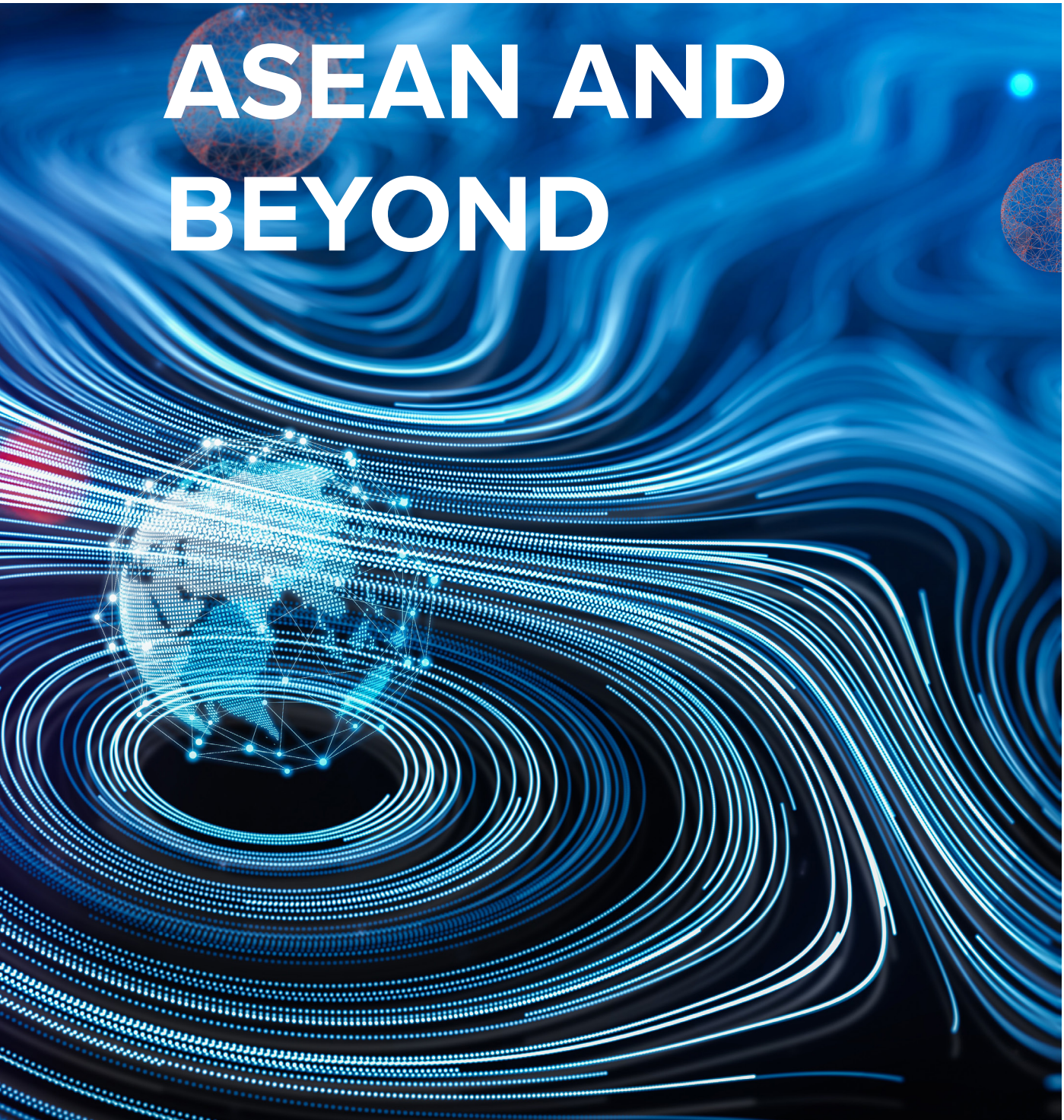
EXECUTIVE SUMMARY

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

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

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

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.

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. This could lead to the adoption of sub-optimal and vulnerable IT infrastructures, which may then increase the risk of cybersecurity attacks.[3]

Intellectual property rights

The digital economy generates a large volume of data, which has great value for economic actors.[4] While data in the personal domain is usually protected by privacy regulation, proprietary compilation of data is normally protected by intellectual property rights (IPR). In a digital environment, intellectual property can be seen as a security measure when data moves across borders, 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.[5]

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. Without this exception, the act of mining and analysing data may infringe copyright, in turn limiting data activities.[6]

Cross-border data mechanisms

The ASEAN framework on Digital Data Governance, adopted in 2017, is an attempt to develop a conducive regulatory framework even in a context of varying national data maturities across countries.[7] 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 when data is transferred.[8] 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.

Potential approaches to enable 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. 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.

