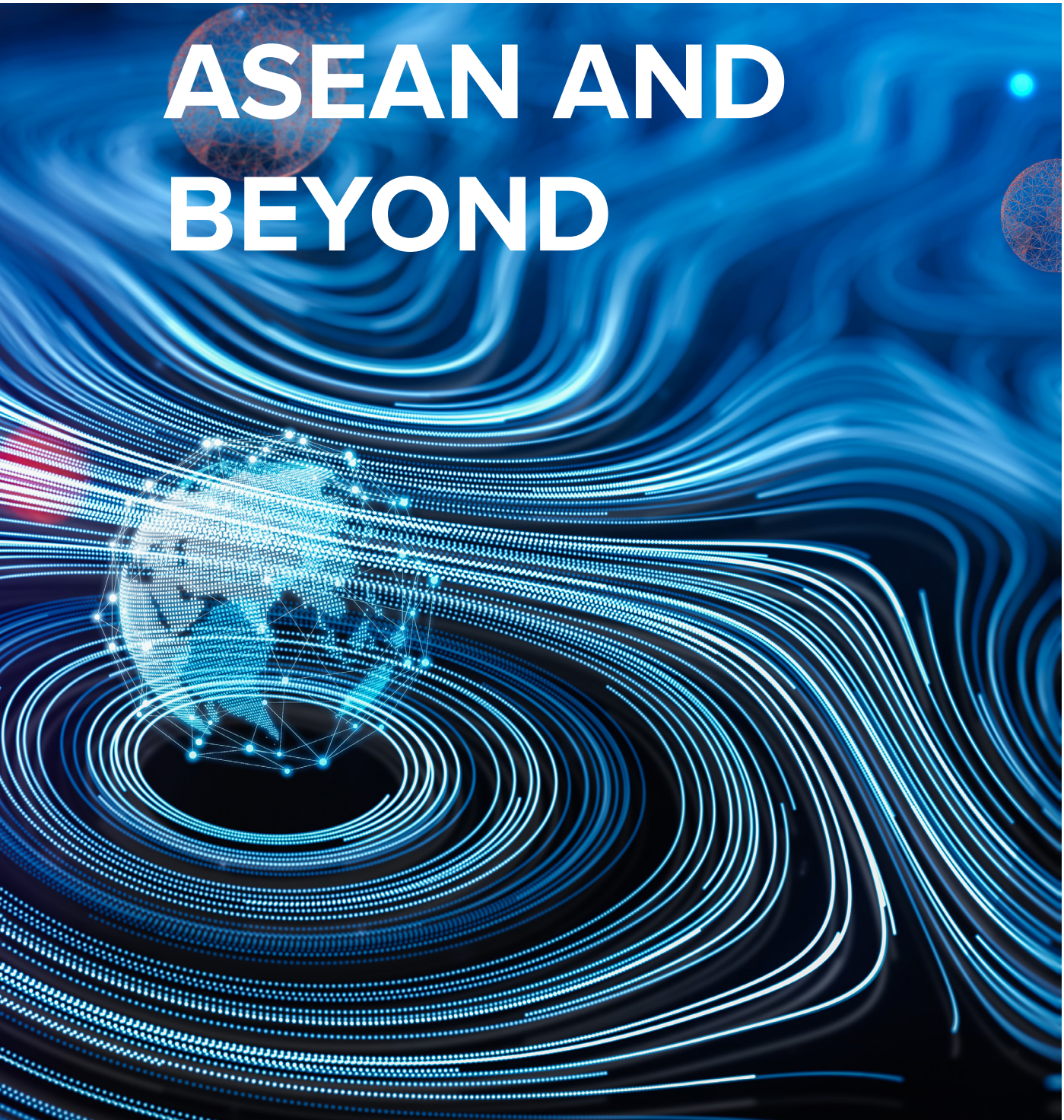
ENABLING CROSS-BORDER DATA FLOW: ASEAN AND BEYOND



The UNDP Global Centre for Technology, Innovation, and Sustainable Development

The UNDP Global Centre for Technology, Innovation and Sustainable Development is a joint initiative by the Government of Singapore and the United Nations Development Programme (UNDP) which aims at identifying and co-creating technological solutions for sustainable development. The Centre curates partnerships, identifies solutions and connects partners and innovations with UNDP's Global Policy Network and development partners.

Acknowledgments

The UNDP Global Centre would like to thank the individuals and organisations who provided key insights during the development of this report. This includes many of the team in the Singapore Personal Data Protection Commission, and representatives from the Singapore Smart Nation Initiative, GSMA, OECD, Union Bank of the Philippines; the ICT Unit at the ASEAN Secretariat, members of the Data Protection Authority in the Philippines and Vietnam, and representatives from the Estonia e-Governance Academy.

Graphic design and layout editing: Peter Kongmalavong, Frederick Lee

United Nations Development Programme (UNDP)

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow at @UNDP.

One United Nations Plaza, New York, NY10017, USA

Overview and progress to-date

In the ASEAN region, only a few countries have established mechanisms encouraging cross-border data flow with the purpose of stimulating innovation and economic growth. However, as technological transformation progresses, the collection and processing of data is accelerating. This transformation also increasingly relies on access to and use of high-quality data that often resides in more than one country.[1]

In this context, there is a need to shape new models of **data governance**, whilst the crucial role of data in driving economic and societal development means that it should not be constrained by national or other geographic borders. This reality demands engagement with the requirements of enabling cross-border data flows.

Making cross-border data happen: policies and Processes

Existing regional and international trade agreements have informed the ASEAN approach to cross-border data flows, although their broad and non-digital focus requires underpinning with more specific policies. This includes national laws, policies and structures – in particular, legislation, regulation, and other guidelines – that inform cross-border data flows. Of particular importance are privacy rights, data protection legislation, intellectual property rights, and cybersecurity.

Data internationalism

In the ASEAN region, one of the main challenges to cross-border data is the fragmented and varying national requirements regarding the use of personal data. In particular, some countries impose **localisation** (or data sovereignty, or data protectionism) measures specifically to force data to be stored and/or kept within the country.

While individuals, business and digital systems are generating enormous flows of data, governments, in response, are struggling with striking a balance between facilitating trade through international data flows and upholding domestic policy objectives of privacy, consumer protection, and cybersecurity, according to the rule of law.[2] However, it is possible to achieve legitimate privacy and security goals in ways that are less impactful on trade and economic growth.

Privacy and data protection

Data governance frameworks for accountable and transparent processing of personal information (both before and after aggregation) are necessary to safeguard rights of privacy. Privacy is a fundamental right enshrined in many international declarations.

Data protection and privacy efforts are still evolving in the context of cross-border data flows. In this setting, there are a number of considerations and challenges. This includes preventing data extraction, or unequal data relationships, and tackling diverging data privacy laws.

Cybersecurity

Confidentiality, integrity, and availability of data, from a regulatory perspective, depends on national cybersecurity policy and legislation. From a cybersecurity perspective, some states may believe that data is more secure if it is stored within national borders. However, data security

Executive Summary

How we manage cross-border data is an important factor of national, regional, and global economic development – including driving progress toward achieving the Sustainable Development Goals. Yet, in the ASEAN region, only a few countries have established mechanisms encouraging cross-border data flow with the purpose of stimulating innovation and economic growth.

To-date, existing regional and international trade agreements have informed the ASEAN approach to cross-border data flows, although their broad and non-digital focus requires underpinning with more specific policies. This includes shaping national laws, policies and structures – in particular, legislation, regulation, and other guidelines – to inform cross-border data flows. Of particular importance are privacy rights, data protection legislation, intellectual property rights, and cybersecurity.

Technical interoperability also plays a fundamental role in cross-border data flows – and in the data life-cycle more broadly. Technical interoperability enables sharing of data between systems, and making use of this data. These systems also require data interoperability and interconnectivity to ensure that data flows in a seamless manner when being provided to those who need it, when they need it, where they need it, and in the form in which they need it.

On a practical level, data is compiled and stored by many organisations at global, national, and local levels. Both proprietary and open technologies are currently employed in the management of data. As such, it can be difficult to distribute or share data across various disjointed applications and databases. The challenges associated with data management can impede cross-border datasharing and hinder horizontal data use mechanisms such as Artificial Intelligence and Internet-of-Things.

Mission	Strengthen Data Ecosystem | Harmonise Legal and Regulatory Frameworks | Foster Data Innovation			
Strategic Priorities	**Data Life Cycle and Ecosystem**	**Cross-Border Data Flows**	**Digitalisation and Emerging Technologies**	**Legal, Regulatory, and Policy**
	Outcomes: • Data governance through the data lifecycle (e.g. collection, use, access, storage) • Adequate protection for different types of data	*Outcomes:* • Business certainty on cross-border data flows • No unnecessary restrictions on data flows	*Outcomes:* • Data capacity (infrastructure and skills) development • Leveraging new technologies	Outcomes: • Harmonised legal and regulatory landscapes in ASEAN (including personal data protection) • Development and adoption of best practices
	Initiative: • ASEAN Data Classification Framework	**Initiative:** • ASEAN Cross-Border Data Flows Mechanism	**Initiative:** • ASEAN Digital Innovation Form	**Initiative:** • ASEAN Data Protection and Privacy Forum
Enablers	Cybersecurity | Capacity Building | Enforcement Cooperation			

Figure 1 – Summary of the ASEAN Framework on Digital Data Governance *(ASEAN)*

An increasing number of business models are founded on the importance of accessing, holding, analysing and utilising data across borders, including Open Banking – discussed as a case study in this report. **Open Banking** is based on the idea of developing a single, cohesive pool of data that spans all products and services. By the end of 2020, 40 per cent of Asia Pacific banks will have invested in Open Banking management platforms. The catalytic potential of cross-border data in this use case highlights that all ASEAN countries – large and small – should play a role in defining, shaping, and iterating the policies, regulations, and technical foundations to drive cross-border data flows

This focus should include engaging with the realities of cross-border data – such as introducing 'open by default' data policies, avoiding data localisation or similarly protectionist approaches, and preventing further divergence around key priorities such as data privacy. Countries should also take a forward-thinking approachto regulation, particularly in the context of a technology-driven and fast-moving sector. The speed of change in the sector may demand a more agile, iterative, and experimental approach to regulation, legislation, and policymaking.

At a national level, governments and other partners should also invest in – and enable – the considerable technical foundations needed to enable cross-border data. These include extensive and high-quality connectivity, developing API functionalities, and building foundational national infrastructure such as data registries. Wherever possible, countries should seek to build on and expand international best practice – particularly to ensure technology-neutrality and future-proofing.

More broadly, there is a key role for the ASEAN community to play in shaping a strong regional data governance framework to leverage the above potential of cross-border data – and to mitigate data-related risks and harm. This includes formalising approaches to share responsibility for data privacy. International trade with regions such as the EU highlight the need for frameworks that move beyond the 'open regionalism' foundations of the ASEAN region.

All of these efforts must be founded on collaboration with all stakeholders in the national, and regional, data ecosystem – particularly the private sector and broader industry. International organisations can also play a key role in supporting coordination, building capacity and expertise, and driving collaboration and shaping best practice.

Overview and Progress-to-date

In the ASEAN region, only a few countries have established mechanisms encouraging cross-border data flow with the purpose of stimulating innovation and economic growth. This is likely due to the challenges encountered by some countries in capturing value from data - including lower-levels of data connectivity , issues with foundational digital infrastructure , weaker data collection processes and abilities, limited data or digital literacy that stifles innovation, and a lack of access to high quality or large datasets. These aspects can also prevent engagement with emerging technology and innovation such as Artificial Intelligence (AI) and data analytics.

In addition, although a growing number of countries in the region have laws protecting personal data, often there are limited funds, tools, abilities and resources to enforce these frameworks. More broadly, international data collaborations or explorations can sometimes be affected by a zero-sum approach to geopolitics. In particular, and as a result of some countries believing that retaining data within their borders creates national opportunities for economic growth based on digitalisation, countries may adopt protectionist approaches to data management, including data localisation. All of these factors risk exacerbating existing digital inequities between countries. They also risk 'locking-out' countries from the benefits of emerging technologies – and from cross-border data flows.

How cross-border data flows are driving digitalisation

As technological transformation progresses, the collection and processing of data is accelerating. New and emerging technologies such as AI, distributed ledgers, drones, and the Internet of Things (IoT) are also producing, storing, and analysing an unprecedented amount of data. Machine-to-machine products and services are also increasingly able to produce, store, and analyse data without human intervention. These technological advancements rely on access to and use of high-quality data that often resides in more than one country[4].

Cross-border data is driving and enabling this increased digitalisation, and perhaps even accelerating the production of data. The scale at which data can be collected and processed is driven by access to technology that is increasingly international in scope – including cloud computing. In order to collect more data, and leverage its potential, looking internationally is proving important.

All of these developments reaffirm the importance and need to shape new models of data governance, whilst the crucial role of data in driving economic and societal development means that it should not be constrained by national or other geographic borders. This reality demands engagement with the requirements of enabling cross-border data flows. This is a comparatively recent challenge. Cross-border data flow differs from the traditional exchange of goods and other services for a number of reasons:

- Suppliers and users do not need to be in the same location.
- The trade of data is fluid and frequent, and it is possible to trade the same data repeatedly.
- The physical location of data accessed is hard to determine, and hence is difficult to assess what data is 'imported' and what is 'exported'. In fact, the physical location of data may be irrelevant, as ultimately what matters is who has access to and control over the data.

- When data flows across borders, it does not necessarily have to be affiliated with a transaction. Data can be simply 'shared' across borders. For instance, in some cases, a copy of the data is undertaken locally. In others, users access data by connecting to the servers where the data is stored.
- There are different types of data, most notably personal data and non-personal data. While cross-border flow of personal data is a much more regulated space, transferring non-personal data across borders tends to be largely unregulated. That said, there is increasing interest in regulating cross-border personal and non-personal data flow.
- In practice, when private sector organisations think about cross border data flow, it is difficult for them to segregate personal data and non-personal data as often these data sets are interrelated.

These aspects highlight how cross-border data flows may not always fit traditional definitions of trade, and reaffirm the need for focused engagement with the emerging and existing realities of cross-border data flows.

The emerging ASEAN approach to cross-border data flow

Efforts to drive cross-border data flow must be founded on the local and regional context. In the ASEAN region, this includes leveraging existing networks and processes to drive digital regional integration. ASEAN countries are committed to regional integration in the 'ASEAN Way' , a distinctive approach to regional cooperation and governance. This approach is based on a commitment to protect national sovereignty, to non-interference in the domestic matters of fellow countries, to decisions based on consensus building, and to informal guiding relationships between leaders. This method of policymaking takes the form of blueprints, declarations, dialogues and fora, which often do not constitute or create legally binding or enforceable obligations at a regional level. As well as the 'ASEAN Way', countries have also undertaken a policy of 'open regionalism' that has shaped cohesion across the Asia-Pacific region[8].

