompatible national regulations on the use and movement of personal data (ADB, 2023). These differences include restrictions on data transfer (requiring specific conditions to be met before transferring data abroad) and requirements for data localisation (requiring citizens' or residents' data to be stored and processed within the borders of that country).

Regional fragmentation has four primary characteristics. They comprise the varying maturity levels of comprehensive personal data regulations; differing cross-border data transfer requirements; bespoke regulations on specific industries; and the lack of commonality in legal definitions. This fragmentation is illustrated in Table 3.

Table 3: Variations of personal data protection (PDP) regulations across Southeast Asia

Country	Comprehensive PDP regulations	Unique cross-border transfer conditions	Relevant bespoke regulations	Examples of different legal definitions
Indonesia	Yes	Notification to relevant authorities	Financial services regulation	
Malaysia	Yes	Consent OR transfer to locations designated by Minister responsible		
Philippines	Yes	Ensure contractual obligation for protection		
Singapore	Yes	Consent AND transfer to locations with equivalent legal obligation		Unique definition of "consent" 1) individuals need to be informed of purposes 2) not being the precondition for using products or services
Thailand	Yes	Consent OR transfer for internal use within business group subjected to prior approval	Credit bureau regulations	
Vietnam	Yes	Onshore copy of data	IT, consumer protection, cybersecurity regulations	
Brunei	No			
Cambodia	No			
Lao PDR	No		Law on Electronic Data Protection	No legal definition of personal data but may fall into the category of sensitive electronic data
Myanmar	No		Electronic Transactions Law	

2.1 Varying maturity levels of personal data regulations

Southeast Asian countries exhibit varying levels of maturity in their personal data regulations, with some having comprehensive laws and others lacking robust frameworks. Maturity in this sense refers to the extent to which the laws adopted by ASEAN members provide overarching regulation on personal data, which can range from comprehensive to non-existent. Comprehensive personal data rules tend to cover the collection, use and disclosure of the data: they provide "one-stop", non-conflicting conditions for businesses as to how the data must be handled.

Within Southeast Asia, the countries with mature personal data regulatory regimes are:

- **Indonesia**: *Law No. 27 of 2022 concerning Protection of Personal Data*
- **Malaysia:** *Personal Data Protection Act 2010*
- **The Philippines:** *Data Privacy Act of 2012*
- **Singapore:** *Personal Data Protection Act 2012*
- **Thailand:** *Personal Data Protection Act B.E.2562 [2019]*
- **Vietnam:** *Personal Data Protection Decree 2023*

All these countries have comprehensive personal data regulations that address cross-border transfer in a generally similar manner. These rules usually have equivalent clauses that prescribe how and when organisations may transfer personal data across borders, specifying what conditions must be satisfied to do so.

At the time of this report, other Southeast Asian countries – Brunei, Cambodia, Lao PDR, and Myanmar – had yet to adopt comprehensive data protection legislation. Consequently, they do not have unified, overarching regulations to address the cross-border transfer of personal data. The variation on how personal data transfers may take place can be sharp. In Cambodia, forexample, there is no legislation whatsoever that addresses either cross-border personal data transfer or data protection in general, with only data belonging to the Ministry of Interior being clearly regulated (DLA Piper, 2024b).

Adding to the complexity, countries without comprehensive regulations may introduce limited or ad hoc rules partially governing a specific form of data or a particular type of activity. Lao PDR, for example, has not enacted personal data protection rules, which means that use of the data may be authorised on an ad hoc basis dependent on category – general, sensitive, or prohibited (DLA Piper, 2024c).

Moreover, the lack of unified legislation also means that organisations have to keep track of multiple amendments and new legislation, reducing the legal certainty of business activities in a given jurisdiction. For example, if data transfer is made between countries with more mature regimes – such as between Thailand and Malaysia – aligned regulatory requirements help simplify compliance, particularly because both countries share rules on user consent. Conversely, if the data transfer is between a country with mature regulations and one without - say, between Singapore and Cambodia – companies may face difficulties.

The disparity in the maturity of regulatory regimes can hinder cross-border flow of personal data. For example, under the data protection laws of Malaysia, Singapore, and Thailand, the principle is that personal data transferred outside their borders may only go to a recipient located in a country with "sufficient" or "equivalent" data protection measures in place (Personal Data Protection Act 2010, Art. 129; Personal Data Protection Act 2012, Part 3(9), 3(10); Personal Data Protection Act B.E.2562 [2019], Section 28, 29). Inadequate protections in the receiving country can lead to prohibitions or severe restrictions on data flow to prevent potential misuse or inadequate safeguarding of sensitive information. Financial institutions may also face legal obligations that require them to ensure that personal data transferred internationally is protected according to specific standards.

2.2 Variation in personal data transfer requirements

Beyond the existence and maturity of personal data regulations, the legal requirements for cross-border personal data transfers can vary considerably from one country to another, even among those with comprehensive and mature data protection regulations based on similar basic principles. This variation increases operational complexities for business. Each country may prescribe its own specific criteria for data transfers across jurisdictions, and these criteria can differ in what is acceptable, as well as the exceptions allowed. As such, even countries with robust regulatory frameworks do not necessarily have laws that are interoperable with one another.

The following four countries all have mature regulatory regimes, yet:

- In **Malaysia,** data transfer can be made a) to jurisdictions that the relevant government minister has designated as having equivalent regulations, or b) when the subject of the data has consented to the transfer, or c) if it is necessary to fulfil contractual obligations (Personal Data Protection Act 2010, Art. 129).

- **Singapore** prescribes that transfer can only be made to destinations with enforceable data protection, and only if approved by the subject of the data after having the details of such protective measures explained to them (Personal Data Protection Act 2012, Part 3(9), 3(10)).

- In **Thailand**, data transfer is allowed only to locations that the Data Protection Commission considers as having sufficient protection, unless the business has previously been specifically allowed to transfer data overseas within their organisation (Personal Data Protection Act B.E.2562 [2019], Section 28, 29).

- In contrast, **Indonesia** still maintains regulations that address the handling of personal data separately from comprehensive law. In particular, the Ministerial Regulations No. 20 (2016) on the Protection of Personal Data in Electronic System (Art. 22) require that plans and results of overseas personal data transfer be reported to relevant authority, including its destination, recipient, date, and purpose.

These variations in legal requirements for cross-border personal data transfer, even in countries with mature personal data regulatory frameworks, make data transfers more complex. Businesses must stay vigilant to avoid inadvertently breaching regulations, even among countries with similar regulatory principles.

2.3 Bespoke industry-specific regulations

Bespoke regulations relevant to personal data in Southeast Asia exist in various forms, ranging from targeting specific sectors to ad hoc data protection. This diversity adds an additional layer of complexity for financial institutions. For the financial sector, a country may prescribe additional regulations such as requiring banks to localise financial data. At the same time, other countries may also adopt digital-only regulations, leading to different regulatory requirements for financial service providers depending on whether they process personal data through traditional or digital channels.

Across Southeast Asia, Vietnam is the country that relies most heavily on bespoke rather than comprehensive laws to regulate personal data. It has three primary laws relevant to data protection and data storage: the Law on Information Technology (2006), the Law on Protection of Consumers' Rights (2010), and the Law on Cybersecurity (2018) (Data Guidance, 2024). In particular, the cybersecurity legislation has a provision that may be considered a type of data localisation. It prescribes that providers of cyber services must store a copy of personal data within Vietnam's borders for a period specified by the government (Law on Cybersecurity 2018, Art. 26(3)). While this regulation does not prohibit data transfer altogether, it adds an additional layer of complexity onto the operations of digital financial services providers in Vietnam.

Jurisdictions with comprehensive regulations on personal data may also include clauses on specific business sectors. One example is **Thailand,** where the credit bureau industry is exempted from general data protection if activities being undertaken are necessary (Personal Data Protection Act B.E.2562 [2019], Section 4(6)). Instead of overarching regulations, Thai laws prescribe that specific regulations governing credit businesses are applicable instead.

Another example is **Indonesia**, where the financial service sector is specifically regulated under OJK Regulation 11 POJK.03/2022. It prescribes that the establishment of data processing activities outside Indonesia by commercial banks are subject to approval (OJK Regulation 2022, Art. 35(3)). This puts a limit on the ability of firms to share data across borders, as business activities involving personal data must be located onshore in Indonesia unless otherwise approved case-by-case.