- **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.[9]

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

- **Binding Corporate Rules** (BCRs). BCRs were established in the EU as a means to transfer data across borders. Organisations adhere to these data protection protocols when transferring any personal data between enterprises or groups.

- **Codes of Conduct**. Codes of Conduct are designed by professional and representative bodies. They can be particularly useful as they allow businesses to develop bespoke data protection provisions that are aligned with their unique requirements.

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. Technical interoperability refers to the 'ability to share data between different systems and to enable those systems to make use of the data'.[10] 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.

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.

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.

Data Standards

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.[11]

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. This will help governments to remain technology-neutral and future-proof.[12]

Data and System Interoperability

Application Programming Interfaces (APIs) are a sophisticated method of ensuring users, applications, and systems can access data sources over the Internet.

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.[13]

Data Sandboxes

Data sandboxes are used for 'trusted access and re-use of sensitive and proprietary data'.[14] 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.[15]

GSMA has put forward a proposal to operationalise the ASEAN Framework on Digital Data Governance through a regulatory sandbox. 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. [16]

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.[17] It represents a method by which users can switch between different service providers.

The main barriers to data portability are of a jurisdictional nature, considering that different countries may implement different definitions and requirements on the conditions under which data portability can occur. This can make it very difficult for start-ups and other SMEs to use data portability as a competition lever to compete with large corporations.[18]

Data Tracing

Data tracing is employed to guarantee the quality of data and its veracity such as reliability, provenance, and accurateness.[19] Digitally traced data can be either private or public.

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**. Distributed Ledger Technologies - for instance, blockchain - can be used to record the origin of any data and subsequently track its use.

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. Data provenance is often a technical issue.[20] If properly implemented, by guaranteeing the origin of data, it can enhance data quality when data is transferred and shared across borders.

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.

Encryption

Encryption is an important element to protect the confidentiality of both stored data and data that is being transmitted between two parties. As such, encryption plays a fundamental role in making sure data is protected during the process of being transmitted.

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 the destination. Encryption can also prevent decryption of data in countries where the data is not allowed to be transferred.[21]

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. 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.[22] A separate project has made the process of validating ships and their crews more efficient by making the certificates accessible for Port State Control officers directly from the national issuers.[23]

Case Study: 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 financial products and services. It is anticipated that it could address many of the issues associated with unifying diverse financial services – and could provide transparency and flexibility.

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. 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. 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 rule for all parties involved.

How technical components could enable Open Banking

Singapore is a leading country on Open Banking in ASEAN. In line with its ambitious **Smart Nation** initiatives.[24] Singapore has encouraged financial institutions to develop and share open APIs with technology and fintech companies.[25] As part of the programme, the Association of Banks in Singapore and the Monetary Authority of Singapore (MAS) in 2016 issued the **Finance-as-Service:** API Playbook, a comprehensive guide for banks, fintech companies, and other stakeholders interested in adopting the Open Banking model.[26] 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.[27]

Exploring the value of Open Banking data

The impact of Open Banking in economic terms is primarily linked to how **data portability** adds value to the data – both through reducing the cost of transferring data between different entities, and the value added by combining 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. Finally, it will provide a more competitive environment that is open to new providers.[28]

The **end user will stand to benefit from services** that are better aligned with their needs. 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.[29]

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.[30]
- Enhances innovation opportunities by combining datasets in novel ways across business entities that were previously operating in siloes.
- 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 time-frames through to fees and liabilities.[31]

Value added at each element of the data lifecycle

Data Collection

- Banks need to standardise data collection practices, digitise data and clean existing datasets to extract value by building an accurate understanding of individuals' financial strength.

Data Integration

- APIs allow the development of standardised interfaces which make it easier for the financial supply-chain (including billers, merchants, and intermediaries) to leverage the value of different platforms producing and hosting different data.[32]

Data Processing

- Data processing and analytics can be used to both generate fresh opportunities and develop bespoke products and services that are based on customer profiles.

Risk Management

- Open Banking requires a foundational data-driven risk management system to minimise risks of fraud and to make the process of exchanging data more secure. Performing credit checks on customers can become faster, smarter, and more reliable. [33]

Data Sharing

- Open standards for data-sharing in banking is expected to increase competition and innovation in the sector.[34] Using established standards reduces standardisation costs and improves the interoperability of applications across institutions.

Concluding Thoughts

There are significant positive multipliers of enabling cross-border data. Recognising this, all ASEAN countries – large and small; digital leaders and explorers – should contribute to this area. This will require:

- National engagement with the realities of
- Ensuring continued convergence between national policies, particularly data protection legislation and other foundational aspects.
- Taking a forward-thinking approach to regulation, particularly in the context of a technology-driven and fast-moving sector.
- Investing in, and enabling, the considerable technical foundations needed to enable

All of these efforts should be founded on working closely with existing initiatives, including alignment with the Working Group on Digital Data Governance (WG-DDG).

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.