The ASEAN organisation has also evolved and expanded its mandate beyond its original remit of shaping regional peace and security. In 2015 the ASEAN Economic Community was established, an audacious plan for enhanced economic integration[9]. As the region moves towards an interconnected and borderless model, the principles on cross-border data flows enshrined in the ASEAN Framework on Digital Data Governance are expected to guide state entities, the private sector and consumers to manage data flows. Notably, the ASEAN Framework on Digital Data Governance (Figure 4) 'is aimed at strengthening the data ecosystem, achieving legal and regulatory alignment of data regulations and governance frameworks; and fostering data-driven innovation across ASEAN Member States to boost the growth of digital economy in the region'[10].

However, although economic convergence between ASEAN's lower and higher-income countries has shown optimistic trends in the past twenty years, paradoxically this progress has been accompanied by growing inequality within countries[11]. The impact of digital transformation has the potential to accelerate development and economic growth. But at the same time, such efforts could slow down – or even reverse – the convergence between countries and risk widening digital and broader inequality between and within states[12].

Practices of cross-border data flow risk also entrench these inequalities. Well-resourced and more developed countries can more effectively extract value from data, and also bring to their shores data that is collected and produced in

Mission	Strengthen Data Ecosystem | Harmonise Legal and Regulatory Frameworks | Foster Data Innovation			
Strategic Priorities	**Data Life Cycle and Ecosystem**	**Cross-Border Data Flows**	**Digitalisation and Emerging Technologies**	**Legal, Regulatory, and Policy**
	Outcomes: • Data governance through the data lifecycle (e.g. collection, use, access, storage) • Adequate protection for different types of data	*Outcomes:* • Business certainty on cross-border data flows • No unnecessary restrictions on data flows	*Outcomes:* • Data capacity (infrastructure and skills) development • Leveraging new technologies	Outcomes: • Harmonised legal and regulatory landscapes in ASEAN (including personal data protection) • Development and adoption of best practices
	Initiative: • ASEAN Data Classification Framework	**Initiative:** • ASEAN Cross-Border Data Flows Mechanism	**Initiative:** • ASEAN Digital Innovation Form	**Initiative:** • ASEAN Data Protection and Privacy Forum
Enablers	Cybersecurity | Capacity Building | Enforcement Cooperation			

Figure 3 – Summary of the ASEAN Framework on Digital Data Governance *(ASEAN)*

his risks creating and entrenching a data dichotomy: between the former countries that have the infrastructure, knowledge, and resources to become digital data hubs that store, retain, and analyse data (for example, to inform data-driven technologies such as machine-learning); and their less-developed counterparts that are simply releasing data - with little or no real benefit from it, except lower value-added tasks within the supply chain of data production, storage, and analysis.

This extractive relationship, resulting in non-inclusive growth, risks increasing political and social instability within countries and could undermine support – and indeed, trust – in greater regional integration[13]. These wider considerations reaffirm the importance of defining an approach to cross-border data – from overarching governance, to the underlying common or recognised technical standards discussed later in this paper, and foundational norms and principles.

However, the above negative outcomes are far from guaranteed. Many less-developed countries are making significant progress in shaping advanced digital skills – including those relevant to critically interrogating and shaping data-driven solutions. Overall, enabling cross-border data flows has considerable potential to create positive economic and social multipliers for countries. Increasingly, much of the technology and expertise of the digital economy is being democratised and becoming accessible from many countries due to cross-border data flows. This can create regionally-competitive firms and industries. Where there is a broader risk of creating or entrenching inequalities between countries – as will be discussed later – is in situations of data protectionism. In these contexts of restricting cross-border data flows, it becomes more challenging for domestic companies to grow beyond their national market. This risks constraining economies, dissuading international talent, and preventing the development of innovative startups and ecosystems.

	Relevant pillars for international cooperation on data flows			
	Transfer mechanisms	**Legal and regulatory cooperation**	**Technical standards and industrial cooperation**	**International trade rules**
Universal availability	● **Unilateral openness (no restrictions imposed)** ● **User consent and other legitimate grounds for data transfer (e.g. contractual reasons, public interest)** ● **Accountability-based mechanisms (binding corporate rules and standard contract clauses**	● **Binding international treaties on legal harmonisation (Budapest Convention)**	● **Standard-setting in multi-stakeholder forums (ISO/IEC, IEEE, 3GPP, among others)**	● **World Trade Organization rules (case law, General Agreement on Trade in Services, and Reference Paper and Annex on Telecommunications) with privacy and other exceptions, along with two-tier test (for least-trade restrictiveness and necessity)** ● **Ongoing World Trade Organization Joint Statement Initiative negotiations**
Limited participation	● **Adequacy decisions to jurisdictions with adequate protection, e.g. EU-Japan reciprocal adequacy, adequacy decision on the EU-US Privacy Shield** ● **Certification programmes (under government oversight), e.g. Asia-Pacific Economic Cooperation Cross-Border Privacy Rules** ● **"Trusted" entity schemes**	● **Regional model laws on e-commerce, cross-border data flows and privacy (EU, ASEAN)** ● **Principles and guidelines on data flows and privacy (OECD Privacy Guidelines, APEC Privacy Framework)** ● **Legal assistance through mutual legal assistance treaties or international conventions** ● **Judicial redress and recourse offered to a list of countries under domestic law** ● **Diplomatic instruments and strategic partnerships (e.g. Australia-Singapore Digital Economy Agreement)**	● **National and regional standard-setting, e.g. United Nations Economic Commission for Europe** ● **Exclusive "data spaces" initiatives and consortium** ● **Bilateral mutual recognition agreements or equivalence decisions**	● **Digital trade commitments (e.g. data flow, prohibition on localisation and source code access disciplines derived from the Comprehensive and Progressive Agreement for Trans-Pacific Partnership - CPTPP) developed in the Japan-US Digital Trade Agreement, the United States-Mexico-Canada Agreement (USMCA), EU texts, the Digital Economy Partnership Agreement - DEPA, with varying exceptions**

Figure 4: Osaka Track architecture for data governance *(World Economic Forum)*

Building the foundations: the role of regional and international trade agreements

In the ASEAN region there are a number of multilateral arrangements ensuring that, when data is transferred across borders, a certain degree of protection is granted. These include non-binding arrangements, such as the ASEAN Personal Data Protection Framework; and principle-based frameworks, such as the APEC Privacy Framework, and the APEC Cross-Border Privacy Rules (CBPR) System – as well as broader initiatives such as the 'Data Free Flow With Trust' concept arising from Japan's 2019 G20 leadership. Other international and regional trade schemes that can facilitate cross-border data flow between ASEAN countries include the Regional Comprehensive Economic Partnership, the ASEAN e-Commerce Agreement, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, and, more widely, the Council of Europe Convention 108/9181.

Active involvement of the private sector is crucial in enabling cross-border data flows.

In addition, bilateral and regional approaches to regulate traditional trade activities, and cross-border data flow, provide important foundations for cross-border data flow. In this context, ASEAN states are working both within ASEAN and with countries outside the region towards a number of mechanisms governing cross-border data flow, including certifications, accreditation, and contractual clauses[14]. Extensive industry engagement has been an important foundation. In this context, for instance, Singapore has recently signed a Digital Economy Partnership Agreement[15] with New Zealand, as well as a separate Singapore-Australia Digital Economy Agreement (SADEA)[16]. This aims to align digital rules and standards that support and encourage cross-border data flow, and to facilitate interoperability between digital systems[17]. Active involvement of the private sector is crucial in enabling cross-border data flows.

Regionally, this overarching framework consists of a collection of norms and principles shaped through fora, dialogues, and declarations. These documents and processes do not constitute or create legally-binding or enforceable obligations at a regional level (although some aspects – such as the ASEAN Model Contractual Clauses, discussed below, are binding) but rather guidelines drawing from privacy, data protection and cybersecurity laws on the one hand; and on the other, from trade agreements.

1. Aaroson, S. A. (2019). Data is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows. Available at https://unctad.org/meetings/en/Presentation/tdb_ede3_2019_p06_SAaronson_en.pdf

2. Chen, L., and Kimura, L. (2020). E-commerce Connectivity in ASEAN. Economic Research Institute for ASEAN and East Asia (ERIA). Available https://www.eria.org/publications/e-commerce-connectivity-in-asean/

3. Beschorner, N., Bartley J. M., Guermazi, B., Treadwell, J. L., Prakosa, P. W. B., Abdul Karim, N. A. B., Van Tuijll, D. A., Bennis, L., Nicoli, M., Van Rees, J., Girot, C. A. H. M. (2019). The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth (English). Washington, D.C. World Bank Group. http://documents.worldbank.org/curated/en/328941558708267736/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth

4. World Economic Forum (2020). A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy. White Paper, June 2020. Available at http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

5. Aaronson, S. A. (2018). Data is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows. IIEP-WP-2018-10. November 2018. Available at https://www2.gwu.edu/~iiep/assets/docs/papers/2018WP/AaronsonIIEP2018-10.pdf

6. Association of Southeast Asian Nations (ASEAN). The ASEAN way and the rule of law. Available https://asean.org/?static_post=the-asean-way-and-the-rule-of-law

7. World Economic Forum (2017). ASEAN 4.0:
What does the Fourth Industrial Revolution mean for regional economic integration? White Paper. November 2017. Available at https://www.adb.org/sites/default/files/publication/379401/asean-fourth-industrial-revolution-rci.pdf

8. Drysdale, P. ASEAN: The Experiment in Open Regionalism that Succeeded. Available at https://www.eria.org/5.1.ASEAN_50_Vol_5_Drysdale.pdf

9. ASEAN news (2018). ASEAN 4.0:What does it mean for regional economic integrations. Available at https://www.thailand-business-news.com/asean/70455-asean-4-0-what-does-it-mean-for-regional-economic-integration.html.

10. ASEAN, Thailand. (2019). ASEAN Deputy Secretary General speaks at ASEAN-UK Reception. In: UK-ASEAN Business Council. Nov 2019. Available at https://www.ukabc.org.uk/news/asean-deputy-secretary-general-speaks-at-asean-uk-reception/

11. Menon and Fink (2019)

12. The World Bank (2019). The Digital Economy in Southeast Asia : Strengthening the Foundations for Future Growth (English). Washington, D.C. World Bank Group. Available at http://documents.worldbank.org/curated/en/328941558708267736/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth

13. Menon and Fink (2019)

14. For the model contract clauses template to be successful, the active involvement of the private sector is necessary. To this end, ASEAN has conducted extensive industry consultation to develop it. In fact, although it is being developed by ASEAN regulators, it is not just a bilateral and regional governmental approach but is used largely for business-to-business (B2B) transactions.

15. Available at https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreements/

16. Available at https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement

17. Grant, J. (2020). Singapore charts its way to digital future for trade. In: Financial Times. 28 September 2020. Available athttps://www.ft.com/content/05504fcb-11e6-47a0-8860-7d156d1d82ab?segmentID=22a4a564-acc0-bdcd-29ab-405d952fdcc3

Making Cross-Border Data Happen: Policies and Processes

Existing regional and international trade agreements have informed the ASEAN approach to cross-border data flows, although their broad and non-digital focus requires underpinning with more specific policies. This includes national laws, policies and structures – in particular, legislation, regulation, and other guidelines – that inform cross-border data flows. Of particular importance are privacy rights, data protection legislation, intellectual property rights, and cybersecurity.

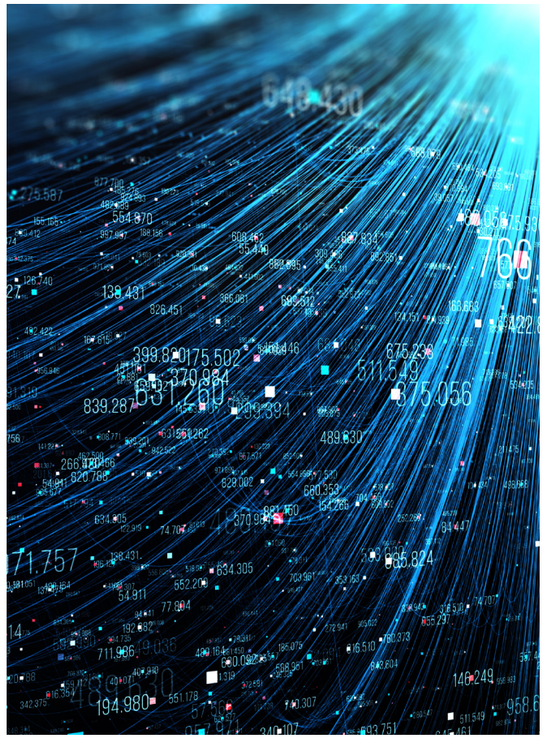
According to the Organisation for Economic Cooperation and Development (OECD), in order to create a data-enabled digital government model, state entities should adopt 'open by default policies'[18], and create mechanisms to engage with different stakeholders around their data needs[19]. This shift has also prompted changes in the data skills needed in national government agencies to govern the entire data life cycle[20], but also the overarching frameworks and foundational components needed to enable the sharing of data across borders .

Data internationalism

In the ASEAN region, one of the main challenges to cross-border data is the fragmented and varying national requirements regarding the use of personal data. In particular, some countries impose localisation (or data sovereignty, or data protectionism) measures specifically to force data to be stored and/or kept within the country.

Vietnam and Indonesia have imposed particularly comprehensive restrictions on cross-border data flows in the ASEAN region[21]. Specifically, Vietnam has a requirement for private firms who want to process data to build a server locally to operate in the country. This infrastructure requirement serves to store data for inspection should a competent authority request provision of information[22] Indonesia's data-localisation laws cover a number of sectors and technologies. The country has expanded its localisation policies as part of its state-directed development and digital protectionism strategies[23].

Several factors drive a more restrictive approach to cross-border data flow, including perceived safeguarding of national security, protecting data privacy, aiding law enforcement (including domestic surveillance), preventing foreign surveillance, and appeals to the fundamental principle of national sovereignty more generally. However, localisation can often impair – or actively undermine – these objectives. For example, data localisation can increase the risks of data breach and impact on privacy as the data is more accessible and large – simplifying and incentivising the work of hackers to locate and access this sensitive data.



Small countries, which are not home to data centres, can incur unnecessary administrative regulatory costs related to enforcing data localisation requirements – whilst foreign investment will be discouraged due to the favouring of local players.