To further complicate matters, **comprehensive personal data regulations may still override bespoke regulations.** For example, **Thailand's** law states that some provisions "shall apply regardless of whether they are repetitious" to sector-specific rules (Personal Data Protection Act B.E.2562 [2019], Section 3(1)). While this helps unify some data protection requirements under the umbrella of the same legislation, it can also add a layer of uncertainty by forcing businesses to be aware of how different regulations interact.

In short, bespoke industry-specific regulations relevant to personal data, and even digital data in general, can introduce additional complexities for financial institutions operating across different jurisdictions. In particular, they oblige companies to ensure compliance with not just data protection law but additional industry-specific data handling requirements that differ between countries.

2.4 Lack of commonality in legal definitions

The lack of common legal definitions and their interpretation creates unpredictability in how regulations apply to digital financial services. The extent to which different regulatory regimes do not "speak the same language" as one another directly affects the legal certainty of data transfer regulations across ASEAN. If similar terms are defined differently or carry different legal interpretations across different jurisdictions, this can lead to discrepancies in what businesses face.

For example, the definition of key terms such as "consent" can vary considerably in each piece of legislation. In the case of **Singapore**, the personal data protection law recognises "consent" when sufficient information about the purpose of data collection, use, and disclosure has been provided, and does not simply consider that an individual has given consent if it is required as a condition for providing a product or service (Personal Data Protection Act 2012, Art. 13-15, 15A).

In contrast, **Malaysia** and **Thailand** do not clearly specify what would amount to consent under the law. Such divergence means that it would be much more complicated for firms to truly receive customer consent under Singapore's stringent requirements: the consent that may have been sufficient in Malaysia or Thailand can easily be non-compliant in Singapore.

In short, the lack of interoperability between personal data regulatory regimes across Southeast Asian countries means that the landscape is complex and difficult for firms to navigate, adding compliance cost for digital financial service providers that operate across the region (UNDP, 2021).

Furthermore, additional complexities such as the differences in specific regulatory nuances can also lead to inadvertent non-compliance as service providers struggle to keep up with a wide variety of legal intricacies. The compliance risks created by fragmentation can have a wide variety of negative impacts, ranging from monetary penalties to damage to reputation and consumer trust – which is the lifeblood of financial services (CDC, 2018).

In the next section, this report will discuss the experiences of industry experts across the fragmented regulatory landscape in Southeast Asia, how businesses navigate such complex environments, and missed opportunities the financial sector could have embraced if personal data regulatory regimes in the region were interoperable.

Section Three:

How the consumer digital financial services industry is experiencing Southeast Asia's fragmented regulatory environment

As outlined, the current regulatory environment for personal data use in Southeast Asia is peppered with diverse rules and standards. This lack of regulatory interoperability poses challenges for many businesses, but especially for digital financial services (Long, 2023; Parekh et al., 2022). Fragmentation may lead to inconsistencies and complexities in data handling practices, making it difficult for financial institutions to effectively navigate the requirements for managing and using customer data across different jurisdictions. It can also obstruct smooth flow of data across borders. In turn, this can increase the cost of conducting business in more than one jurisdiction, especially compliance costs and long-term operational expenditures. It is also a barrier to upfront investment.

Despite this, interviews with digital financial services providers in the region indicate that the lack of regulatory interoperability across the region is not an overarching obstacle. For one, personal data rules – fragmented or otherwise – are not entirely negative for digital financial services aimed at individual consumers. Regulations can determine all-important consumer trust in digital financial services, thus merely having them is critical to the businesses of both banks and fintech firms. Meanwhile, digital financial service providers suggested that negative impacts of fragmentation can be mitigated through various strategies, discussed below along with opportunities being missed as a result of fragmentation.

For financial services, it is all a matter of prioritisation. For example, the focus of local banks and fintech firms has been on growing their digital products to expand the domestic customer base rather than on pushing for regional interoperability in personal data regulations. As mentioned in Section 1, local markets continue to remain significantly underserved by financial services. This prompts companies offering digital financial services to commit significant resources to capturing the new market, putting the immediate side-effects of regulations posed by the lack of interoperability to a secondary status. At the same time, large multinational banks with a global presence have extensive experience in operating within fragmented regulatory landscapes across the world. Their familiarity with complex regulatory environments equips them to effectively navigate the diverse markets across Southeast Asia if needed.

> **Providers of digital financial services accept the status quo due to prioritisation, preferring to place more importance on maintaining trust before actively attempting to reduce compliance costs.**

3.1 Building consumer trust through compliance

Since financial services are fundamentally built on trust, regulations help maintain this trust even when they are not regionally interoperable. Consumer trust is widely recognised as a vital component in the adoption and advancement of digital financial services in Southeast Asia (Kim et al., 2022). Interviews with financial sector businesses and regulators in the region revealed a consensus that regulation is directly linked to consumer trust in financial services. The mere presence of fundamental regulations such as for personal data protection, and the fact that businesses must comply with such regulations is viewed as one of the deciding factors for whether consumers would perceive businesses as safe, reliable and trustworthy enough to use. Therefore, stringent and non interoperable personal data protection regulations are not a significant concern for these key stakeholders as they seek to build their market.

Regulatory strictness also affects the perception of reliability and trustworthiness of financial services in Southeast Asia. The region's financial services industry has been characterised by strict regulation. Dedicated regulatory institutions such as central banks as well as other relevant authorities (such as the Monetary Authority of Singapore or the OJK in Indonesia) have been highly proactive in closely scrutinising firms under financial and banking legislations, specialised licences, and other requirements specific to the sector. As a result, this underpins how trust can be fostered between consumers and businesses.

Any gaps that could undermine trust would defeat one of the primary goals of digitalising the Southeast Asian financial sector: financial inclusivity. As previously mentioned, financial inclusion is one of the primary objectives for the financial sector that leads them to deploy digital solutions. However, there would simply be no point for them to digitalise if the very target at which their digital products is aimed – the segment of population previously underserved by conventional banking services – does not trust them and refuses to come onboard as users. This consideration has so far led digital financial services providers to prioritise compliance rather than actively trying to reduce compliance costs.

3.2 Reduction in efficiency does not present an insurmountable obstacle

While regulatory fragmentation may lead to reduced efficiency, it is not an insurmountable obstacle for businesses. One of the reasons that regulatory fragmentation can remain at low priority during expansion is that it has so far had limited effects on both established and new businesses.

Firstly, legacy banks in the region – both regional and multinational – usually have an established presence and ecosystem in place upon which they can build their digital services. That means the significant compliance costs required for entering the market entry have largely been made. This is especially true for the major international banks which have always been operating in a fragmented regulatory environment around the world – from Europe to the Middle East, Africa, the Americas and Asia Pacific. As a result, the complexity of regional regulations does not necessarily prevent these banks from providing their digital financial services across borders.

Secondly, critical aspects of consumer finance in Southeast Asia are heavily localised due to financial regulatory requirements and market conditions. The discussions with industry players suggested that digital financial services tended to be developed locally and delivered in each country due to business regulations such as licensing. This means that processes that require personal data to work, such as user-authentication in eKYC, are largely conducted within the confines of national borders to comply with local data protection and privacy regulations. Since these processes are currently managed within individual jurisdictions, the limitations on cross-border data flow due to regulatory fragmentation is less relevant. For example, a multinational bank operating in multiple countries might still verify the identity of its local customers through its business entities in each country, and with the government authorities of that country. It would not need to transfer data across borders.

Similarly, local fintech firms typically operate primarily within their domestic markets or separately in other markets, often without the need to transfer personal data internationally. If these firms do not need to offer their products in another jurisdiction or to operate across borders, the upfront compliance cost and limitations on cross-border flow caused by fragmentation can be minimal.