Governments have also restricted the transfer of data across national borders to foster the development of the technology sector domestically[24]. But at the same time states that implement such significant data protectionism practices, particularly data localisation can end up stifling their economies[25]. These requirements have a real, significant, and negative effect on the GDP of a country. In the context of a digital economy, they can also increase the price of (or actively prevent access to) specific services such as cloud computing - a crucial platform in catalysing digitally-focused small- and medium-enterprises, which are an essential growth sector for any country.

From a broader private sector perspective, data localisation disincentives the entry of international firms – leading to less competition - as companies will incur additional capital and operational expenditures to create local data storage, data centres, and other infrastructure. Domestic digital firms – whose business models may rely on data – will also be unable to freely transfer data and benefit from economies of scale to the fullest extent. These localisation measures also create a barrier to these firms' entrance into foreign markets. This can also have a broader and negative impact. If a country has strict data localisation policies, it can limit the potential for it to become a digital 'hub' or similar – and the total addressable growth opportunity in that market will be constrained only to the domestic digital economy. This will, in turn, affect the overall value-proposition of building infrastructure and investing in that country, compared to a neighbouring country that permits cross-border data flows. In summary, commercial risk may increase whilst investment attractiveness could decrease when a country has data localisation measures in place.

Small countries, which are not home to data centres, can incur unnecessary administrative regulatory costs related to enforcing data localisation requirements – whilst foreign investment will be discouraged due to the favouring of local players. Data localisation requirements also increase the administrative expenses related to compliance - for governments and the private sector. Data protection officers are required to obtain consent mechanisms to transfer data across organisations and borders, whilst companies need to identify and determine the categories of data that need to be stored locally, and which data can be moved offshore. This will also slow down the pace of innovation as the ability to experiment is severely impeded – as it will either now take too long, be too costly or both - by onerous compliance requirements.

On a more fundamental level, over-assertion of state control raises concerns about the 'Balkanisation of the Internet'[26]. This risks shattering – perhaps irreparably - the interoperability and unified nature of the Internet, thus diminishing the value of the Internet, its multipliers and network effects, in supporting international trade transactions. If this

practice becomes widespread, there would be a need for a significant redesign of the technical and governance structures of the Internet.

Considerations: cross-border data and data internationalism

While individuals, business and digital systems are generating enormous flows of data, governments, in response, are struggling with striking a balance between facilitating trade through international data flows and upholding domestic policy objectives of privacy, consumer protection, and cybersecurity, according to the rule of law[27]. However, it is possible to achieve legitimate privacy and security goals in ways that are less impactful on trade and economic growth.

- **Cross-border data sharing based on adequate and comparable protection.** Similar to the EU approach, the Philippines, Malaysia and Singapore may allow data transfer to organisations outside their territories only when destination countries have adequate safeguards comparable to protections granted under their own jurisdictions[28]. These approaches facilitate legitimate cross-border data flows if certain conditions are met. For example, an entity may transfer personal data outside Singapore if the recipient organisation is bound by legally enforceable obligations such that the personal data transferred has a standard of protection which is comparable to that under Singapore's Personal Data Protection Act[29]. These approaches underline that it is possible to ensure that cross-border data flow does not abrogate national data protection and privacy standards[30].

- **Regulatory cooperation and the role of governance.** Confidence that domestic policy objectives will be met even if data flows out of jurisdiction creates trust between policymakers. An approach that both embraces data flow and protects citizens and nnational assets through regulatory objectives require regulatory cooperation. Southern East Asian governments have already started to pursue this through bilateral, regional and international agreements within the ASEAN Economic Community (AEC).

- **Technical solutions.** Protecting personal, confidential or data of national security should consider both policies, regulatory and technical aspects. The hosting location of the data does not necessarily provide high levels of privacy, confidentiality, security, availability and integrity. Instead, it is the combination of secure networks and system architectures and clarity on the legal protection regime (and enforcement) that guarantee privacy and security of data. The ASEAN certification scheme discussed below takes this approach.

Without a clear path towards achieving legitimate policy objectives and maximising the benefits of the digital economy, governments may increasingly opt for approaches that restrict data flows. Building relatively new policy and regulatory virtual borders is increasingly disrupting the global Internet and jeopardising service supply and choice, value chain integration and essential innovations that might otherwise be of great significance for the development of national digital economies.

Therefore, if after careful consideration of both technical and legal aspects on privacy and data protection, confidentiality, availability and integrity of data, data localisation is still a national requirement, it becomes essential to highlight the existence of options and clarity on what classes of data can be shared across borders. Nevertheless, these different approaches to data sharing should be carefully crafted to prevent undue regulatory complexity, for instance, by introducing too many categories of data that are not clearly described or relying on vague conditions for sharing data. A consideration of 'open by default' could be important.

Privacy and Data Protection

Data governance frameworks for accountable and transparent processing of personal information (both before and after aggregation) are necessary to safeguard rights of privacy. Privacy is a fundamental right enshrined in many international declarations. Article 12 of the Universal Declaration of Human Rights (UDHR) proclaims the right to be free from arbitrary interference of one's privacy, family, home or correspondence. Similarly, Article 17 of the International Covenant on Civil and Political Rights 1966, Article 14 of the UN Convention on Migrant Workers, and Article 16 of the UN Convention of the Protection of the Child make reference to privacy[31].

Privacy is a fundamental human right, and should therefore be carefully balanced against competing rights and public interest goals.

In the ASEAN region, Article 21 of the ASEAN Human Rights Declaration[32], inspired by Article 12 of the UDHR, includes the concept of personal data. It declares that 'every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data.' With the aim of increasing cooperation to facilitate border transactions at a regional level, one of ASEAN's e-commerce key action lines[33] is to develop 'Regional Data Protection and Privacy Principles'. In addition, the ASEAN Strategic Action Plan for consumer protection (2016-2025) includes an initiative to modernise the legislation to reflect relevant provisions on consumer data privacy[34].

Privacy is a fundamental human right, and should therefore be carefully balanced against competing rights and public interest goals. One of these competing rights is transparency, including in relation to 'right to know' or 'Freedom of Information' laws. Another is in relation to facilitating data sharing – including in the context of cross-border data flows. The solution to address these conflicts between transparency, openness and privacy lies in putting in place procedures that acknowledge privacy risks and harms linked to sharing personal data, and setting out appropriate steps to address these concerns. Data protection law is one mechanism to protect individual rights to privacy and to reduce privacy violation risks, particularly in the context of regional cross border data flow.

In the contemporary context of 'Big Data', the potential for re-identification of individuals - by combining different sources of de-identified data through analytics and machine learning (the so-called mosaic effect[35]) – sharpens data privacy concerns. Malaysia, Singapore, the Philippines, and Thailand have developed comprehensive personal data protection laws

of Information' laws. Another is in relation to facilitating data sharing – including in the context of cross-border data flows. The solution to address these conflicts between transparency, openness and privacy lies in putting in place procedures that acknowledge privacy risks and harms linked to sharing personal data, and setting out appropriate steps to address these concerns. Data protection law is one mechanism to protect individual rights to privacy and to reduce privacy violation risks, particularly in the context of regional cross border data flow.

In the contemporary context of 'Big Data', the potential for re-identification of individuals - by combining different sources of de-identified to tackle this problem, while Indonesia has a draft law that is in a relatively advanced stage[36]. Lao PDR, Vietnam, and Cambodia have legislation applying to specific sectors or mediums (for instance, relating to the press in case of Cambodia[37]). Myanmar and Brunei do not have any specific data protection laws[38].

While losing control over an individual's data is a form of harm, in a data-driven setting the potential consequences of this loss of control are amplified. For instance, a breach of sensitive personal data (e.g. financial, health, or biometric information) may impact on a person's ability to secure insurance, gain employment, and other benefits - or it may result in discrimination or social stigma. Similarly, concerns over losing control of privacy could lead citizens to share less data[39]. This reaffirms why data protection should be paramount – regardless of data being transferred across borders. It should continue to be protected as though it was still in the jurisdiction of origin.

Considerations: cross-border data, privacy, and data protection

Data protection and privacy efforts are still evolving in the context of cross-border data flows. In this context, there are a number of considerations and challenges:

- **Preventing data extraction, or unequal data relationships.** Citizens of countries with lower levels of data protection may find their data more exposed than those in states with robust data protection frameworks. When a data protection law is in place, governments and private sector organisations are obliged by privacy and data protection laws to avoid disclosing personal information except for authorised purposes, but these protections are only viable if enforcement is possible. In some countries, enforcement may not be viable.
- **Data privacy laws may be diverging.** The majority of ASEAN countries have effectively applied the high-level concepts and principles contained in international legal frameworks, instruments, or guidelines. As a result, their national legal systems on data protection are compatible across the region[40]. Notwithstanding, the transposition of high-level concepts and principles in national jurisdictions has not achieved the expected goal of regional consistency. In fact, when moving from the text of newly-enacted legislations on data protection to the practicality of compliance and enforcement, divergence increases as nations prescribe an increasing number of specific requirements. In this context, both regional and local efforts should aim at promoting the convergence of existing data protection laws[41]. Many ASEAN countries are reviewing their own data protection legislations and may consider broader regulatory approaches – perhaps similar to the GDPR, with Europe a significant trading partner for the region - to protect citizens' privacy and enable local businesses to operate globally[42] through some sort of conformity in approach[43]. Another scheme for ASEAN countries is the Cross-Border Privacy Rules (CBPR) System of APEC. The APEC CBPR has the benefit of enabling cross-border personal data flow even if governments have not formally recognised the equivalence of their respective privacy laws. APEC CBPR empowers privateentities to ensure that any data collected and transmitted to third-parties, either domestically or internationally, adheres to data protection consistent with the APEC principles of privacy[44].
- **The risks of data extraction.** Conversely, in countries where data protection laws are weak or not existent (for example, Myanmar

and Brunei), corporations and other governments could adopt practices that do not consider local people's right to privacy. These practices could extract value by collecting personal data locally, while placing vulnerable and marginalised communities at risk of privacy violation. This could lead to 'regulatory shopping', where companies or other entities collect and use data from countries or regions with more favourable – or non-existent - data protection policies and legislation.

Cybersecurity

Confidentiality, integrity, and availability of data, from a regulatory perspective, depend on national cybersecurity policy and legislation. However, to protect users' online safety and security, some countries may impose restrictions on data sharing and transfer by enacting cybersecurity legislation. These can be barriers to the free flow of data. From a cybersecurity perspective, some states may believe that data is more secure if it is stored within national borders.

Notwithstanding, both the digital economy and national security are legitimate concerns for states. While cross-border data flows can facilitate the digital economy, data localisation can facilitate national security. Data which supports the digital economy should be supported by compatible cross-border data transfer frameworks, while data which impacts on national security will need to be more tightly secured, which may require other measures such as data localisation.

However, data security is a function of the technical, physical, and administrative controls in place by the service provider - regardless of where the data is geographically stored. In the case of a security breach, if countries have cybersecurity legislation in place, a private entity operating in these countries will be subject to these laws. However, data breaches can happen independently from where the data is physically stored. Therefore, it is crucial that the organisation managing data implements all measures to prevent such breaches[45], including encryption[46].

As noted above, in the ASEAN region, countries such as Vietnam has enhanced cybersecurity laws that impose data localisation requirements placing restrictions on digital trade. The recently adopted Cybersecurity Law imposes local data storage requirements for both domestic and foreign organisations that provide internet, telecommunications, and value-added services. The data is requested to be temporary locally stored and the specific requirements are set by the regulatory authorities. However, these restrictive data localisation provisions are currently under revision[47].

Considerations: cross-border data and ensuring cybersecurity

Despite differences in terms of regulatory models between ASEAN countries, improving the compatibility of cross-border data transfer frameworks would enhance legal certainty, with a positive impact on collective and national positions on cross-border data flow. Conversely, laws prescribing different conditions for the collection, storage, and transferring of data can increase the burden on private sector organisations.

Data security is a function of the technical, physical, and administrative controls in place by the service provider - regardless of where the data is geographically stored.

Considering that data can fuel countless applications across different industries and benefits society as a whole, Singapore has recently proposed changes to its copyright act recommending an exception to copyright law for data analysis.

This could lead to the adoption of sub-optimal and vulnerable IT infrastructures, which may then increase the risk of cybersecurity attacks[48].

The security of data (including confidentiality, integrity and availability) does not depend on the physical location of the servers which are hosting such data. Rather, it is a function of the normative rules - including norms, policies, regulations, and laws; protocols (such as data standards and technical interfaces), and implementation of technologies and security measures – such as encryption, firewalls, and access controls - that are put in place by public or private service providers in the way that they store, access, share and use the data. These should be a priority consideration in any data setting.

Intellectual property rights

The digital economy generates a large volume of data, which has great value for economic operators[49]. While data in the personal domain is usually protected by privacy regulation, proprietary compilation of data is normally protected by intellectual property rights (IPR). These include copyright, trade secrets, patents, and contractual frameworks[50].

The role of IPR in cross border trade cannot be overstated, considering that private sectororganisations which want to trade their goods internationally need assurances that their intellectual property rights are protected on foreign territories. In a digital environment, intellectual property can be seen as a security measure when data moves across borders[51], and therefore, compilation of data (such as annotation, creative arrangements, or selection of data) covered by IPR may be subject to restrictions of crossing borders.

New rights for creators in the digital environments have been introduced by the World Intellectual Property Organisation Copyright Treaty. According to the Treaty, the author or successor-in-title is the only subject that can authorise the distribution of a piece of work to the public. It also has the exclusive right to communicate the work to the public, including through the Internet. In other words, the copyright holder controls who can access a work covered by copyright[52].

Considerations: cross-border data and intellectual property rights

It is uncommon, at least in ASEAN – and besides the Singapore case - to assign IPR to public sector data. In general, it is accepted and expected that public sector data should be made available through open data, free of any intellectual property restrictions and free of charge[53]. This data can be made available in the public domain if there are no conflicting interests - such as national security or law enforcement

Considering that data can fuel countless applications across different industries and benefits society as a whole, Singapore has recently proposed changes to its copyright act recommending an exception to copyright law for data analysis. This exception applies to any 'reproduction that [is] performed in the course of text and data mining', when automated

techniques are involved to extract, analyse and copy large quantities of data, to capture new meaning and information. Without this exception, the act of mining and analysing data may infringe copyright, in turn limiting data activities[54].