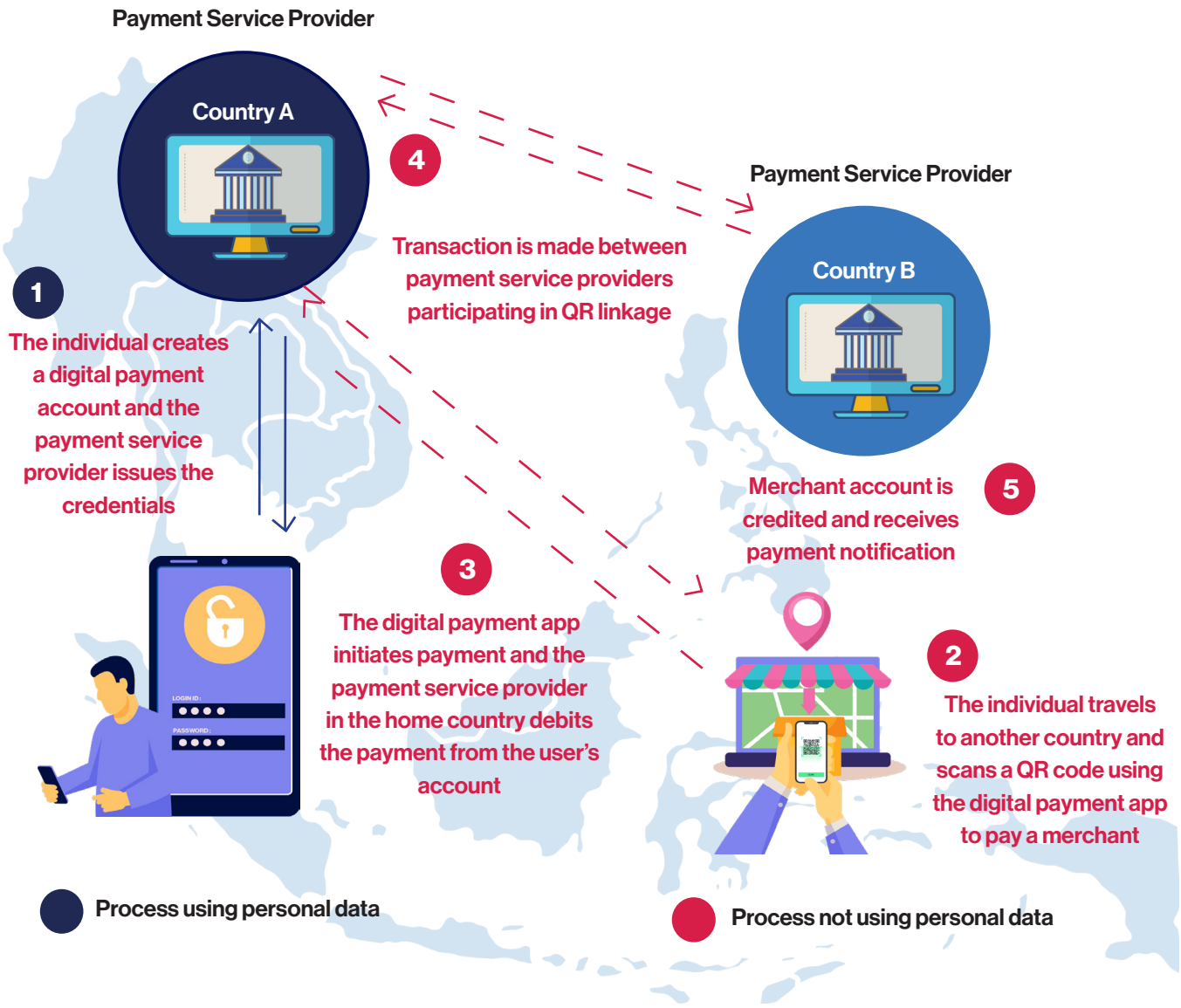
As a result, the lack of regulatory interoperability due to fragmentation does not necessarily become a "pain point" for many providers of digital financial services. This has rendered the cross-border interoperability of personal data regulations within Southeast Asia less of an immediate issue for banks and fintech firms.

3.3 Strategies for navigating regulatory fragmentation

Digital financial service providers that do face fragmentation barriers have adopted innovative work-around strategies as regional integration led by governments and regulatory bodies in Southeast Asia has deepened (Yulius et al., 2023a). Circumventing the fragmentation of regulations – not regulations themselves – through these strategies can help businesses and other stakeholders in the financial services sector to mitigate the challenges posed by the lack of regulatory interoperability.

One such measure is the privacy by design approach, including the use of so-called *privacy-enhancing techniques.* Through this method, businesses design their service offerings in a way that inherently avoids interaction with the differences in regulatory requirements. This approach can take the form of adhering to the "data minimisation" principle, which means that the use of personal data is avoided as much as possible unless such data is necessary for the service. This principle includes using digital solutions that do not require sharing personal data across borders, and thus inherently limits any concern about regulatory interoperability. For example, using Southeast Asia's existing cross-border interoperable QR payment link, firms can conduct eKYC checks on customers locally and issue credentials that do not contain consumers' personal data. Banks or intermediaries process any relevant personal data within their local jurisdictions and provide eKYC electronic credentials back to the businesses without personal data being transferred. This means that if a traveller from Thailand uses a QR code to pay a merchant in Malaysia via a mobile banking app, the transaction can rely on credentials issued by their bank in Thailand (Figure 4). As such, their personal data stays within Thailand and is not transferred overseas to Malaysia with their payment information.

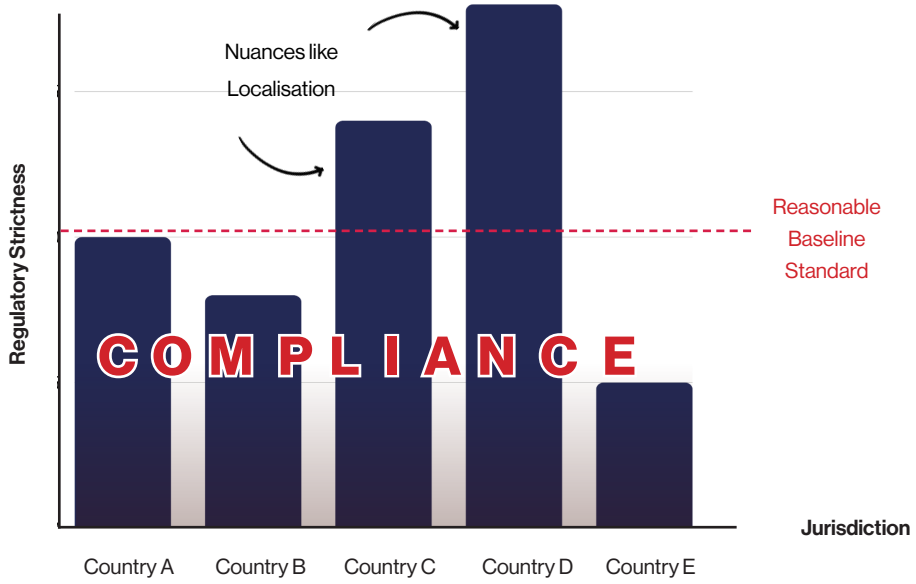
Figure 4: Simplified example of cross-border QR payment



Another approach is proactive self-regulation. Under this measure, businesses adopt the strictest reasonable baseline standard – such as the EU's GDPR – across their entire business regardless of which market they operate in. This means personal data is handled under a standard either equivalent to or well above the basic rules of most countries, making them mostly compliant in multiple jurisdictions no matter what personal data regulatory requirements may be prescribed locally (Figure 5).

By being proactive in self-regulation, digital financial service providers can meet regulatory requirements in different jurisdictions, even across those with different maturity levels, to maintain trust and minimise the risk of reputational damage due to non-compliance. In cases where that existing baseline is insufficient, these banks can make minimal adjustments to their compliance procedures to meet specific requirements, such as data localisation.

Figure 5: Self-regulating via baseline standard policy



Digital financial service providers can also work around fragmented regulations by relying on third-party providers to outsource compliance workload and minimise the cost of conducting business. This can be in the form of hosting service on the enterprise cloud servers of major providers such as Amazon (AWS), Microsoft (Azure), or Google (GCP) to comply with localisation requirements without the need to invest in their own local in-house data centres. Companies can also choose to form partnerships with intermediaries to handle all cross-border data transfer activities while financial service providers only handle domestic data processing. As a result, financial service providers would not need to bear the burden of navigating the fragmented regulatory landscape on their own.

These work-arounds suggest not only that providers of digital financial services remain interested in cross-border activities despite consumer finance being heavily localised, but also that they will not remain passive. Banks and fintech firms do not necessarily wait for personal data regulations to be interoperable across the region before deploying cross-border products or services targeted at individual consumers. In short, regulatory harmonisation – while desirable – is not necessarily a precondition for business.

3.4 Missed opportunities remain

None of this is to say that a fragmented regulatory landscape has no negative impact: there are many missed opportunities. The fragmented personal data regulatory regimes across Southeast Asia lack a cohesive regulatory environment necessary for businesses to further improve and innovate effectively. For example, unaligned cross-border data transfer rules and localisation requirements can complicate efforts for digital financial service providers to centralise data processing activities in regional hubs or share data across national branches.

> **While fragmentation may not present a major issue for businesses, regulatory interoperability can eventually make business stakeholders better off by enabling improvements in effectiveness and efficiency, including through the adoption of new innovations.**

As such, harmonising regulations across the region could further improve business and unlock innovation. This is particularly relevant for businesses that want to operate beyond the confines of their domestic markets. Even though consumer financial products are heavily localised, industry experts from financial services providers that are operating across multiple jurisdictions have suggested that the more data can be shared across different jurisdictions, the more efficient and effective such services can be.

For example, if regional regulatory regimes are interoperable and allow for easier cross-border flows of digital data, including personal data, it would be simpler for businesses to offer services from a centralised regional hub. This would not only lower the cost of doing business due to the economy of scale, but firms could offer higher quality, more secure services by concentrating resources and talents in a single location. Data-sharing also allows firms to improve resilience. For example, a data centre in Singapore may be able to act as an offshore backup for another data centre in Thailand, ensuring minimal disruption if an onshore data centre were to fail.

At the same time, data-sharing can also increase the scope of innovation. For example, with the rise of artificial intelligence, the larger and richer the dataset, the more effective data analytics can be. As a result, access to customer data translates into an improvement in risk management as well as the ability to tailor services to customer needs. In turn, achieving regulatory interoperability would help support the expansion and integration of digital financial markets in Southeast Asia by making such data more widely available under sufficient protective measures.

In addition, interoperability can make deployment of digital solutions in a new market easier. Industry experts said it can be simpler to introduce products or services into a market which operates under the same rules and principles that already exist than into an entirely new regulatory environment. Under such conditions, a multinational bank or digital wealth app already operating in Singapore, Indonesia, and Thailand would be able to more easily expand to neighbouring Lao PDR and Cambodia, providing consumers with more choices and digital financial service options.

Recognising the advantages of regional economic integration and the opportunities lost due to regulatory fragmentation, ASEAN has undertaken several initiatives to enhance personal data regulatory interoperability and support the growth of region's digital economy at the multilateral level. The following section will explore various ASEAN initiatives aimed at managing personal data flows across member states, as well as the challenges associated with their adoption. It will also explore additional obstacles to harmonising personal data regulations – member countries' capacity to implement standards set by ASEAN-wide agreements.

Section Four:

ASEAN's works on regulatory interoperability

Southeast Asian countries have been making continuous efforts to improve personal data regulatory interoperability via ASEAN. The regional grouping aims to promote economic and security cooperation among its 10 members: Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. The consensus among ASEAN states is that a harmonised legal and regulatory environment across the region is imperative for digital economic development. They consider data to be "the lifeblood of the digital economy" and as such requires a "forward-looking and enabling framework" (ASEAN, 2018, pp. 1, 5).

Significant challenges remain, however, due to the diversity of regulations and the varying national approaches to data protection. Furthermore, ASEAN-level initiatives are non-binding, making the creation of a new regulatory landscape complex.

4.1 ASEAN agreements and frameworks related to personal data protection

ASEAN has, nonetheless, made notable efforts to address the issue of jurisdictional differences in digital data management regulations, including for personal data. It has introduced ASEAN- wide initiatives to help stakeholders navigate the regulatory landscape more easily.

Major efforts at the ASEAN level include, but are not limited to:

1. The ASEAN Framework on Personal Data Protection (2016), which sets out general principles on data protection. On cross-border data flow, for example, this framework states that the transfer of data should be based on consent or that the protection is consistent with other principles listed in the framework (ASEAN, 2016). These principles include the idea of using data only to the extent necessary for a specific purpose, so-called "data minimisation" (ASEAN, 2016).

2. The ASEAN Framework on Digital Data Governance (2018), which prescribes strategic priorities, principles, and initiatives as a guidance for members to use as the basis for their digital data regulations. This framework explicitly emphasises that safeguards and regulations, especially on cross-border flow, need to be harmonised and minimised to reduce business compliance costs and to foster innovation (ASEAN, 2018, p. 5).

The framework further spawns three different mechanisms:

- **The ASEAN Data Management Framework,** which develops a data governance structure and safeguards, and encourages the adoption of existing standards such as those of the ISO, the International Organization for Standardization (ASEAN, 2021a).

- **The ASEAN Cross Border Data Flows Mechanism,** which addresses regulatory certainty on how cross-border transfers can be made. It consists of two main parts: 1) the ASEAN Model Contractual Clauses (MCC) for Cross Border Data Flows and 2) the ASEAN Certification for Cross Border Data Flows (the latter had not yet been endorsed at the time of this report). ASEAN MCC is a template for terms and conditions that can be applied by the parties involved in the transfer of data across borders (ASEAN, 2021b). Since the data protection maturity level is different between countries and there is no permanent regional mechanism to transfer data across borders, having a template reduces uncertainty for recipient companies across the region by providing them with clear and consistent methods (Personal Data Protection Commission Singapore, 2023).

- **The ASEAN Data Protection and Privacy Forum** formed an annual meeting for discussion between regulators and policymakers (National Privacy Commission of the Philippines, 2019). Here, relevant authorities are expected to share data regulation know-how to develop best practices together and to assist ASEAN states that do not possess relevant regulations and/or regulatory bodies to establish them (GSMA, 2019). However, the extent to which these best practices have been adopted in the establishment of data protection bodies among the member states remains unclear.

3. The ASEAN Regulatory Pilot Space for Cross-Border Data Flows (2019), which is a sandbox created in cooperation with the mobile network operators' GSM Association in 2019. Essentially, the sandbox is a controlled, "safe space" in which solutions can be tested. It allows for "trial and error" and highlights the real-world benefits of freer data flow by providing evidence on the efficiency advantages that new mechanisms would give to countries that adopt them (GSMA, 2019). Nevertheless, at the time of this report, the sandbox had not yet demonstrated a tangible result for digital financial services personal data flow.

4.2 Challenges to ASEAN-wide initiatives

While ASEAN countries have introduced several tools at the multilateral level to help governments in Southeast Asia build interoperable personal data regulations, they still fall short of creating a significant breakthrough. Despite the efforts and clear vision of interoperable regulatory regimes, personal data regulations within major ASEAN economies continue to be largely fragmented. There are several underlying issues that may contribute to this lack of progress, including how the agreements are designed to work and the challenges each jurisdiction faces in implementing them consistently.

The first issue is the non-binding nature of ASEAN-level initiatives. Unlike the EU, which has the power to pass legally binding regulations such as the GDPR, ASEAN's initiatives are often non-binding and rely on consensus among member states. The recurring feature of ASEAN multilateral efforts is that they are mainly guidelines and loose standards. Some examples are:

- **The Framework on Personal Data Protection** states that it is simply "a record of the Participants' intentions", essentially providing no legal obligations in any way domestically or internationally. It also emphasises that the principles provided in the document are not binding or enforceable (ASEAN, 2016, p. 2).
- **The Data Management Framework** specifically provides "voluntary and non-binding" guidelines and does not oblige any jurisdiction to define or classify data under similar standards of data management (ASEAN, 2021a, p. 8). It is designed to introduce "best practice" by acting as a model for both public and private sector entities, but it has never aimed to constitute a legal or regulatory tool (ASEAN, 2021a, p. 8).
- **The Cross-Border Data Flow Mechanism** is also intended to help create "voluntary baseline standards", especially for adoption by SMEs without existing data transfer arrangements (ASEAN, 2021c). As such, states are neither required to promote them nor encouraged to prescribe their use. It also allows the use of other mechanisms such as ISO standards. While this ensures flexibility on paper, it also undermines certainty for stakeholders by letting states opt for other standards.

The non-binding nature of these agreements undermines their effectiveness in enforcing uniform data protection standards across the region.

Without binding commitments, inconsistencies in implementation and adherence are likely to arise due to diversity in governance and economic development approaches.

A second issue is the domestic obstacles within each country, particularly the capacity to implement standards set by ASEAN-wide agreements. The implementation of these standards must be done at the national level. However, even with agreed standards, real-world implementation processes can also vary depending on the institutional and technical capacity of each country. For example, despite having a comprehensive data protection law since 2022, Indonesia still does not possess its own national data protection authority, although it is in the process of establishing one at the time of this writing (Mokoginta and Tisnadisastra, 2024).