18. OECD (2019). Data availability: Policy frameworks, stakeholder engagement and data release. Available at https://www.oecd-ilibrary.org//sites/cea2bbb6-en/index.html?itemId=/content/component/cea2bbb6-en#fig-9.5

19. Boyd, M., Frejova, J., and Wilde, E. (2020). Better governance, one API at a time. Axway White Paper. Available at https://www.apidays.co/wp-content/uploads/2020/06/axway-wp-better-governance-en.pdf

20. For the various phases of the data lifecycle, see Wing, J. M. (2019). The Data Life Cycle.(1). https://doi.org/10.1162/99608f92.e26845b4

21. The World Bank (2019). The Digital Economy in Southeast Asia Strengthening the Foundations for Future Growth. Available at http://documents1.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf

22. Ferracane (2017).

23. Cory, N. (2017). Cross-Border Data Flows: Where are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation. May 2017. Available at http://www2.itif.org/2017-cross-border-data-flows.pdf

24. The World Bank (2019).

25. Prapangpong (2018)

26. Kurbalija, J. (2012). The Internet and 'balkanisation through regulation'. In: Diplo. Available at https://www.diplomacy.edu/blog/internet-and-'balkanisation-through-regulation'
27. Prapangpong (2018)

28. (Section 129 (1) and (2) of the Malaysia's Personal Data Protection Act 2010; Section 26 (1) and (2) of the Singapore's Personal Data Protection Act 2012). In the Philippines, the 'Accountability Principle' contained in the Data Privacy Act of 2012 (DPA) s 21 gives responsibility to the controller over "personal information under its control and custody, including information that has been transferred to third parties for processing, whether domestically or internationally".

29. Linklaters (2020). Data Protected – Singapore. Available at https://www.linklaters.com/es-es/insights/data-protected/data-protected---singapore

30. World Bank (2019)

31. Privacy International (2017). What Is Privacy? Available at https://privacyinternational.org/explainer/56/what-privacy

32. ASEAN Human Rights Declaration. Available at https://www.asean.org/storage/images/ASEAN_RTK_2014/6_AHRD_Booklet.pdf

33. ASEAN AEM and AEC Council, ASEAN Economic Community 2025 Consolidated Strategic Action Plan, number 90. Available at https://asean.org/storage/2012/05/Consolidated-Strategic-Action-Plan-endorsed-060217rev.pdf

34. ASEAN. The ASEAN Strategic action plan for consumer protection (ASAPCP) 2016-2025: meeting the challenges of a people-centered ASEAN beyond 2015. Available at https://aseanconsumer.org/file/post_image/The%20ASEAN%20Strategic%20Action%20Plan%20For%20Consumer%20Protection%202016_2025%20Meeting%20The%20Challenges%20of%20A%20People%20%20Centered%20ASEAN%20Beyond%202015.pdf

35. Centre for Humdata (2020). Exploring The Mosaic Effect on HDX Datasets. 22 July 2020. Available at https://centre.humdata.org/exploring-the-mosaic-effect-on-hdx-datasets/

36. The Jakarta Post (2020). Indonesia to conclude data protection bill in November. September 2, 2020. Available at https://www.thejakartapost.com/news/2020/09/02/indonesia-to-conclude-data-protection-bill-in-november.html

37. Zico law (2020). Personal Data Protection in ASEAN. ASEAN insiders series. Available at https://www.zicolaw.com/wp-content/uploads/2020/09/ASEAN-INSIDERS_PDPA-in-ASEAN-3.pdf

38. For a summary, see ZICO law (2020). ASEAN insiders series. Available at https://www.zicolaw.com/wp-content/uploads/2020/09/ASEAN-INSIDERS_PDPA-in-ASEAN-3.pdf

39. State of Open Data. Privacy. Available at https://stateofopendata.od4d.net/chapters/issues/privacy.html

40. The World Bank (2019). The Digital Economy in Southeast Asia Strengthening the Foundations for Future Growth. Available at http://documents1.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf

41. The World Bank (2019)

42. PR Newswire (2020). Raising the standards of authentication. In: Tech Vantage. 16 June, 2020. Available at https://thetechvantage.net/raising-the-standards-of-authentication/

43. Financier Worldwide Magazine (2019). The EU GDPR's impact on ASEAN data protection law. Available at https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law#.X3drF5MzZTY

44. To date, in Asia, Japan, the Philippines, Singapore, South Korea, and Taiwan have joined the scheme.

45. Cory (2017).

46. Although encryption does not necessarily prevent data breaches, it can mitigate the risks considering that in the event encrypted data are leaked, they cannot be read.

47. Vishwakarma, N. (2019). Vietnam plans to narrow data localization requirements under its cybersecurity law. In: MEDIANAMA. Available at https://www.medianama.com/2019/10/223-data-localisation-vietnam/

48. Asian Business Law Institute (2020). Transferring Personal Data in Asia: A path to legal certainty and regional convergence. Available at https://www.abli.asia/NEWS-EVENTS/Whats-New/ID/134/Transferring-Personal-Data-in-Asia-A-path-to-legal-certainty-and-regional-convergence

49. European Commission (2016). Facilitating cross border data flow in the Digital Single Market.

50. OECD (2020). Mapping approaches to data and data flows. Report for the G20 Digital Economy Task Force. Saudi Arabia, 2020. Available at http://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf

51. WEF (2020).

52. Research ICT Africa (2020). SADC PF Discussion Paper on the Digital Economy and Society.

53. OECD (2020).

54. Foo, G. (2019). Singapore's biggest copyright report in 30 years. WIPO Magazine. Available at https://www.wipo.int/wipo_magazine/en/2019/04/article_0003.html

Cross-Border Data Mechanisms

The ASEAN framework on Digital Data Governance[55] (Figure 5), adopted in 2017, is an attempt to develop a conducive regulatory framework even in a context of varying national data maturities across countries. It aims to maximise the free flow of data within the region to encourage a dynamic data ecosystem while ensuring that the necessary protections are in place with data is transferred[56].

One of the four 'Strategic Priorities of Digital Data Governance' in the framework is cross-border data flows. The outcomes of this priority are to ensure business certainty regarding cross-border data flows, and to ensure that there are no unnecessary restrictions on data flows. These aims are being explored through a voluntary and non-binding Mechanism[57], which encompasses regulatory certainty on the practice of data sharing, including 'who they may share data with, the types of data that may be shared, and how they may share such data'[58].

Potential approaches to enabling cross-border data

The underlying objective of the mechanism is to take into consideration the various maturity levels and national laws that are in place in every Member State within the ASEAN region. Countries can subsequently evaluate their participation in the mechanism. This approach respects digital sovereignty and is a way to explore cross-border data flows with the underlying objective of guiding national policies. The mechanism involves two fundamental methods:

- **Certification.** Organisations that demonstrate they have reliable and effective data management practices in place are provided with a certification that confirms they operate in compliance with data management requirements. For example, they have proven to have measures in place that safeguard protection of people's rights to privacy and have effective security mechanisms in place.

Mission	Strengthen Data Ecosystem | Harmonise Legal and Regulatory Frameworks | Foster Data Innovation			
Strategic Priorities	**Data Life Cycle and Ecosystem**	**Cross-Border Data Flows**	**Digitalisation and Emerging Technologies**	**Legal, Regulatory, and Policy**
	Outcomes: • Data governance through the data lifecycle (e.g. collection, use, access, storage) • Adequate protection for different types of data	*Outcomes:* • Business certainty on cross-border data flows • No unnecessary restrictions on data flows	*Outcomes:* • Data capacity (infrastructure and skills) development • Leveraging new technologies	Outcomes: • Harmonised legal and regulatory landscapes in ASEAN (including personal data protection) • Development and adoption of best practices
	Initiative: • ASEAN Data Classification Framework	**Initiative:** • ASEAN Cross-Border Data Flows Mechanism	**Initiative:** • ASEAN Digital Innovation Form	**Initiative:** • ASEAN Data Protection and Privacy Forum
Enablers	Cybersecurity | Capacity Building | Enforcement Cooperation			

Figure 5 – Summary of the ASEAN Framework on Digital Data Governance *(ASEAN)*

Over the last few years, more and more regional nations, such as Japan and South Korea, have put certification systems in place as a means of assisting businesses to prove they operate in compliance with the national data protection laws. These systems provide encouraging signs for interoperability[59]. Organisations achieve certification if they can adequately demonstrate that they take appropriate precautions and manage data in a safe and effective way in accordance with the data protection laws in place in different jurisdictions. In some cases, different certification schemes may emerge; as such, one business may receive different certifications according to different frameworks. In some jurisdictions, such as Singapore, and Thailand, it is not possible for self-regulatory, non-binding certification mechanisms to effectively operate under the data transfer rules that are in place as it is typically a requirement that certification policies can be enforceable for application in such situation[60]. Certifications can also provide confirmation that a given organisation has appropriate data minimisation and security protocols in place that adequately prevent data from being accessed by any unauthorised party[61].

- **Model Contractual Clauses (MCCs).** MCCs, which are also referred to as data transfer agreements, are contractually enforceable and mandate that all personal data is fully protected in the event that it is transferred to an overseas territory[62]. They also clearly outline the data protection mechanisms that are in place, the obligations that govern data transferring, responsibilities for data management, data portability and data access - including how data subjects can exercise their right to delete, access and move the data[63]. MCCs can also indicate the governing law for any contract involving data, and therefore the authority that will be responsible for any data breaches. These are widely agreed to provide a valid method by which organisations can ensure that they are in agreement with data transfer requirements. In the case of countries that are putting data protection mechanisms in place and have yet to finalise their enactment, MCCs can be implemented as a lawful foundation for the transfer of data within the region.

The Working Group on Digital Data Governance (WG-DDG) is in charge of developing 'the implementation details and guidelines for ASEAN Certification and ASEAN Model Contractual Clauses, including the appropriate enforcement mechanisms, standards, policies, and processes', and of guiding TELSOM[64] and TELMIN[65] on capacity building needs and interoperability with other international frameworks and mechanisms[66].

Certifications and MCCs should be accessible for all organisations in all industries throughout the ASEAN region and should not be limited to specific sectors. This helps to guarantee that data subjects will benefit from equal protection mechanisms and will enable businesses that are based in the ASEAN region to optimise the associated benefits[67].

Many legal professionals are in broad agreement that evaluating the suitability of each country's privacy regime on a case-by-case basis would incur significant practical liability. This would be exacerbated in situations in which the law does not provide a list of fundamental standards that serve to prove that the legal requirements that are in place in an alternative legal setting afford a comparable standard of data protection. Furthermore, industry actors have highlighted how assessments of this nature are not realistic and are at risk of becoming rapidly out of date due to changes in the situation in each respective jurisdiction.

They also argue that, even if it were possible to secure resource and time required to perform such evaluations, the hypothetical legal adequacy of a given regime would not focus on problems such as practical conformity, execution or enforceability in the jurisdiction of interest[68]. As such, it is not particularly effective for a 'data exporter' to perform self-assessment because it does not guarantee that the data protection mechanisms are compatible. Even in situations in which self-assessment is deemed to be legitimate for cross-border data transmissions, there is a need to have clear rules regarding how such an assessment is performed and by whom[69].

Various other mechanisms are in place that facilitate cross-border data flow. The two more favourable approaches are outlined below:

- **Binding Corporate Rules (BCRs).** BCRs were established in the EU as a means to transfer data across borders in a manner that complies with Directive 95/46/EC (Article 25) - now EU GDPR (Article 47). Organisations adhere to these data protection protocols when transferring any personal data between enterprises or groups. The primary feature of BCRs are relatively standard per EU legislation. In a comparable way to Codes of Conduct (detailed below), BCRs make sure organisations operate in a way that adheres to local legal requirements while simultaneously ensuring that any data transferred across borders is sufficiently protected[70]. BCRs also include more relaxed internal regulations that govern how personal data is shared within corporate groups. They are legally binding on all appropriate bodies and individuals who form the group. BCRs are often supported by a wide-ranging privacy and compliance framework that spans procedures, policies, governance processes, data protection officers, training systems, communication channels, and assessments. On a holistic level, they adhere to the primary aspects of corporate compliance mechanisms[71]. As the implementation of BCRs can be less time-, resource-, and cost-intensive than alternative methods, such as model contracts, they can be advantageous for organisations that engage in numerous data transfers. As such, they are particularly attractive to SMEs. Over a long period of time, it is anticipated that the costs of compliance as a result of the use of BCRs will typically be lower than alternative approaches to managing more complicated transfers across intra-group entities – in the EU setting at least[72]. ASEAN's Model Contractual Clauses take this approach, with modification. By adding modularity, they result more flexible than the EU's Standard Contractual Clauses (SCC).
- **Codes of Conduct.** Codes of Conduct are designed by professional industry societies and other representative bodies. They can be particularly useful as they allow businesses to develop bespoke data protection provisions that are aligned with their unique requirements. A further benefit of such Codes is that market efficiencies can emerge when organisations adhere to the underlying provisions on a voluntary basis. The body or association that is responsible for developing a Code of Conduct is required to perform an in-depth review of any applicant that is seeking membership of the wider group or that is expressing a desire to comply with the Code[73]. Prescribing to a Code of Conduct can mean that an organisation does not need to perform its own evaluation of a prospective provider's system as it can, instead, find processors or providers that have already been found to be in adherence with the rules specified in the Code and can depend the association to ensure compliance[74].

55. ASEAN (2017). Telecommunications and Information Technology Ministers Meeting (TELMIN). Framework on Digital Data Governance. Available at https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf

56. ASEAN (2017). Framework on Digital Data Governance.

57. ASEAN. Key approaches for ASEAN cross border data flows mechanism. Available at https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf

58. ASEAN (2017). Framework on Digital Data Governance.

59. Legal domain in which certification schemes in place that are valid for the purse of data transfers are sufficiently broad to facilitate certification in accordance with international standards; for example, ISO/IEC 27701:2019 on Privacy Information Management System (PIMS). This has the capability to facilitate data flows not only from one-country-to-many-countries but also from most-countries-to-most-countries.

60. Asian Business Law Institute (2020). Transferring Personal Data in Asia: A path to legal certainty and regional convergence. Available at https://www.abli.asia/NEWS-EVENTS/Whats-New/ID/134/Transferring-Personal-Data-in-Asia-A-path-to-legal-certainty-and-regional-convergence

61. Digital Europe (2020). An early analysis of Schrems II – key questions and possible ways forward. 21 August 2020. Available at https://www.digitaleurope.org/resources/an-early-analysis-of-schrems-ii-key-questions-and-possible-ways-forward/

62. Asian Business Law Institute (2020).

63. ASEAN. Key approaches for ASEAN cross border data flows mechanism. Available at https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf

64. The ASEAN Telecommunications and Information Technology Senior Officials Meeting

65. The ASEAN Telecommunications Ministers Meeting

66. ASEAN. Key approaches for ASEAN cross border data flows mechanism.

67. Digital Europe (2020).

68. Bellamy, B., Heyder, M. (2017). Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy. Centre for Information Policy Leadership. Hunton & Williams LLP. Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf. Cited in: Asian Business Law Institute (2020).

69. Asian Business Law Institute (2020). Transferring Personal Data in Asia: A path to legal certainty and regional convergence

70. Bellamy, B., Heyder, M. (2017).

71. Asian Business Law Institute (2020).

72. Asian Business Law Institute (2020).

73. Heimes, R. (2016). Top 10 operational impacts of the GDPR: Part 9 - Codes of conduct and certifications. The Privacy Advisory. Available at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/

74. Heimes, R. (2018). Top 10 Operational Responses to the GDPR – Part 9: Vetting and contracting with processors. Available at https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-9-vetting-and-contracting-with-processors/

Making Cross-Border Data Happen: Technical Components

Technical interoperability plays a fundamental role in cross-border data flows – and in the data life-cycle more broadly (*see boxout-forthcoming*). Technical interoperability refers to the 'ability to share data between different systems and to enable those systems to make use of the data'[75]. Systems need to have the ability to achieve data interoperability and interconnectivity to ensure that the information flows in a seamless manner when being provided to those who need it, when they need it, where they need it, and in the form in which they need it.

On a practical level, data is compiled and stored by many organisations at global, national, and local levels. Both proprietary and open technologies are currently employed in the management of data. As such, it can be difficult to distribute or share data across various disjointed applications and databases. The challenges associated with data management can impede cross-border data sharing and hinder horizontal data usage entities in different industries and data use mechanisms such as AI and IoT[76].

Connectivity

Both wired and wireless (3G, 4G, and 5G) technologies represent fundamental aspects of the process through which data is collected, shared, distributed and analysed. They provide connectivity between systems and processes, and are crucial foundations in enabling data collection and transfer.

It is essential that a minimum level of meaningful connectivity[77] is set and appropriate levels of investment are made to ensure last-mile access. The cross-border flow of data can also be aided through the use of low-cost connectivity systems, such as community networks, and by releasing spectrum bands to catalyse wireless connectivity.

Considerations

National connectivity can be enhanced through the establishment of various mechanisms. These include local and high-quality Internet Exchange Points, which can drive the development of local connectivity ecosystems. Investments in high-quality wired – including full-fibre – and wireless networks can also lead to significant economic and wider multiplier effects. More broadly, connectivity is founded on strong and effective collaboration between the public and private sectors. This also includes the importance of an enabling environment – including policy and regulation to guide fair spectrum allocation, to balance the rights of landowners with the importance of delivering connectivity, and to accelerate the deployment of network apparatus.

Data Standards

Porism describes how data standards could be explicitly defined as a means of setting out how data is shared, distributed, and accessed by different people and access points[78]. Data standards form the backbone of technical interoperability as they ensure that different applications and systems can reuse metadata and other key components of information in a given data value chain. Operating in accordance with standards is important to achieve interoperability and to improve the quality of data[79].

To accommodate any future reiterations that can be observed in response to data policy changes, novel information sources, and other evolutions in the data supply and value chain, standards need to be both technology-neutral and flexible. Two well-known global bodies that are responsible for managing data standards are the International Organization for Standardization (ISO) and the World Wide Web Consortium (W3C).

Considerations

A W3C study of practices and tooling for Web data standardisation found that the primary objective of data standards is to facilitate service growth while also ensuring interoperability. As per the findings of the W3C, interoperability is only possible when the data formats and items of the vocabulary pertaining to data items are known. Common formats of representing data include Comma Separated Values, JSON (JavaScript Object Notation), and XML.

The W3C encourages data providers to employ common data representations to simplify the future development of services[80] and present a description of their datasets and associated reference guide to alternative data providers. Such descriptions can cover the constraints that may be applied to validate the information and verify the absence of any inconsistency. Communities that are formed of data providers and data users all stand to benefit from the development and implementation of data standards. Such standards can be community-based or may necessitate a more formal approach whereby global players engage in an international agreement pertaining to how the standards are created and managed[81].

State entities can endorse the implementation of standards to facilitate interoperability across applications, databases, and services. One method of promoting the use of standards could involve incentivising organisations in each participating jurisdiction to develop comparable data standards without actually enforcing a distinct set of criteria. This will help governments to remain technology-neutral and future-proof[82].

Data and System Interoperability

Application Programming Interfaces (APIs) are 'computing interface[s] allowing access to a software or technical system and defining the conditions under which the system can be used. APIs are typically intermediate in a standardised manner a series of data (and information) flows between systems'[83]. They represent a sophisticated method of ensuring users, applications, and systems can access data sources over the Internet.

Through using APIs to ensure that higher volumes of real-time data are available to a variety of systems, applications, and users, businesses are better placed to develop cutting-edge offerings. APIs provide interoperability between systems and software, and in this sense they can drive cross-border data flow by connecting not only various datasets and systems across different organisations within the same jurisdictions, but also located in different countries.

These technologies can also be strong mobilisational drivers for national and regional policies and processes. For example, APIX – the open-architecture platform led by the Monetary Authority of Singapore, the International Finance Corporation, and the ASEAN Bankers Association.

Considerations

In a cross-border data flow context, APIs can be employed to ensure secure data exchange. They can embed dynamic identity management controls, for instance, to provide authentication, to determine real-time access privileges, and to track identifies through the data life cycle. A service management platform based on APIs can support the monitoring of large data flows through scanning for anomalies which may represent security or fraudulent events[84].

The OpenAPI Specification[85] has arisen as the standard structure by which it is possible to delineate the interface between services and client applications, Through the use of OpenAPI, players can tap into the power of databases of distributed services a means of making it simpler and more cost-effective to develop applications.

However, it is currently very expensive to integrate legacy system APIs into the more contemporary OpenAPI standards, and some organisations are required to administrate several API services or tailored services to specific uses. One alternative method of enhancing API interoperability is by developing 'API mashups' or an API 'middle layer'. These service provisions extract data from a series of APIs (legacy APIs or alternative services) and re-bundle them in the form of a new API endpoint. API aggregations of this nature can significantly enhance the integration experience and outcomes[86].

However, it was recently noted that communication protocols - i.e. a system which 'defines a set of messages that can be sent between two or more systems to share information and invoke features – via the Internet or other networks (or even on the same computing system)[87]' are better suited to open-up platforms to higher levels of competition underpinned by peer-to-peer communications models[88]

Data Sandboxes

Data sandboxes are used for 'trusted access and re-use of sensitive and proprietary data'[89]. They can be described as 'any isolated environment, through which data are accessed and analysed, and analytic results are only exported, if at all, when they are non-sensitive'[90]. They are a data access mechanism which offer a strong level of control, and therefore they promise to provide access to very sensitive data across borders[91].

Considerations

GSMA has put forward a proposal to operationalise the ASEAN Framework on Digital Data Governance through a regulatory sandbox. The regulatory sandbox is a controlled environment, created for a defined purpose and for a predefined amount of time. According to GSMA, this can be an important first step towards a more formalised mechanism for cross border data flow. It can be viewed as a testing ground to address all concerns that may arise during the implementation of the mechanism[92].

Data Portability

Data portability refers to the ability to transfer data across different systems. It aims at empowering individuals by giving them control and rights over their personal data[93]. It represents a method by which users can switch between different service providers. Vendor lock-in represents one of the primary barriers to achieving data portability. It can arise when proprietary systems, pricing models, and system architectures issue penalties or excessive charges for removing data from a system[94].

Data portability is often regarded as a good way to promote cross-sectoral and cross-border re-use of data (while providing individuals with control rights over their personal or business data). Overall, data portability has a positive effect on the economy and can promote. competition by reducing switching costs across service providers[95].

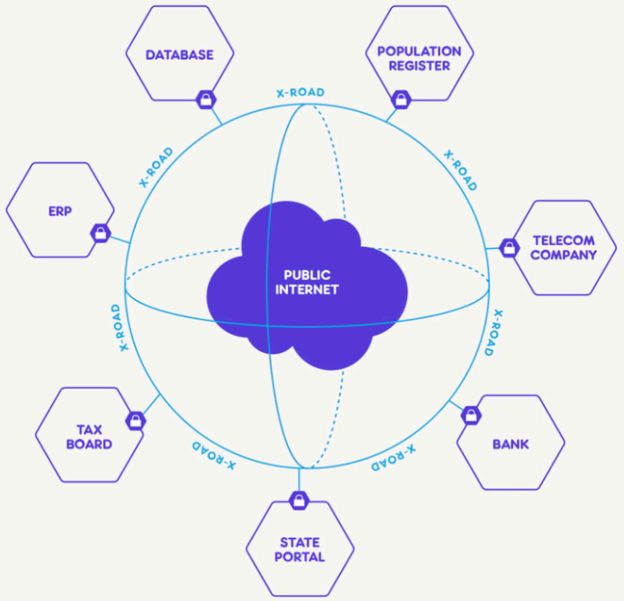
Considerations

The main barriers to data portability are of jurisdictional nature, considering that different countries may implement different definitions and requirements on the conditions under which data portability can occur. However, due to the 'network effects' of many platforms, users may find it difficult to switch to competing services, especially where a significant amount of data is required to be transferred. This can make it very difficult for small start-ups and other small firms to use data portability as a competition lever to compete with large corporations[96].

From a technical point of view, data portability issues may arise due to limitations in the speed at which a physical network infrastructure can permit real-time update to a new system. Finally, if providers put unreasonable contractual clauses pertaining to, for instance, bundling, users may find it difficult to move to a new system. Vendor lock-ins can impede the transmissionof data both locally, nationally, and internationally. It can also prevent new market entrants from participating in the market[97]. More widely, supporting and promoting interoperability standards can have positive multiplier effects in this context.

Data Tracing

Data tracing is employed to guarantee the quality of data and its veracity such as reliability, provenance, and accurateness[98]. It can be defined as the 'digital records of activities and events that are produced, stored and retrieved using information technologies'[99]. Digitally traced data can be either private or public. Private digitally traced data remains inaccessible to the general public, or it can be made available for a fee, while public digital trace data is accessible to the general public.



X-Road (Figure 6)

X-Road (or 'X-Tee') is the foundation to Estonia's digital government, and digital society. It has also been applied in other countries and settings. Founded on canonical data registries, security servers, and 'once-only' legislation, the system ensures that data is not duplicated and can be processed whilst adhering to strict privacy requirements. The Estonian and Finnish governments have established X-Road systems in their respective countries, enabling cross-border data exchange.

Distributed Ledger Technologies (DLT) can support data tracing by providing a cryptographically secure and immutable record of transactions with their associated metadata. It can be defined as an encoded and distributed database which serves as a ledger which records and stores transactions. Cryptography is used in each transaction update[100]. In the context of cross border data flow, the Singapore TradeTrust Initiative uses DLT to provide proof of authenticity and provenance (discussed below). To address some of the inefficiencies caused by manual handling and verification processes, DLT is employed to facilitate the interoperability of electronic trade documents exchanged across different digital ecosystems[101].

Considerations

Although data tracing has potential for facilitating cross border data flow by providing authenticity and provenance of data during the process of transfer, in order for this to be realised the quality of digital data tracing needs to be properly addressed.

However, during the collection, storage, and retrieve, and transformation phases of the datalife cycle, data quality might be compromised. DLT - for instance, blockchain - can be used to record the origin of any data and subsequently track its use through a largely tamper-proof record system. Any operation that is performed on the data is tracked and traced[102].

Data Provenance

Data provenance involves delineating the origin and the owner of the data and subsequently compiling records for all actions involving the data since the point at which it was first collected. The authenticity of the data can be preserved through a robust system of provenance[103].

Data provenance is often a technical issue[104]. If properly implemented, by guaranteeing the origin of data, it can enhance data quality when data is transferred and shared across borders.

Considerations

It can be very challenging, if not impossible, to ensure provenance for de-identified data or any alternative forms of data for which historical information pertaining to its origins is missing. Furthermore, data is typically produced by secondary data producers. As a consequence, in some cases, it can be hard to track the journey of a single data point from its origin through to the point at which it reaches the user.

In these, and other, cases, establishing data provenance is very problematic – if not impossible. In some instances, it could be useful to determine or highlight that a set of data lacks provenance. This designation would then inform any users of that data that there is a potential risk associated with its use or reuse.

Encryption

Encryption is an important element to protect the confidentiality of both stored data and data that is being transmitted between two parties. Encrypting data prevents unauthorised parties from reading it and limits a service providers' capacity to share it with illegitimate users. As such, encryption plays a fundamental role in making sure data is protected during the process of being transmitted.

Encryption systems should be specifically tailored to ensure that they deliver the highest level of data security and privacy. In this context, it is important to protect and safeguard organisations' ability to implement and develop such encryption systems[105].

Considerations

Instructing the development of 'backdoors' or disclosure requests will have explicit consequences in terms of an organisation's ability to achieve the certification requirements or adhere to the contractual conditions related to the transfer of data cross borders. This will ultimately have negative impact on the extent to which data subjects are protected. In this context, states bodies' requirements for the use of encryption should be considered through a principle-based approach to effectively identify and question requests that are unnecessary or disproportionate[106].

When data is transferred across borders, it is important that such transfer happens in a secure way, and that the data is made available at destination. Encryption should be employed at each step of this process, including the transferring, the storage, and while it is displayed at destination. Encryption key management can be leveraged also to prevent decryption of data in countries where the data is not allowed to be transferred[107].

Data Registries and Data Exchange

A data registry is a repository of data, and often allows public and private entities alike to use a shared set of data. By providing support for the creation of administrative level data standards, it ensures that data collected as part of an administrative process is validated and disaggregated[108]. Data registries improve exchange of business-related documents or data and between public sector administrations. In the EU, a federated IT architecture for cross-border data flow across the region has been

set-up, with the aim of connecting registries and e-government architectures across many countries in Europe[109].

Considerations

A good practice of how data registries can be used to facilitate cross border data flow is a project implemented in Estonia and other Northern European countries on online ship and crew certificates maintained by national Maritime Administrations. The process of checking and validating ships and their crews has been made more efficient by making the certificates accessible for Port State Control officers directly from the issuers - not through the Master of the ship as it was previously. The project improves the efficiency of re-using information that exists across different administrative bodies by connecting databases of national Maritime Authorities or internationally recognised classification societies and makes the information available to authorised parties[110].