According to the ASEAN Digital Integration Index – which includes institutional and infrastructure readiness as one of its six pillars – ASEAN members are at different levels of readiness for digital economy integration (ERIA, 2023). Some ASEAN states with a higher level of readiness, such as Singapore, can use personal data management and protection standards more easily than others, especially in terms of technical capacity such as existing digital infrastructure. Readiness also includes other aspects including institutional capacity, for example, the ability of enforcement authorities or political incentives to adopt these standards in domestic laws and implement them.

4.3 Is the ASEAN Digital Economy Framework Agreement (DEFA) the solution?

To address these persisting issues, ASEAN and its members have continued to push for the introduction of additional ASEAN-level agreements. The primary work-in-progress is the ASEAN Digital Economy Framework Agreement (DEFA), which has been under formal negotiation since 2023 and is expected to be finalised by the end of 2024, brought forward from the original plan to be launched in 2025 (Asia House, 2024). The primary objective of DEFA is the "establishment of common rules and principles" for various aspects of the digital economy across Southeast Asia. This inevitably includes addressing the digital personal data regulatory policies at the regional level. Since DEFA is expected to be a regionwide legally-binding instrument on digital economy, it differs from other past ASEAN initiatives, being a hard law and a treaty with legal obligations and dispute settlement provisions (ASEAN, 2023a; Hsien-Li, Sze- Wei and Foo, 2024).

The formulation of DEFA emerged after ASEAN leaders signed the Bandar Seri Begawan Roadmap in 2021, which laid the foundation for the integration of the ASEAN digital economy and affirmed their interest in establishing a region-wide framework to ensure the interoperability of digital economy systems (ERIA, 2023). Government representatives interviewed for this report indicated the agreement is being built on a set of inputs that produced a "checklist" of what past initiatives worked and what additional efforts are required.

ASEAN has received input from both the public and private sector, the latter ranging from MSMEs to large corporations (ASEAN, 2023b). Central banks and other financial regulators, business associations, and multinational banks also provide input. Relying on such feedback means ASEAN and its members can make an informed decision with a clear vision for the regional digital economy – and by extension, personal-data regulatory regimes and the digital finance industry.

In short, DEFA is primarily meant to be a continuation of previous efforts rather than a completely new set of common rules and principles, while introducing the idea of it being legally binding. This should, in theory, address the previous issue of the lack of compulsory, enforceable measures that plague previously adopted frameworks and mechanisms. This includes ensuring that the countries without data protection regulations and authorities would take necessary steps to establish such regulations and regulating bodies in accordance with the best practice shared across the region.

At the time of writing, the actual text of DEFA has yet to be published, so it remains to be seen how broad or detailed the clauses will be, and in turn how much effect it may have on the members' commitment in the real world.

4.4 Commitment-capacity mismatch: an obstacle to harmonisation

There is a disparity between commitment and capacity that continues to be a significant barrier to harmonising personal data regulations across Southeast Asia. Even though the DEFA aims to address the capacity gap between different countries, the capacity-building process cannot be forced upon their economies.

DEFA has the potential to address relevant public sector capacity issues in some Southeast Asian countries. The agreement, for example, can help incentivise the creation of dedicated government agencies responsible for the digital economy as well as personal data protection.

In accordance with their pledged commitment, countries would be establishing a dedicated regulating body responsible for data protection, which would build up institutional capacity that had previously been lacking, as in the previously mentioned case of Indonesia.

Digital readiness, however, is equally driven both by private entities and the broader population. In other words, while joining legally binding international agreements can demonstrate political commitment from governments, it does not guarantee that a country will be able to effectively implement them. For example, the differences in digital literacy in civil society across the region may lead to persisting lack of digital trust in some countries and more openness in others, making the alignment between countries and regional integration more difficult.

4.5 Securing Southeast Asia's place on the world stage through harmonised regulatory environment

Ensuring seamless regional integration through an effective, enabling, and interoperable regulatory environment is crucial for positioning Southeast Asia effectively in the international arena. The regional ambition to be at the forefront of the digital economy globally is reflected in various ASEAN "world first" initiatives, such as the Digital Economy Framework Agreement (ASEAN, 2023a). However, as the region emerges as a leading digital market in sectors such as e-commerce, policymakers and regulators are struggling to keep pace (World Economic Forum, 2023). As such, how they address the current regional fragmentation will shape the future of digital governance in Southeast Asia. Enhancing digital interoperability could pave the way for greater interconnectedness with other parts of the world and demonstrate that Southeast Asia can serve as a practical role model, which is essential for the region to become a global leader in the digital economy.

In summary, there have been extensive efforts to improve regional regulatory interoperability of personal data at the multilateral level through ASEAN. However, earlier initiatives were hindered by limitations such as their non-binding nature and a capacity divide. The upcoming Digital Economy Framework Agreement is expected to address such limitations by building on the experience of earlier initiatives. This will also be a fundamental step in determining where Southeast Asia could stand on the global stage. Business stakeholders across the region will presumably welcome this, even if, as mentioned in Section 3, they are already responding to demand without waiting for fully established interoperability.

Section Five:

What now for Southeast Asia's digital finance?

The digital financial service industry in Southeast Asia continues to evolve alongside the development of regional personal data regulatory landscape. Businesses have already devised strategies to work around the currently fragmented environment, not remaining static until full regional interoperability is reached. However, this can also introduce undesirable side effects such as additional cyber risks. Meanwhile, the extent to which digital finance benefit from interoperability also hinges on the market's progress, both via technological innovation within the industry and the readiness of consumers themselves.

5.1 Side effects of compliance choices

The choices made by businesses to remain compliant in a fragmented regulatory landscape may have negative repercussions. Because digital financial services rely heavily on trust, just a single weak link or even non-malicious disruption in their services can cause reputational damage as well as potential regulatory penalties. For example, at the time of writing, Singapore's DBS bank faced a six-month ban on non-essential activities and was required by the Monetary Authority of Singapore to have approximately SG$1.6 billion (US$1.2 billion at the time of this report's publication) additional regulatory capital set aside as a buffer against risk (Tan, 2024). The trigger was multiple digital-service disruptions from unidentified causes.

From a cybersecurity perspective, maintaining an organisation's own control over personal data is important for the data's confidentiality, integrity and availability. This means that the trend of financial service providers to limit cost while remaining compliant by relying on third-party intermediaries – a current workaround – could introduce cyber vulnerabilities. For example, if data centres used by banks are managed by third party providers, banks may not be able to guarantee that there is no unauthorised access. Nor would they be able to ensure that no one can "flip the switch" and render their services inoperable. While cybersecurity measures can be taken to ensure resilience and mitigate such risks, they can increase costs which businesses may be trying to avoid by using third-party intermediaries. This can ultimately undermine the purpose of making these choices in the first place.

To illustrate, Indonesia is a jurisdiction that requires data to be hosted locally. This has prompted foreign banks to host their services onshore. Yet Indonesia's cybersecurity standard is plagued with a track record of data breaches, including in financial services. One example is the case of Bank Syariah Indonesia's data breach in 2023 (Nadarajah et al., 2024). Even if third party intermediaries are operating on local safety standards, overseas digital financial service providers must still closely scrutinise the level of security in order to mitigate their risks. In addition, experts also suggest that while privacy enhancement techniques such as anonymised credentials can help firms remain compliant while bypassing barriers posed by the fragmented regulatory landscape, they must also constantly make sure that the data being transferred is truly "sanitised" and contain no personal data.

5.2 Limited prospects for innovation slows down urgency

Meanwhile, the benefits of regulatory harmonisation still depend heavily on the market for specific products or services. There is currently little development of innovations requiring cross-border personal data regulatory interoperability, one of the reasons that financial institutions have assigned a lower priority to advocating for such interoperability. Interviews with digital finance experts indicate that they do not expect much change in this area in the foreseeable future. Consider, for example, a regionally-recognised digital ID system that can enable identity verification under the same standard within the entire region. According to experts, the introduction of such a digital ID is still in the very early stage even domestically, and there is limited coordination between different national government gencies responsible for ID systems. Cross-border usage such as Singaporean nationals using Singpass to prove their identities to Indonesian banks and vice versa remains far away.

5.3 Improvements in grassroot digital and financial literacy are key

Readying consumers and by extension propelling markets and innovation, depends largely on the improvement in grassroot digital and financial literacy. As outlined in Section 1, the bane of financial sector in Southeast Asia is getting consumers to use their services. Since both digital and financial knowledge form the foundation for consumer engagement with digital financial services – from simply accessing them to moving beyond basic services like e-wallets to more sophisticated products – improving their literacy is essential for the future (Kim et al., 2022).

In short, as Southeast Asia's digital finance develops in parallel to the region's personal data regulations, its trajectory continues to be shaped by the industry players' own choices and market dynamics. These factors underscore how businesses need to carefully balance operating costs with risks that can undermine their foundation – consumer's trust in safe and reliable digital financial services – and how much can they reap the benefits of interoperability.

Section Six:

Conclusion

Governments in Southeast Asia are increasingly regulating the use and movement of personal data, moves that affect the blossoming digital financial services industry throughout the region. Through digitalisation, the financial sector is expanding its consumer market, regularly seeking personal data collected from consumers as the basis for innovations. However, with each country in the region developing its own personal data regulations, the legal landscape is fragmented, making navigating compliance requirements across jurisdictions difficult and costly, and restricting the smooth cross-border flow of data essential to many digital solutions.

Faced with this, businesses are seeking workarounds rather than waiting for promised harmonisation. Their resources and attention are focused primarily on increasing digital finance penetration into a large underserved market, with the interoperability of regulations a secondary priority, at least for now. There is little objection to data-use regulations per se; in general, they are considered useful for fostering consumer trust. And the current lack of interoperability across jurisdictions – while potentially expensive – can be overcome, especially by large, experienced global companies and by local players that do not engage in extensive cross-border transfer of data.

Ultimately, however, cost remains one of the underlying factors for any successful business. Even if firms can absorb additional costs incurred in the current Southeast Asian regulatory landscape, once the cost of compliance becomes higher than the returns, business cannot be viable. In other words, if the cost required for firms to comply with regulations within a specific jurisdiction passes the acceptable threshold set by themselves, the market would cease to be attractive. This would have significant spill-over effects on regional growth and emerging consumer wealth. As such, any additional efficiency and flexibility improvements – both in technical areas and business operations – that arise from making the region's personal data regulations interoperable would stimulate business competitiveness and economic growth.

Accordingly, efforts to enhance regional regulatory interoperability of personal data have been advancing at the multilateral level through ASEAN. Significantly, new mechanisms are expected to be stronger than previous efforts to end fragmentation. Whereas ASEAN's early efforts to harmonise digital regulations across the region tended to be non-binding and hampered by different countries' capacities, the upcoming Digital Economy Framework Agreement is expected to be legally binding and take some steps towards narrowing the capacity gap.

In the meantime, many industry players are not waiting. Discussions with industry stakeholders suggest that they are actively looking for opportunities to expand their digital offerings across the region despite the lack of interoperability. Many businesses are implementing measures to circumvent fragmentation issues. This may come in the form of "privacy by design" to avoid the differences in regulatory requirements, proactive self- regulations or outsourcing their data storage needs.

Overall, digital financial service providers will deliver solutions that comply with regulations, but caveats remain. No matter how complex the regulatory environment is to navigate, complying with the rules is the bottom line for businesses in the financial sector. Banks and fintech firms may tolerate or employ measures to manage the regulatory complexity in Southeast Asia, but each decision comes with its own set of considerations. This includes evaluating whether the business is viable given the compliance costs, safety concerns, and potential missed opportunities.

The way forward boils down to striking a balance of interests between stakeholders. This can include sovereignty, consumer protection, economic development, competitiveness, trust, cost, and technical considerations. In the case of Southeast Asia, governments may retain primacy over regulatory policy decisions to assert sovereignty over data, while businesses are weighing how to balance trust, cost, and opportunities while operating in that regulatory landscape.

Currently, regulators, businesses, and civil societies are working together to create progressive, forward-looking standards of governance across the region. These are complemented by bottom-up activities like increasing digital awareness and literacy among consumers of digital financial services, which is also crucial not only in addressing the mismatch between commitment and capacity, but also the region's market dynamics. As both digital financial services and personal data regulations in Southeast Asia remain constantly evolving, these interactions will continue to shape the future of data governance in the region and help define its place on the world stage.

Bibliography

AAA Global (2024), Riding the Wave: Exploring the Phenomenal Growth of Fintech in Southeast Asia. Available at: https://aaaglobal.co.uk/blog/exploring-the-phenomenal-growth-of-fintech-in- southeast-asia/
(Accessed 7 August 2024)

ADB (2023), Financial Digitalization and Its Implications for ASEAN+3 Regional Financial Stability. Available at *https://www.adb.org/sites/default/files/publication/857596/financial-digitalization-asean3-financial-stability.pdf*
(Accessed 1 May 2024)

additiv (2024), Consumer Study 2024: Embedded Finance Opportunity in Southeast Asia. Available at: *https://www.additiv.com/insights/embedded-finance-seasia-consumer-study-2024/*
(Accessed 30 July 2024)

AFI (2019), Digital Financial Services: Basic Terminology. Guideline Note No. 19. Available at: https://www.afi-global.org/sites/default/files/publications/2016-08/Guideline%20Note-19%20DFS-Terminology.pdf
(Accessed 20 June 2024)

APIB (2021), Growing Champions: Vast wealth management potential in Malaysia but players need to restructure operating model. Available at *https://apdib.com/growingchampions-vast-wealth-management-potential-in-malaysia-but-players-need-to-restructure-operating-model/* (Accessed 7 August 2024)

ASEAN (2016), Framework on Personal Data Protection. Available at *https://asean.org/wp- content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf*
(Accessed 14 March 2024)

ASEAN (2018), Framework on Digital Data Governance. Available at *https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf*
(Accessed 14 March 2024)

ASEAN (2021a), ASEAN Data Management Framework. Available at *https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf*
(Accessed 14 March 2024)

ASEAN (2021b), ASEAN Model Contractual Clauses for Cross Border Data Flows. Available at *https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border- Data-Flows_Final.pdf*
(Accessed 14 March 2024)

ASEAN (2021c), Implementing Guidelines for ASEAN Data Management Framework and ASEAN Cross-border Data Flows Mechanism. Available at *https://asean.org/wp- content/uploads/2021/08/Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows.pdf*
(Accessed 14 March 2024)

ASEAN (2023a), 10th ASEAN Economic Community Dialogue unpacks world's first regionwide framework agreement on digital economy. Available at *https://asean.org/10th-asean-economic- community-dialogue-unpacks-worlds-first-regionwide-framework-agreement-on-digital-economy/*
(Accessed 30 July 2024)

ASEAN (2023b), Digital Economy Framework Agreement (DEFA): ASEAN to leap forward its digital economy and unlock US$2 Tn by 2030. Available at *https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/*
(Accessed 3 July 2024)

ASEAN (no date), Development of Micro, Small and Medium Enterprises in ASEAN - Overview.
Available at: *https://asean.org/our-communities/economic-community/resilient-and-inclusive-asean/development-of-micro-small-and-medium-enterprises-in-asean-msme/overview/ (Accessed 31 July 2024)*

ASEAN and USAID (2021). ASEAN Digital Integration Index: Measuring Digital Integration to
Inform Economic Policies. Available at: *https://asean.org/wp-content/uploads/2021/09/ADII- Report-2021.pdf*
(Accessed 19 February 2024)

Asia House (2024), ASEAN's Digital Economic Framework Agreement may be in place by the end of 2024. Available at: *https://asiahouse.org/news-and-views/aseans-digital-economic-framework-agreement-may-be-in-place-by-the-end-of-2024/*
(Accessed 22 June 2024)

Asian Banking & Finance (2022), How are superapps changing the digital banking landscape? Available at: *https://asianbankingandfinance.net/banking-technology/exclusive/how-are-superapps-changing-digital-banking-landscape* (Accessed 22 June 2024)

Bain & Company and Facebook (2021), Southeast Asia, the home for digital transformation: A SYNC Southeast Asia Report. Available at: *https://www.facebook.com/business/news/southeast-asia-the-home-for-digital-transformation* (Accessed 30 July 2024)

Banerjee, A. Deuble, S. Kaushik, V. Kotanko, B. and Sengupta, J. (2023), McKinsey & Co.: WealthTech in Asia–Pacific: The next frontier in financial innovation. Available at: *https://www.mckinsey.com/industries/financial-services/our-insights/wealthtech-in-asia-pacific-the-next-frontier-in-financial-innovation* (Accessed 7 August 2024)