Another good practice on exchanging data across organisations is X-Road (Figure 6), a free and open source data exchange layer software which provides a 'standard, cohesive, collaborative, interoperable and secure data exchange layer' which combines different services and data sources in a cost efficient and simple way[111]. X-Road is based on a set of standards that facilitates data exchange while at the same time it ensures confidentiality, integrity, and interoperability between data exchange entities. It is the foundation to Estonia's digital government[112].

75. World Economic Forum (2020). A Roadmap for Cross Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy. White Paper. June 2020. Available at http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

76. World Economic Forum (2020).

77. A4AI (2020). Meaningful Connectivity — unlocking the full power of internet access. Available at https://a4ai.org/meaningful-connectivity/

78. Porism. What is a standard? Available at https://standards.porism.com/doc.html#/

79. WEF (2020).

80. W3C study of practices and tooling for Web data standardization. Available at https://www.w3.org/2017/12/odi-study/#standards

81. W3C (2017)

82. WEF (2020)

83. European Commission DG Connect, The Digital Services Act package, 2 June 2020. In: Brown, I. (2020). The technical components of interoperability as a tool for competition regulation. Available at https://cyberbrics.info/the-technical-components-of-interoperability-as-a-tool-for-competition-regulation/

84. Boyd, M., Frejova, J., and Wilde, E. (2020). Better governance, one API at a time. Axway White Paper. Available at https://www.apidays.co/wp-content/uploads/2020/06/axway-wp-better-governance-en.pdf.

85. OpenAPI Specification. Available at https://github.com/OAI/OpenAPI-Specification

86. WEF (2020).

87. Brown, I. (2020). The technical components of interoperability as a tool for competition regulation.

88. Brown, I. (2020)

89. OECD (2020). Mapping approaches to data and data flows.

90. OECD (2019). In: OECD (2020). Mapping approaches to data and data flows.

91. OECD (2020).

92. The GSMA regulatory Sandbox is available at the following link: https://www.gsma.com/asia-pacific/wp-content/uploads/2019/11/ASEAN-Sandbox-Proposal-EXTERNAL-_Final_20190403.pdf

93. OECD (2020). Mapping approaches to data and data flows.

94. WEF (2020)

95. OECD (2020). Mapping approaches to data and data flows. Available at http://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf

96. Brown, I. (2020). Interoperability as a tool for competition regulation. Pre-print. Available at https://osf.io/preprints/lawarxiv/fbvxd

97. WEF (2020)

98. Haviluddin, R. A. (2019). Big data: issues, trends, problems, controversies in ASEAN perspective. Bulletin of Social Informatics Theory and Application, Vol. 3, No. 2, December 2019, pp. 80-93. ISSN 2614-0047. Available at https://repository.unmul.ac.id/bitstream/handle/123456789/3902/2.%20BUSINTA-Big%20Data%20Issues.pdf?sequence=1&isAllowed=y

99. Vial, Gregory (2019). Reflections on quality requirements for digital trace data in IS research, Decision Support Systems, Volume 126, 2019, 113133, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2019.113133. Available at (http://www.sciencedirect.com/science/article/pii/S0167923619301629)

100. I-scoop. Blockchain technology and distributed ledger technology (DLT) in business. Available at https://www.i-scoop.eu/blockchain-distributed-ledger-technology/

101. Loh, S. Y. (2018). TradeTrust: A Singapore Initiative. Available at https://www.unece.org/fileadmin/DAM/cefact/cf_forums/2018_China/Blockchain_Bio-PPT/PPT-07-Loh.pdf

102. WEF (2020)

103. WEF (2020)

104. Casalini, F., and Gonzalez, J. L. (2019). Trade and Cross-Border Data Flows. OECD Trade Policy Papers No. 220, OECD Publishing, Paris. Available at https://www.sipotra.it/wp-content/uploads/2019/03/Trade-and-Cross-Border-Data-Flows.pdf

105. Digital Europe (2020). An early analysis of Schrems II – key questions and possible ways forward. 31 August 2020. Available at https://www.digitaleurope.org/resources/an-early-analysis-of-schrems-ii-key-questions-and-possible-ways-forward/

106. Digital Europe (2020)

107. Epiq Reach. Cross-Border Data: Managing the Risks. Available at https://www.epiqglobal.com/epiq/media/ResourceFiles/Cross-Border-Data-White-Paper-2016.pdf

108. Kwantu. Data Registry. Available at http://www.kwantu.net/data-registry

109. TOOP. Providing data once-only.eu. Available at https://www.toop.eu/info

110. TOOP. Pilot Area 3. Online Ship and Crew Certificates. Available at https://www.toop.eu/pilot-area3

111. GitHub page of X-Road, available at https://github.com/nordic-institute/X-Road

112. X-Road project page. Available at https://x-road.global

Cross-Border Data In Practice: Open Banking

An increasing number of business models are founded on the importance of accessing, holding, analysing and utilising data, including Open Banking. Open Banking is based on the idea of developing a single, cohesive pool of data that spans all products and services. It is anticipated that it could address many of the issues associated with unifying diverse financial services.Open Banking represents an exciting development in the region. The model is expected to provide more transparency and flexibility in financial services. It is estimated that by the end of 2020, 40 per cent of Asia Pacific banks will have invested in open banking management platforms[113].

The complexities associated with measuring the value of data

To measure the value of Open Banking data, a new economic and accounting paradigm is needed. This should take into consideration elements including: (a) the methodologies to assess the value of the data, which should consider the distinctive characteristics of different stakeholders involved; (b) the variety of datasets involved, and what the data contained in the different data repositories is used for; (c) the assessment should treat the data as an asset, including depreciation and amortisation values, the monetised value of data in the balance sheet, and profits and revenues of data[114].

Data is a different type of asset. It is not uniquely consumable, and it does not get destroyed after used, like any other perishable item[115]. Also, the same data can have different value for different stakeholders depending on the intended use of the collector and processor. Last but not least, standard and structured data might have more value than unstructured and 'raw' data. At the same time, data can become a liability if not well-secured and protected. Therefore, in addition to its capacity to generate revenue, a balance sheet should consider the costs to secure it. Another challenge of assessing the value of data is how to attribute revenues, profits, or loss across the different components of the data lifecycle. In the case of Open Banking, for instance, to share or transfer data from one organisation to another can significantly save the costs of collecting data from scratch,

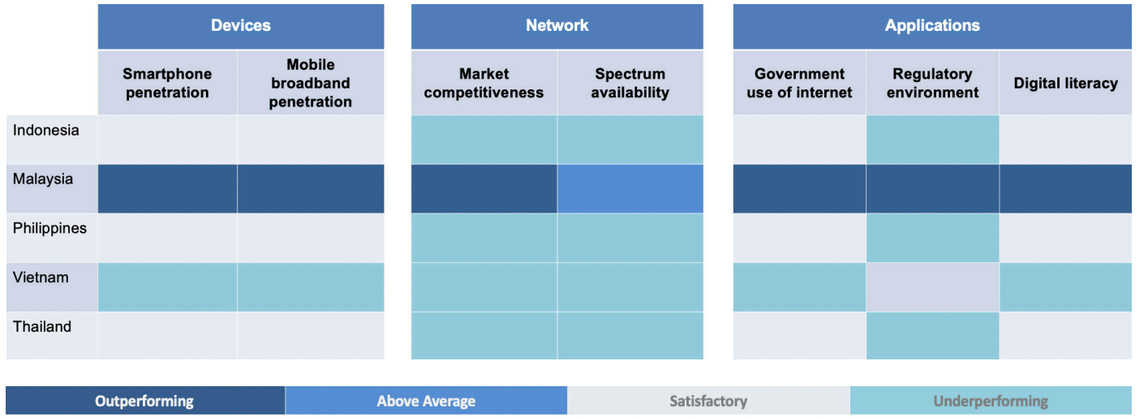


Figure 7 – Variations across devices, networks and applications in digital landscape *(BBVA)*

and can improve the analytics capacity of companies providing banking or other financial services. These companies can then focus their business proposition on value-added and personalised services. In this scenario, the core value of these organisations is not only banking and finance, but a good portion an be attributed to data analytics, optimisation, and data science more broadly.

On a more fundamental level, trust remains crucial. Growth in mobile and Internet banking (estimated to increase by 400 per cent by 2025 in Vietnam[116]) could be hindered by lack of trust in sharing information online. Approximately 70 per cent of digital buyers in the Philippines, 60 per cent in Thailand, and 40 per cent in Singapore are reluctant to share financial information online[117].

An attribution framework to drive cross-border data

An attribution framework could enable cross-border data. This framework should leverage the value of data as a controlled asset, with measurable revenue streams, and with ways to mitigate risks and breaches when they may occur. An attribution framework should also consider the declining value of data over time, to help account for depreciation and data scheduling. In addition, the framework should include security or mis-use costs. The attribution framework could also support taxation, as it would provide a method to reflect the refinement of data (from its initial raw status) and the added value[118] at each stage of the data lifecycle.

Trading rules of attribution can be set through the international and regional trade agreements discussed above, while the methods implementing the ASEAN data governance framework can then provide the right certification and contractual clauses to trade such asset across organisations and borders. At a national level, data protection and cybersecurity legislations should provide legal certainty in terms of protection granted under national jurisdictions – particularly in cases where, during the transaction, either privacy or data security is violated.

How Open Banking is linked to cross-border data

Open Banking is a direct result of digitisation and digitalisation in the finance, banking and payment industries. These sectors are now characterised by increased use of network and digital technologies. This foundational work is proving important. Since the beginning of the COVID-19 pandemic, many banks in the region have reported a surge in online banking activities, including increases in digital transactions and payments - and a rise in the opening of digital accounts. Open Banking architectures have also encouraged financial institutions to innovate quickly to avoid the risk of falling behind.

Open Banking processes significantly increase the flow of data within the economy. By adopting open banking, financial institutions (including banks and 'fintech' organisations) that benefit from extensive access and use of datasets, can generate more effective insights and introduce services that are more closely aligned with their customers' needs. At present, Singapore-based fintech companies dominate the ASEAN fintech sector[120], with Thailand in second place and Indonesia third. The sector is proving to be particularly vibrant; as such, some of the more traditional institutions have started to re-evaluate their portfolio and reposition their offerings.

Data that is shared across different sectors and organisations can be employed and merged in a variety of different ways, leading to the development of novel business frameworks and cutting-edge services as part of a holistic Digital Economy. However, Open Banking is associated with elevated compliance costs. If properly implemented, it is likely that organisations will

seek to pass these costs on to the end-users. Nonetheless, Open Banking is expected to yield a positive net-effect as compliance expenses should be incremental to requirements to offer enhanced access to services, something that will be possible as a result of Open Banking systems[121]. As such, there is a requirement to evaluate compliance as a means of certifying that Open Banking requirements are effectively implemented. Such evaluations should include consideration of competition law and personal data protection law, consumer protection requirements, data protection requirements, data management practices, and the security and interoperability processes used.

How policies and processes could drive Open Banking

Many countries and their regulatory agencies are aware of the potential of Open Banking and are developing regulatory guidance to facilitate a new era of financial services. In Europe, Open Banking is regulated by the European Commission Revised Directive on Payment Services (PSDR2), which introduced a data portability scheme and the concept of Open Banking. PSDR2's provisions require financial institutions to share their customers' financial data with third parties. As with the GDPR, the individual controls what data they are willing to share and who they are willing to share it with.

Some ASEAN countries have accelerated their efforts towards this model. But, contrary to Europe, the region has adopted a market-driven approach to Open Banking. This is broadly in line with the 'ASEAN way' discussed earlier, which centres around voluntary and informal aspects rather than policy or regulatory-driven approaches. Instead, policymakers are introducing a series of measures to accelerate and promote the uptake of frameworks to facilitate data sharing in banking[121].

The potential of Open Banking also depends on technologies, rules and regulations of data portability. Therefore, one of the main challenges of Open Banking is to obtain customer consent for data sharing and portability between different systems used by the same institution, or with external and third party organisations. Considering that an individual's financial data is private, the future of these services depends on the application of a stable regulatory framework and guidelines that set high data protection rules for all parties involved.

According to a Study on Data Portability in Singapore, from a regulatory perspective, implementing data portability requires considering not only data protection legislation, but also competition law. This combination is about determining the best approach to maximising benefits from such a provision, while keeping costs and impact manageable[123].

Data plays an integral role in the development of new products within the financial sector. If a given organisation is not able to access and use key data, it will be at a competitive disadvantage. The implementation of data portability standards could help institutions to access critical information and reduce the barriers to entry that impede expansion and development. This will help to encourage more competition and challenge the status quo that has resulted from the emergence of a small number of dominant players[124].

From the perspective of competition, establishing data portability within the banking sector could help to generate efficiencies for both the banks and any other entities that interact with them by making it more straightforward for entities to access data from a variety of sources. In turn, this could enhance financial institutions' ability to develop new products and services that are aligned with customer needs as the organisation will have better access to meaningful customer insights. Data portability could also decrease the cost of switching from one bank to another as a

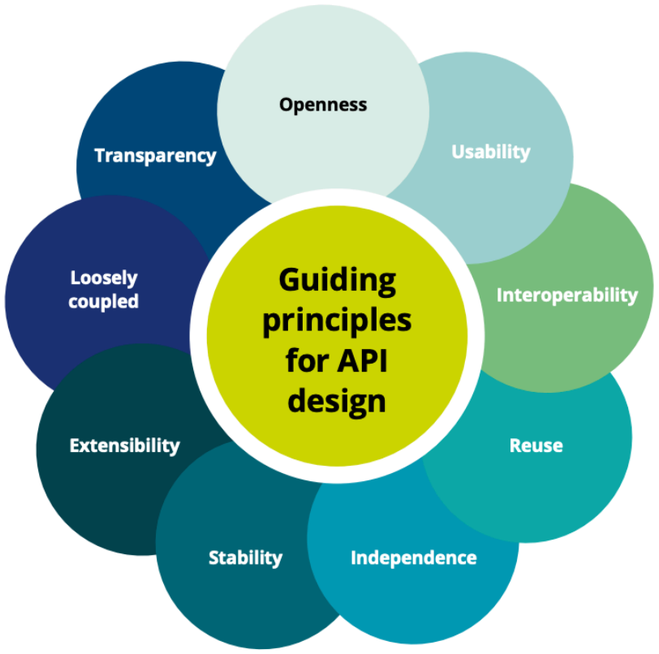


Figure 8 – Guiding principles for API design *(MAS)*

customer can initiate a transfer of his or her data without having to provide it afresh. This would make it easier for consumers to quickly and easily switch suppliers according to which institution is offering the most attractive product or service. Again, this would serve to increase competition[125].