Bank of Thailand (2024), Cross-border Payment Linkages. Available at: *https://www.bot.or.th/en/financial-innovation/digital-finance/digital-payment/cross-border-payment.html* (Accessed 1 August 2024)

BCA (2023), Countries Where You Can Make Cross-Border QR Transactions via BCA mobile. *https://www.bca.co.id/en/informasiEdukatips/2023/05/11/10/48/ini-dia-negara-yang-bisa-transaksi-qris-lintas-negara-cross-border-lewat-bca-mobile* (Accessed 30 July 2024)

Bender, Y. (2023), Professional Wealth Management, Financial Times, London: Asia's rising prosperity creates boom market for wealth management. *https://www.pwmnet.com/asias-rising-prosperity-creates-boom-market-for-wealth-management.* (Accessed 1 August 2024)

CCAF, ADBI and FinTechSpace (2019), ASEAN Fintech Ecosystem Benchmarking Study. Available at: *https://www.jbs.cam.ac.uk/wp-content/uploads/2022/12/2022-ccaf-asean-access-to-digital-finance-study.pdf* (Accessed 20 June 2024)

CDC (2018), Principles for assessing risk to customers in financial services. Available at: *https://assets.bii.co.uk/wp-content/uploads/2018/12/05151151/Principles-for-assessing-risk-to-customers-in-financial-services.pdf* (Accessed 13 August 2024)

Citi (2020), Non-bank Financial Institution Casebook. Available at *https://www.citi.com/tts/sa/flippingbook/2020/CITI_NBFI_Casebook/20/index.html* (Accessed 7 August 2024)

Data Guidance (2024), Vietnam - Summary. Available at *https://www.dataguidance.com/jurisdiction/vietnam* (Accessed 14 March 2024)

DLA Piper (2024a), Data Protection Laws of the World. Available at: *https://www.dlapiperdataprotection.com/* (Accessed 19 February 2024)

DLA Piper (2024b), Data Protection Laws of the World: Cambodia. Available at: *https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=KH* Accessed 19 February 2024)

DLA Piper (2024c), Data Protection Laws of the World: Laos. Available at: *https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=LA* (Accessed 19 February 2024)

ERIA (2023), Understanding the ASEAN Digital Economy Framework Agreement: A Means to Support ASEAN Integration. Available at *https://www.eria.org/uploads/media/policy-brief/FY2023/Understanding-the-ASEAN-Digital-Economy-Framework-Agreement.pdf* (Accessed 3 July 2024)

Ghanem, E. (2020),Capgemini Belgium: A Hyper-Personalized Wealth Management Client Journey is Becoming Table Stakes. Available at: *https://www.capgemini.com/be-en/insights/expert-perspectives/a-hyper-personalized-wealth-management-client-journey-is-becoming-table-stakes/* (Accessed 20 June 2024)

Goodman, M.P. and Risberg, P. (2021), Center for Strategic and International Studies, Washington DC: Governing Data in the Asia-Pacific. Available at: *https://www.csis.org/analysis/governing-data-asia-pacific* (Accessed 1 May 2024)

Google, Temasek, and Bain & Company (2019), Fulfilling its Promise: The future of Southeast Asia's digital financial services. Available at: *https://www.bain.com/globalassets/noindex/2019/bain-report-fulfilling-its-promise.pdf* (Accessed 30 July 2024)

GSMA (2019), White Paper: Advancing the ASEAN-GSMA Policy Dialogue on Cross Border
Data Flows. Available at *https://www.gsma.com/asia-pacific/wp-content/uploads/2019/11/ASEAN-Sandbox-Proposal-EXTERNAL-_Final_20190403.pdf*
(Accessed 14 March 2024)

Habir, M. and Negara, D. (2023), ISEAS, Singapore: The Digital Transformation of Indonesia's Banking Sector: Current Trends and Future Prospects. Available at: *https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2023-78-the-digital-transformation-of-indonesias-banking-sector-current-trends-and-future-prospects-by-manggi-habir-and-siwage-dharma-negara/*
(Accessed 30 July 2024)

HSBC (2022), A 3D view of Southeast Asia: demographics, digitisation and dynamism.
Available at: *https://www.business.hsbc.com/en-gb/insights/growing-my-business/a-3d-view-of-southeast-asia*
(Accessed 7 August 2024)

Hsien-Li, T., Sze-Wei, C. & Foo, Y. (2024), Tech for Good Institute, Singapore: Unveiling the ASEAN Digital Economy Framework Agreement (DEFA): An Overview of its Origins, Substance, and Legal Structure. Available at: *https://techforgoodinstitute.org/blog/expert-opinion/unveiling-the-asean-digital-economy-framework-agreement-defa/#:~:text=As%2the%20pioneering%20binding%20regional,%2C%20and%20long%2Dterm%20horizons.*
(Accessed 30 July 2024)

Indonesia. Law No. 27 of 2022 concerning Personal Data Protection [UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI]. Available at:
https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf [Indonesian]
(Accessed 14 March 2024)

Indonesia. OJK Regulation 11 11/POJK.03/2022 [Peraturan OJK 11/POJK.03/2022
Penyelenggaraan Teknologi Informasi Oleh Bank Umum]. Available at:
https://ojk.go.id/id/regulasi/Documents/Pages/Penyelenggaraan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%2011%20-%2003%20-%202022.pdf [Indonesian]
(Accessed 14 March 2024)

Inoue, K. (2024), Nikkei: ASEAN finance chiefs agree to expand cross-border QR payments.
Available at: *https://asia.nikkei.com/Politics/International-relations/ASEAN-finance-chiefs-agree-to-expand-cross-border-QR-payments*
(Accessed 20 June 2024)

Kapron, Z. (2024), Forbes: The Southeast Asia Fintech Sector is at an Inflection Point. Available at: *www.forbes.com/sites/zennonkapron/2024/02/09/the-southeast-asia-fintech-sector-is-at-an-inflection-point/*
(Accessed 20 June 2024)

Kim, J., Tan, M., Lim, A. and Aboucabar, M. (2022), Tech for Good Institute, Singapore: Digital
Financial Services for Financial Inclusion in Southeast Asia.
Available at: *https://techforgoodinstitute.org/wp-content/uploads/2022/10/TFGI_DFSFIISA-Report_111122.pdf*
(Accessed 20 June 2024)

Kominfo (2023), QRIS Simplifies Payments in ASEAN Countries.
Available at: *https://asean2023.id/en/news/qris-simplifies-payments-in-asean-countries*
(Accessed 20 June2024)

Konsyg (2023), Southeast Asia's SME Backbone: Emerging Entrepreneurs. Available at: *https://konsyg.com/2023/11/20/southeast-asias-sme-backbone/*
(Accessed 13 August 2024)

KPMG (2021), Digital Wealth Management in Asia Pacific.
Available at *https://asean.org/our-communities/economic-community/resilient-and-inclusive-asean/development-of-micro-small-and-medium-enterprises-in-asean-msme/overview/*
(Accessed 22 June 2024)

Lee, J. (2023), World Economic Forum: Is ASEAN on the cusp of fulfilling its long-held promise? Available at: *https://www.weforum.org/agenda/2023/01/is-asean-on-the-cusp-of-fulfilling-its-long-held-promise-davos-2023/*
(Accessed 7 August 2024)

Li, X. (2022), The Diplomat: Southeast Asia's Data Localization Push Is a Double-Edged Sword.
(Accessed 20 June 2024)

Long, K. (2023), The Banker: Data residency laws frustrate Asian banks' cross-border activity.
Available at: *https://www.thebanker.com/Data-residency-laws-frustrate-Asian-banks-cross-border-activity-1674470200 .*
(Accessed 20 June 2024)

Macquarie Capital (2022), Delivering digital financial inclusion in Southeast Asia. Available at: *https://www.macquarie.com/au/en/insights/delivering-digital-financial-inclusion-in-southeast-asia.html*
(Accessed 20 June 2024)

Malaysia. Personal Data Protection Act 2010, Available at: *https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf*
(Accessed 14 March 2024)

Medina, A. F. (2023), ASEAN Briefing: ASEAN to Increase Local Currency Trade, Reducing Reliance on the US Dollar. Available at: *https://www.aseanbriefing.com/news/asean-to-increase-local-currency-transactions-reducing-reliance-on-the-us-dollar/*
(Accessed 31 July 2024)

Mokoginta, P. and Tisnadisastra, A. A. (2024), International Comparative Legal Guides: Data Protection Laws and Regulations Indonesia 2024 *https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia*
(Accessed 7 August 2024).