Banking. PSDR2's provisions require financial institutions to share their customers' financial data with third parties. As with the GDPR, the individual controls what data they are willing to share and who they are willing to share it with.

Some ASEAN countries have accelerated their efforts towards this model. But, contrary to Europe, the region has adopted a market-driven approach to Open Banking. This is broadly in line with the 'ASEAN way' discussed earlier, which centres around voluntary and informal aspects rather than policy or regulatory-driven approaches. Instead, policymakers are introducing a series of measures to accelerate and promote the uptake of frameworks to facilitate data sharing in banking[121].

The potential of Open Banking also depends on technologies, rules and regulations of data portability. Therefore, one of the main challenges of Open Banking is to obtain customer consent for data sharing and portability between different systems used by the same institution, or with external and third party organisations. Considering that an individual's financial data is private, the future of these services depends on the application of a stable regulatory framework and guidelines that set high data protection rules for all parties involved.

How technical components could enable Open Banking

Singapore is a leading country on Open Banking

Singapore is a leading country on Open Banking in ASEAN. In line with its ambitious Smart Nation initiatives[126], Singapore has encouraged financial institutions to develop and share open APIs with technology and fintech companies[127]. As part of the programme, the Association of Banks in Singapore and the Monetary Authority of Singapore (MAS) in 2016 issued the Finance-as-a-Service: API Playbook (Figure 8), a comprehensive guide for banks, fintech companies, and other stakeholders interested in adopting the Open Banking model[128]. MAS has also implemented a regulatory sandbox.

Malaysia has also recently begun to explore Open Banking. The country's Central Bank has published its Open Banking Guidelines, focusing on the implementation of Open APIs in three areas: vehicle insurance, credit card products and services, and SME financing[129].

Exploring the value of Open Banking data

Although Open Banking is still a nascent sector in the ASEAN region, a number of indicators relating to the broader economic trends in the region provide a good indication of its potential[130]. According to the World Bank, there are 264 million 'unbanked' adults in Southern East Asia, representing a sizeable customer-base for Open Banking[131]. In addition, more than a half of the ASEAN population are young – and often tech-savvy. 161 million citizens of the region are aged between 15 and 29.

Beyond this, the total amount of digital payments in Asia is anticipated to reach over US$1 trillion by 2025 - accounting for almost half of the spending in the region[132]. By the same year, the e-wallet market is expected to be worth US$114 billion – a fivefold increase from its

	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
Population (in million), 2016	261.1	31.2	108.3	5.6	68.9	92.7
Individual internet users (per 100 people), 2016	25.4	78.8	55.5	81.0	47.5	46.5
Fixed broadband subscribers (per 100 people), 2016	1.9	8.7	5.5	25.4	10.7	9.9
Mobile subscriptions (per 100 people), 2016	149.1	141.2	109.2	146.9	172.6	128.0
Active mobile-broadband subscriptions (per 100 inhabitants), 2016	67.3	91.7	46.3	144.6	94.7	46.6
Smartphone penetration, 2016	24%	35%	15%	85%	37.7%	36%
Network Readiness Index (rank out of 139 countries), 2016	73	31	77	1	62	79
Number of branches (per 100,000 people), 2015	17.8	10.7	8.8	9.3	12.6	3.8
Number of ATMs (per 100,000 people), 2015	58.3	51.1	25.3	60.0	113.5	24.0

Figure 9 – Digital readiness of ASEAN countries (UOB)

value in 2019. Many organisations in the region are also willing to embrace innovation and new technology. A 2016 TRA survey conducted in three ASEAN countries revealed that 71 per cent of organisations in Indonesia intended to invest in online payments in 2016 while approximately 40 per cent were about to deploy mobile wallets. In Singapore, 33 per cent of firms expected to adopt contactless payments in 2017. COVID-19 has likely increased these totals. In a survey conducted by the Emerging Payments Association Asia (EPAA), 75 per cent of industry participants believe that Open Banking will bring value to the payments industry, and that interoperability is needed to reach its full potential. Approximately half of the respondents indicated that national and cross-border interoperability is very important in driving Open Banking[133].

Open Banking can lead to greater personalisation of products, services, marketing and advertising. Indeed, the fact that many digital services are offered at a 'zero price' to the consumer — in exchange for the data and information generated while using them — demonstrates he value of data in the digital economy[134]. This builds on strong foundations. ASEAN consumers find fintech products easy to use, offering fast service, and providing a good user experience. In 2016, investments in the ASEAN fintech market rose about 33 per cent and increased to US$252 million. This growth was primarily supported by seed and angel investors[135]. By September 2017, total investment had already exceeded that of 2016 and was standing at US$338 million.

Key aspects of values

The value of increased data flow resulting from Open Banking comes from a number of interrelated factors. This includes increased competition in the market segment - by creating new and personalised services for customers; through improving productivity, and by increasing transparency and accountability. This latter aspect adds value from a regulatory perspective.

The impact of Open Banking in economic terms is primarily linked to how data portability adds value to the data. Specifically, data portability on the one hand brings about a reduction in the cost of transferring data between different entities (i.e. banks and fintech organisations, for instance); and on the other, value is added by the ability to combine data from different sources.

From the perspective of market competition, Open Banking has the potential to reduce the cost of switching, remove barriers to entry for new service providers, and facilitate expansion. The establishment of data portability will enable consumers to switch between financial institutions.

The value of increased data flow resulting from Open Banking comes from a number of interrelated factors. This includes increased competition in the market segment - by creating new and personalised services for customers; through improving productivity, and by increasing transparency and accountability.

Finally, it will provide a more competitive environment that is open to new providers[136]. The end user will stand to benefit from services that are better aligned with their needs. Furthermore, by exploiting a combination of customer-centric data and real-time credit risk assessments, underlying analytics engines will be able to produce targeted offers that take unique needs into consideration. Individuals' applications for new products and services could also be streamlined, particularly as the vast majority of the data required will already be available to institutions through analytics engines and APIs[137].

More broadly, Open Banking:

- Can increase productivity as a result of facilitating the development of a central repository of data derived from a myriad of sources. This will serve to reduce the cost of delivering data-enabled offerings[138].
- Enhances innovation opportunities by combining datasets in novel ways across business entities that were previously operating in silos.
- Offers benefits from a regulatory perspective. Under Open Banking requirements, financial institutions are required to ensure that user data can be securely accessed. It also fosters transparency across service providers on all aspects of banking - from transaction timeframes through to fees and liabilities.

Value added at each element of the broad data lifecycle

The value of data grows as it moves through the value chain of Open Banking, and it can be repeatedly reused and shared. To maximise such value, the system necessitates both a certain level of standardisation of the data and technical interoperability. Open Banking demonstrates why interoperability is key to increase the value of data across organisations and borders[140].

Data collection

As banks across the region become more digital, they need to standardise data collection practices, digitise (historical) data and clean existing datasets to extract value from them. Banks and other financial institutions collect personally identifiable information about their customers, and by analysing all their transactions (including loans, deposits, and purchase made through credit, debit cards, money transfers and e-wallets), they can have an accurate understanding of individuals' financial strength.

An important element related to their ability to extract value from the data is their capacity for straight-through processing (STP), which refers to the process of consistent and automated data processing. It can considerably reduce human resource costs required in this processing – and save further costs by reducing errors, and error correction. For STP to work effectively, structured and unstructured data needs to be cleaned, and a proper data governance framework must be in place. While siloed systems can transfer data between each other using APIs, the reality is that different systems might use different data structures and taxonomies.

Primarily, banks can open up three datasets, datasets, namely 1) channel-interaction data, for example, cookies and call-centre logs; 2) transaction data; and 3) demographic data. Banks can also source additional data through strategic partnerships with external sources, such as credit bureaus, e-commerce websites, social media platforms, and other service providers[142]. The depth and variety of data and information also presents a challenge in how to create a

single view of the customer. As many financial institutions are a conglomeration of mergers, acquisitions, and divestitures of businesses, each has its own view of the customer. Data associated with customers must be accurate and integrated into one data reference. Open Banking provides the opportunity to aggregate data for a single customer - taking data from a variety of sources to enrich the view of the customer[143]. Single customers' views can be required by regulation, such as in the Philippines.

Data integration and sharing infrastructure

Open Banking platforms rely on APIs, which enable developers to create services for the financial sector. APIs are considered the communication standard of Open Banking. They allow financial institutions and fintechs to connect their systems and provide new offerings to customers[144]. APIs can also facilitate Data Portability.

APIs allow the development of standardised interfaces which make it easier for the financial supply-chain (including billers, merchants, intermediaries, and fintechs) to leverage the value of different platforms producing and hosting different data[145]. They have particular importance in catalysing broader Digital Economy opportunities[146].

APIs are opening up banking systems by providing new services such as central access to banking operations and balances from different financial institutions; real-time querying of a customer's bank before facilitating payments; and allowing instant transfers between different banks and accounts[147]. This is a growing space. As of November 2019, Singapore's API Register has logged 238 transactional and 279 informational APIs[148].

Data Processing and Analytics

Data processing can be used to both generate fresh opportunities and develop bespoke products and services that are based on customer profiles. Open Banking facilitates the integration of multiple datasets, thereby making it possible for financial services to design sales campaign based on customer profiles and insights. It also provides organisations with access to crucial information such as predicted conversion rates based on prior activity, revenue forecasts, and potential prospects.

Financial services can also use the information that is available through Open Banking to develop a customer-centric sales approach. For example, banks can profile customers in accordance with their preferred contact methods. In some cases, customers may be happy to be contacted via email, while others may prefer to be contacted via phone[149].

Multiple forms of sales initiatives can be designed based on the outputs of data analytics. For example, a bank could launch an event- based offering that is triggered when a customer reaches a certain milestone - for instance, fully paying off a loan. Propensity models of this nature can enable banks to reach customers at the most opportune time – and using the most effective channel[150].

In addition to the more traditional methods of automation, Robotic Process Automation (RPA) can act as a supplemental approach that harnesses the power of software-based robots, or AI-supported workers, to emulate interactions between human users and software systems.

Data risk management

For Open Banking to build a sustainable and scalable business model, it requires a foundational risk management framework. Such a framework for Open Banking should cover a number of components. These include cybersecurity, regulatory compliance (related to the institutions' responsibilities to ensure compliance, and prevent money laundering), data privacy (through a consent management framework with regulatory guidelines), contract management (including API and other service-level agreements), and product management (i.e. a procedural framework to foster innovation at a product level)[151].

A data-driven risk management system can be employed to minimise risks of fraud and to make the process of exchanging data more secure. For instance, by enabling access to account data, banks can grant account information services that are legally compliant and digitally analysed. In this way, performing credit checks on customers can become faster, smarter, and more reliable[152].

Data Sharing

The development of open standards for data-sharing in banking is expected to increase competition and innovation in the sector[153]. Financial institutions can transition towards a pan-regional cross-border payment system by working with technology providers which embed privacy and security by design and leveraging existing standards such as ISO 20022. At the same time, this will allow them to retain extensibility for future upgrades and extensions[154]. Using established standards reduces standardisation costs and improves the interoperability of applications across institutions.

There is a significant value associated with the adoption of standards such as ISO 20022[155]. ISO 20022 is an international standard for financial communication and electronic data exchange between financial institutions. It is considered the global and common language for financial communications of the future[156]. The standard is agnostic of technology and can be used in different formats (including XML, JSON, etc.)[157]. It can be used to execute payments, to trade in securities, and finance supply chain, or to manage clients' accounts[158].

113. Backbase (2020). Available at https://www.backbase.com/2020/04/22/best-fintech-digital-banking-articles-in-asean-of-april-may-2020/

113. Backbase (2020). Available at https://www.backbase.com/2020/04/22/best-fintech-digital-banking-articles-in-asean-of-april-may-2020/

114. Institute of international finance (2020). Briefing note: Data Monetization – a new accounting paradigm? The Global Dialogue on Digital Finance. September 2020. Available at https://www.iif.com/Portals/0/Files/content/Innovation/09_28_2020_iif_briefing_note.pdf

115. Institute of international finance (2020).

116. Backbase (2020). Best Fintech & Digital Banking Articles in ASEAN of April & May 2020. April 22, 2020. Available at https://www.backbase.com/2020/04/22/best-fintech-digital-banking-articles-in-asean-of-april-may-2020/

117. BBVA Research (2017). Fintech in Emerging ASEAN. Trends and Prospects. June 2017. Available at https://www.bbvaresearch.com/wp-content/uploads/2017/07/June-2017-ASEAN-Fintech-Trends1.pdf

118. Hardoon, D. (2020). In: Institute of international finance (2020).

119. PDPC Singapore (2019). Discussion paper on Data Portability. 25 February 2019). Available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf

120. BBVA Research (2017). Fintech in Emerging ASEAN. Trends and Prospects. Available at https://www.bbvaresearch.com/wp-content/uploads/2017/07/June-2017-ASEAN-Fintech-Trends1.pdf

121. PDPC Singapore (2019).

122. Deloitte. Blurring the lines. Creating an Open Banking data-sharing ecosystem. Available at https://www2.deloitte.com/ie/en/pages/financial-services/articles/Creating_an_Open_Banking_data_sharing_ecosystem.html

123. Competition & Consumer Commission Singapore (2019). Discussion Paper on Data Portability: Personal Data Protection Commission In collaboration with Competition and Consumer Commission of Singapore. Available at https://www.cccs.gov.sg/resources/publications/occasional-research-papers/pdpc-cccs-data-portability

124. PDPC Singapore (2019).

125. PDPC Singapore (2019). Discussion paper on Data Portability. 25 February 2019). Available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf

126. Smart National Singapore. Transforming Singapore through technology. Available at https://www.smartnation.gov.sg

127. Monetary Authority of Singapore. Application Programming Interfaces (APIs). Available at https://www.mas.gov.sg/development/fintech/technologies---apis

128. Finance-as-a-Service: API Playbook. Available at https://abs.org.sg/docs/library/abs-api-playbook.pdf

129. Bank Negara Malaysia (2019). Policy Document on Publishing Open Data using Open API. 07 Jan 2019. Available at https://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement&ac=687

130. Tech Research Asia TEMENOS (2019). Open Banking: The New Paradigm In Asia Pacific Financial Services Open APIs ensure beneficial collaboration in financial sector. Available at https://www.temenos.com/wp-content/uploads/2019/07/open-banking-apac-paradigm-whitepaper-2018-apr-23.pdf

131. De Luna-Martinez, J. (2016) How to scale up financial inclusion in ASEAN countries. World Bank Blogs. Available at https://blogs.worldbank.org/eastasiapacific/how-to-scale-up-financial-inclusion-in-asean-countries