Monetary Authority of Singapore (2024), Joint Statement of the 11th ASEAN Finance Ministers' and Central Bank Governors' Meeting. Available at: *https://www.mas.gov.sg/news/media-releases/2024/joint-statement-of-the-11th-asean-finance-ministers-and-central-bank-governors-meeting*
(Accessed 20 June 2024)

Nadarajah, H., Iskandar, A., Lee, S. and San, S. T. (2024), Asia Pacific Foundation of Canada: Indonesian Government Under Fire Following String of Cyber Breaches. Available at *https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches*
(Accessed 1 August 2024)

Nanayakkara, N., Wightman, M., Birkin, A., Lee, M. and Hennessey, P. (2021), Ernst & Young Global: How digitalization can drive personalization in wealth management. *https://www.ey.com/en_se/wealth-asset-management/how-digitalization-can-drive-personalization-in-wealth-management*
(Accessed 20 June 2024).

National Privacy Commission of the Philippines (2019), Philippines leads ASEAN move to protect privacy. Available at: *https://privacy.gov.ph/2019/08/ph-leads-asean-move-to-protect-privacy/*
(Accessed 14 March 2024)

Parekh, S., Reddin, S., Rowshankish, K., Soller, H. and Strandell-Jansson, M. (2022), McKinsey (global): Localization of data privacy regulations creates competitive opportunities. Available at: *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities*
(Accessed 1 May 2024)

Personal Data Protection Commission Singapore (2023), Remarks by Deputy Commissioner, Mr Yeong Zee Kin, at the IAPP Global Privacy Summit. Available at: *https://www.pdpc.gov.sg/news-and-events/press-room/2023/06/remarks-by-deputy-commissioner,-mr-yeong-zee-kin,-at-the-iapp-global-privacy-summit-on-5-april-2023,-at-dc,-washington*
(Accessed 14 March 2024)

Sangfor Technologies (2023), What is Data Localization? A Special Focus on Southeast Asia.
Available at:
https://www.sangfor.com/blog/cloud-and-infrastructure/what-is-data-localization-a-special-focus-on-se-asia
(Accessed 20 June 2024)

Sarat, O. (2024), ASEAN-Japan Centre, Tokyo: The ASEAN-Japan Insights Webinar Series: The Future of Cross-Border Digital Payment Systems in ASEAN and Japan [Webinar]. Available at *https://www.asean.or.jp/en/event-report/20240202/*
(Accessed 31 July 2024)

Sarah, M. (2024), J-PAL, Cambridge, MA.: Using alternative data and artificial intelligence to expand financial inclusion: Evidence-based insights. *https://www.povertyactionlab.org/blog/3-21-24/using-alternative-data-and-artificial-intelligence-expand-financial-inclusion-evidence*
(Accessed 1 August 2024)

Singapore. Personal Data Protection Act 2012. Available at: *https://sso.agc.gov.sg/Act/PDPA2012#top*
(Accessed 14 March 2024)

StashAway (no date), What document would I need to open an account?. Available at:
https://www.stashaway.sg/help-center/900000812046-what-document-would-i-need-to-open-an-account
(Accessed 13 August 2024)

Tan, A. (2024), Straits Times: MAS to ensure DBS identifies root cause of recent disruptions and addresses it effectively. Available at: *https://www.straitstimes.com/singapore/mas-to-ensure-dbs-identifies-root-cause-of-recent-disruptions-and-addresses-it-effectively*
(Accessed 14 August 2024)

Thailand, Personal Data Protection Act B.E.2562 [2019]. Available at:
https://data.thailand.opendevelopmentmekong.net/en/laws_record/2562/resource/ec616be5-9fbf-4071-b4b5-cb1f3e46e826 [English translation]
(Accessed 14 March 2024)

The Philippines, Data Privacy Act of 2012. Available at: *https://privacy.gov.ph/data-privacy-act/*
(Accessed 14 March 2024)

UNDP (2021), Enabling Cross-border Data Flow: ASEAN and Beyond. Available at:
https://www.undp.org/sites/g/files/zskgke326/files/2021-10/enabling-cross-border-data-flow-asean-and-beyond-report.pdf
(Accessed 13 August 2024)

UOB (2023), FinTech in ASEAN 2023: Seeding the green transition. Available at:
https://forms.uob.com.sg/eservices/techecosystem/fintech-in-asean-2023.html
(Accessed 20 June 2024)

Vietnam, Law on Cybersecurity 2018. Available at:
https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf [English translation]
(Accessed 14 March 2024)

Vietnam, Personal Data Protection Decree 2023. Available at:
https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx
[Vietnamese]
(Accessed 14 March 2024)

Wong, S. (2024), 1AP Capital, Singapore: What Are Robo Advisors In Singapore And Are They Safe To Invest In?. Available at *https://www.1apcapital.com.sg/what-are-robo-advisors-in-singapore-and-are-they-safe-to-invest-in/*
(Accessed 7 August 2024)

World Bank (2019), ID4D Practitioner's Note: Digital ID and the Data Protection Challenge.
Available at *https://documents1.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf*
Accessed 19 February 2024)

World Bank (2021), The use of Quick-Response Codes in Payments. Available at
https://fastpayments.worldbank.org/sites/default/files/2021-10/QR_Codes_in_Payments_Final.pdf
(Accessed 1 August 2024)

Yulius, Tjhin, D., Lukiman, Y., Sjahrir, P., Yu, Y. and Wijaya, V. (2023a), Boston Consulting
Group (global): Interoperable QR Code Payment Ecosystem in ASEAN: What it Means for the World. Available at: *https://web-assets.bcg.com/9c/ac/72af6ed244c39123f679ffc899ee/bcg-asean-interoperable-qr-code-payment-ecosystem-in-asean.pdf*
(Accessed 31 July 2024)

Yulius, Tjhin, D., Lukiman, Y., Wijaya, V., Yu, Y., Chew, Y. X. and How, Q. Y. (2023b), Boston Consulting Group (global): Digital Lending Can Turn the Dial on Financial Access for MSMEs.
Available at: *https://web-assetsbcgcom/55/2ca18c9a1453dac65c7e8e35c5d15/bcg-asean- digital-lending-can-turn-the-dial-on-financial-access-for-msmes.pdf*
(Accessed 7 August 2024)

Zylstra, P. (2023), Hubbis, HK: The Rise of Digital Wealth Management in the Growth Markets of ASEAN. Available at:
https://www.hubbis.com/article/the-rise-of-digital-wealth-management-in-the-growth-markets-of-asean
(Accessed 20 June 2024)

Appendix

Research methodology

The research for this report employed a qualitative approach and sought to understand how personal data regulatory fragmentation affects digital financial services in Southeast Asia. The questions that the study aimed to answer were:

- What is the current personal data regulatory landscape in Southeast Asia?
- How do key stakeholders view the role of personal data regulations in shaping digital financial services in Southeast Asia?
- What measures are being taken to improve the interoperability of personal data regulations in the region?
- How do stakeholders respond to such interoperability improvement measures?

To address these questions, the research was conducted using two primary methods: semi- structured interviews and document analysis.

Semi-structured interviews

Thirteen semi-structured interviews with a range of participants representing different stakeholder groups were conducted. They included experts from the digital financial services industry and other supporting industries, policy practitioners, and representatives from governments and international organisations in Southeast Asia.

Prior to the interview, each respondent was given a reference document which outlined a summary of the research, objectives of the interview, and key themes to be discussed. The document also included the assurance that their responses will not be directly quoted in the report unless otherwise agreed, and that all information would be anonymised and retain no link to their name or organisation.

The interviews were conducted remotely via either Zoom or Microsoft Teams platforms and lasted between 20 to 40 minutes. It was optional for participants to consent to the recording of the conversation for the purposes of transcription and analysis. Eleven recorded interviews were transcribed manually. Notes of key insights from the two unrecorded interviews were created immediately after the conversation.

Document analysis

This part of the research involved reviewing existing laws, multilateral agreements, official publications, media releases, and other literature to identify recurring terminology and triangulate the findings.

Thematic analysis

To answer the key questions of the research, thematic analysis was manually conducted on the transcripts, interview notes, and documents to determine recurring themes and key patterns.