132. Francisco, J. (2019). How Southeast Asia is Playing a Crucial Role in Driving Payment Flexibility. December 23, 2019. Available at https://www.entrepreneur.com/article/344183

133. Fintechnews Singapore (2020). Singapore Leads Asia Pacific in Open Banking. February 28, 2020. Available at https://fintechnews.sg/37980/openbanking/singapore-open-banking-apac/

134. Institute of International Finance (2018). Reciprocity in customer data sharing frameworks. July 2018. Available at https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf

135. UOB. State of FinTech in ASEAN. Available at https://www.uobgroup.com/techecosystem/pdf/UOB-State-of-FinTech-in-ASEAN.pdf

136. PDPC Singapore (2019).

137. McKinsey&Company (2013). Retail banking in Asia. Actionable insights for new opportunities. Available at https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/financial%20services/latest%20thinking/consumer%20and%20small%20business%20banking/retail_banking_in_asia_actionable_insights_for_new_opportunities.pdf

138. PDPC Singapore (2019).

139.https://www.pymnts.com/api/2019/open-banking-cross-border/

140. WEF (2020).

141. Banking Hub (2017). Straight-through processing: taking current opportunities and overcoming challenges. Case study: successfully implementing straight-through processing. Available at https://www.bankinghub.eu/banking/finance-risk/straight-processing-taking-current-opportunities-overcoming-challenges

142. McKinsey&Company (2013)

143. McKinsey&Company (2013)

144.https://www.pymnts.com/api/2019/open-banking-cross-border/

146. https://www.paymentscardsandmobile.com/open-banking-market-could-be-worth-7-2bn-by-2022/

147. Limonetik (2019). Grégory Boulanger presents: Using APIs for payment: a trade-off between openness and security. 28 March 2019. Available at https://www.limonetik.com/gregory-boulanger-presents-using-apis-for-payment-a-trade-off-between-openness-and-security/

148. Monetary Authority of Singapore. Financial Industry API Register. Available at https://www.mas.gov.sg/development/fintech/financial-industry-api-register

149. Banking Hub (2017). Straight-through processing: taking current opportunities and overcoming challenges. Case study: successfully implementing straight-through processing. 14 December 2017. Available at https://www.bankinghub.eu/banking/finance-risk/straight-processing-taking-current-opportunities-overcoming-challenges

150. McKinsey&Company (2013)

151. The Digital Fifth (2020). Risk Management: Most Critical Element to Open Banking. March 3, 2020. Available at https://thedigitalfifth.com/risk-management-most-critical-element-to-open-banking/

152. FintecSystems (2020). How Open Banking Increases the Security, Speed and Intelligence of Risk Management. 13 January 2020. Available at https://knowledge.fintecsystems.com/en/blog/open-banking-risk-management

153. The Open Banking Standard. Available at http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf

154. Daily News Starkville (2020). Southeast Asia's Cross-Border Real-Time Payments Network Emerges with Payments Innovation as Driving Force, New Research from ACI Worldwide and Kapronasia Reveals. Available at http://business.starkvilledailynews.com/starkvilledailynews/news/read/40108873/southeast_asia%E2%80%99s_cross

155. 'SWIFT estimates that by 2023, 80 percent of high-value payments by volume and 90 percent by value will already have migrated to ISO 20022'. https://bankingblog.accenture.com/iso-20022-watershed-moment-payments-industry

156. Accenture (2019). ISO 20022: A watershed moment for the payments industry. Available at https://bankingblog.accenture.com/iso-20022-watershed-moment-payments-industry

157. heikh, S. (2019). ISO 20022: a better payments experience for customers. In: Finextra. Available at https://www.finextra.com/blogposting/18222/iso-20022-a-better-payments-experience-for-customers

158. Sheikh (2019).

Concluding Thoughts

There are significant positive multipliers of enabling cross-border data, as highlighted in the Open Banking case study. In addition, there are a number of risks. Recognising this, al ASEAN countries – large and small; digital leaders and explorers – should contribute to shaping the policy, regulatory, and technical standards of cross-border data. This will require:

- National prioritisation and engagement with the realities of cross-border data – from policies (including those on internet access, data usage, and privacy) through to the underlying technical architecture highlighted below. For the former, this includes 'open by default' data policies – which could catalyse cross-border data, in a similar way to how they have enabled national data efforts in many countries.

- Shaping a strong regional data governance framework to boost the above potential – and mitigate data-related risks and harm. This includes formalising 'cooperation mechanisms to ensure shared responsibility for data privacy' and other priorities. The contractually-enforceable ASEAN MCCs are a strong foundation, whilst international trade with regions such as the EU highlight the need for frameworks such as the GDPR that move beyond the 'open regionalism' foundations of the ASEAN region.

- Avoiding data localisation or similar protectionist approaches. This includes regional discussion between those countries that have implemented data localisation or residency requirements, in order to identify ways of removing these barriers to national and regional benefits.

- Ensuring continued convergence between national policies, particularly data protection legislation and other foundational aspects. This does not require case-by-case assessment of each country's privacy regime – but at least a focus on avoiding further divergence.'

- Taking a forward-thinking approach to regulation, particularly in the context of a technology-driven and fast-moving sector. Singapore's consideration of permitting the use of copyrighted material to inform text and data mining is one example, as well as emerging discussions around data trusts and other initiatives. The speed of change in the sector may also require a more agile, iterative, and experimental approach to regulation, legislation, and policymaking.

- Investing in, and enabling, the considerable technical foundations needed to enable cross-border data. These include extensive and high-quality connectivity, shaping data standards, and developing API functionalities. Foundational national infrastructure – such as data registries, and technologies such as DLTs – are also important. Wherever possible, countries should seek to build on and expand international best practice – particularly to ensure tech-neutrality and future-proofing.

All of the above is founded on collaboration with all stakeholders in the national, and regional, data ecosystem. However, of particular importance is the need for extensive industry engagement – from rolling-out connectivity, through to shaping standards.

The speed of change in the sector may also require a more agile, iterative, and experimental approach to regulation, legislation, and policymaking.

Singapore's recent Digital Economy Partnership Agreement, drawing on extensive private sector engagement, is a strong example here.

A pathway to convergence

Broader work on shaping an effective governance framework around open data can be extended to facilitate cross-border data flow. In particular, the 'ten key elements of an effective governance framework'[160] have particular relevance beyond borders.

The elements of the framework are:

1. A strategic vision – defining and guiding actions, actors, and sector initiatives in pursuit of common strategic objectives. A shared strategic vision should be complemented by a roadmap or action plan for implementation and should be backed by clear public leadership.

2. Legal and regulatory framework – providing for required changes in the laws or regulations to support safe and effective release and reuse of open data.

3. Institutional and organisational leadership arrangements – providing a focal point for reforms, but distributing responsibilities for data release and use across government as far as is appropriate given capacity.

4. Technical infrastructure – providing for data searching, access, sharing, and reuse.

5. User engagement – increasing the value of data as a public good by meeting user requirements and identifying priority high-value datasets.

6. Partnerships – establishing partnerships both across government institutions and with other governments, civil society organisations, and the private sector. Established partnerships move beyond ad hoc interaction to have an on-going model of engagement with clear, stable, and transparent processes for public administration officials to work together on publishing and using data.

7. Sustainable funding – identifying sustainable sources to resource the implementation of open data policy and related initiatives.

8. Capacity building – establishing programmes that ensure the necessary intellectual, human, and financial resources for on-going provision and use of data.

9. Communication planning – ensuring broad communication of intentions, efforts, and results.

10. Measurement processes – assessing and publishing results of open data efforts in order to take corrective actions as needed to realise the strategic vision for open data, secure value creation, and ensure continuous support for reforms.

Cross-border data is an important aspect of national, regional, and global economic development – including driving progress toward achieving the Sustainable Development Goals.

The role of international partners

Reflecting the international nature of cross-border data exchange, the role of international organisations – including the private sector, and multilateral institutions, is important. This includes driving progress in cross-border data development and usage by:

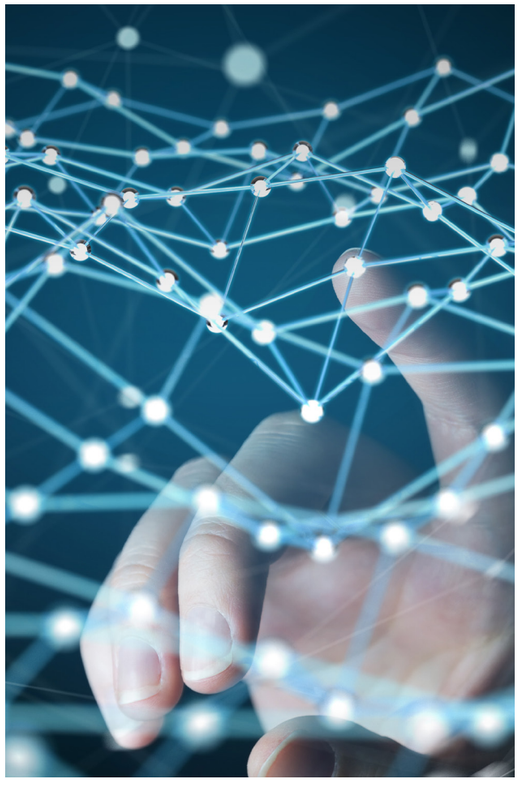
- Supporting coordination at an ASEAN level, including guiding alignment of cross-border data privacy – and other standards – in the region in order to drive economic and broader benefits.

- Building capacity and expertise, particularly in supporting policymakers and regulators in engaging with a complex, fast-moving, and evolving technical and technological landscape.

- Driving collaboration and shaping best practice. In addition to capacity building activities, there is scope to facilitate more substantive coordination. For example, defining a multi-stakeholder group focusing on driving cross-border data flows for economic and social development. This would build on the existing and important efforts of the ASEAN Data Protection and Privacy Forum.

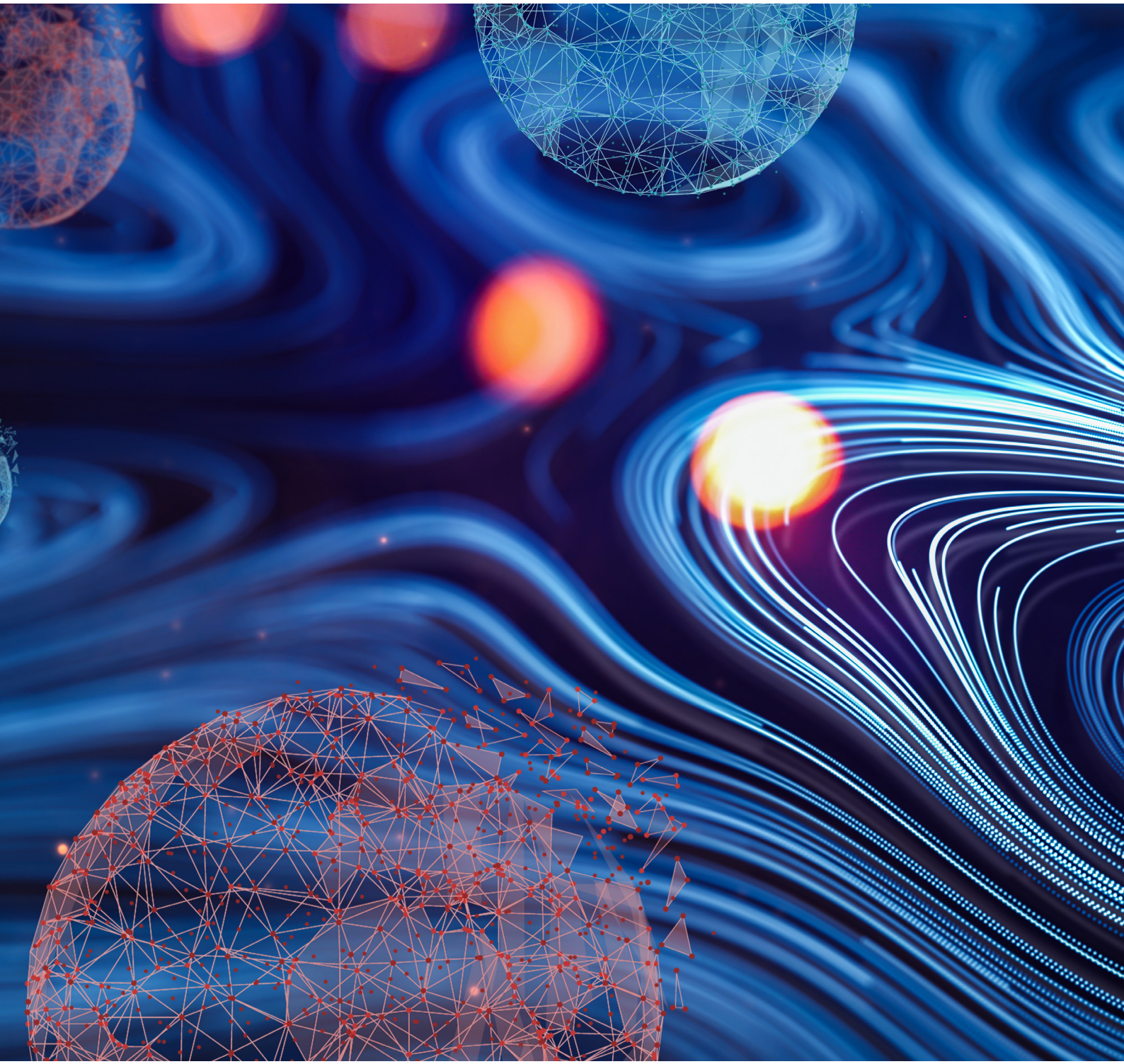
All of these efforts should be founded on working closely with existing initiatives, and not duplicating efforts. This includes alignment with the Working Group on Digital Data Governance (WG-DDG), which is appointed to develop the standards, requirements and processes for the operationalisation of the ASEAN Cross Border Data Flows Mechanism.

How we manage cross-border data is an important aspect of national, regional, and global economic development – including driving progress toward achieving the Sustainable Development Goals. Similarly, leveraging the benefits of emerging and new technologies will demand looking outward – recognising the digitalisation, data, and innovation often do not recognise borders. This perspective will be crucial in seizing opportunities, as well as addressing shared global challenges in using data to drive policymaking, service delivery, and wider development.



159. WEP Roadmap

160. Ubaldi, B. (2019). Governments. In: State of Open Data. Open data for development. Available at https://stateofopendata.od4d.net/chapters/stakeholders/government.html



@UNDPtech
registry.sg@undp.org