



TECH FOR
GOOD
INSTITUTE



Report – January 2024

Evolution of Tech Regulation in the Digital Economy

Spotlight On Southeast Asia



This spotlight is produced in collaboration with Australian National University's Tech Policy Design Centre.



Australian
National
University



TECH POLICY
DESIGN CENTRE

Table of Contents

| | |
|--|----|
| About this Paper | 03 |
| Foreword | 04 |
| Acknowledgments | 05 |
| About the Tech for Good Institute | 06 |
| Executive Summary | 07 |
| 1. Tech Regulators in Southeast Asia's Digital Economy | 09 |
| 2. Country Overviews | 11 |
| Indonesia | 12 |
| Malaysia | 17 |
| Philippines | 22 |
| Singapore | 25 |
| Thailand | 32 |
| Vietnam | 37 |
| 3. Regulatory Trends in Southeast Asia's Digital Economy | 41 |
| 3.1. Existing regulators are seeing their roles expand | 42 |
| 3.2. Specialist agencies emerge with fresh mandates | 42 |
| 3.3. Increasing the need for coordination | 43 |
| 4. Coordination Recommendations | 44 |
| 4.1. Between government agencies | 44 |
| 4.2. Between the public and private sector | 45 |
| 4.3. Between governments in Southeast Asia | 45 |
| References | 48 |

About this Paper

The Tech for Good Institute was founded to encourage conversations and collaborations on how the promise of technology and the digital economy may be leveraged for sustainable, equitable and inclusive growth for Southeast Asia. The Institute believes that this is only possible if technology and technology-enabled business models evolve within an ecosystem in which the public, private and civil sectors collaboratively shape the future of our communities and societies.

The Tech for Good Institute is thus delighted to work with the Tech Policy Design Centre (TPDC) to provide an overview of the tech regulator landscape in six Southeast Asian countries: Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam.

Taken collectively as “SEA-6,” these countries are part of a young, ambitious, diverse and fast-growing region. Each is balancing the challenges of encouraging innovation while maintaining national security, ensuring that markets work and safeguarding society.

Building on the TPDC’s report *Tending the Tech Ecosystem*, this paper identifies the regulators responsible for key areas of governance related to the digital economy. It is our hope that a shared understanding of “who” is developing and enforcing policy enables citizens, companies, researchers and policymakers to better interpret “how” technology governance is pursued in each jurisdiction.

This review is but a “snapshot” of current practice as of 2023. We are keenly aware that the rapid evolution of technology, coupled with the pace of change within each country, will mean continued changes in the tech regulatory landscape. We welcome your feedback, especially with regard to any inaccuracies, omissions or obsolete information. We are keen for this to be a useful resource and your comments would be greatly appreciated.

Nevertheless, as a starting resource, we hope that this foundational work will be useful to policymakers, researchers, industry practitioners and others who continuously work to co-create a safe and vibrant digital economy for all.

Foreword

This paper from the Tech for Good Institute could not be timelier.

Governments the world over are grappling with how best to regulate technology. Identifying tech regulators is a vitally important and deceptively complex task.

Just as technology has pervaded every aspect of our lives, it has pervaded nearly every aspect of existing regulatory frameworks, with varying degrees of maturity.

In 2022, The ANU Tech Policy Design Centre partnered with Tech for Good Institute to produce TPDC's inaugural research report, Tending the Tech Ecosystem. Our research considered best practice models for regulation of the tech-ecosystem.

That report advocated for upskilling and improving coordination among existing tech regulators. It also underscored the need for better coordination among and between regulators and policymakers. The knowledge asymmetry between industry and regulators was also a dominant theme.

Tending the Tech Eco-System included a compendium of tech regulators in 13 jurisdictions globally. I am delighted that in this paper, Spotlight on Southeast Asia: Evolution of Tech Regulation in the Digital Economy, the Tech for Good Institute expands and updates that work to cover the "Southeast Asia 6": Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam.

Each country organises itself differently, so it is not possible to draw direct comparisons. However, the overviews and information in this paper will help deepen understanding of different approaches, highlighting where they converge and diverge as well as lessons and/or models that may be transferable to other jurisdictions.

I firmly believe that it is possible to reward innovation, drive economic growth, strengthen democracy, enhance security and shape an environment (online and offline) in which individuals and communities can thrive. These objectives are not mutually exclusive – but to achieve each concurrently requires nuanced regulatory responses. Understanding the regulatory landscape is foundational to achieving the nuance that will underpin effective tech regulation. I commend this paper to anyone interested in deepening their understanding of how Southeast Asian jurisdictions regulate technology.

My team and I look forward to continuing to work with Tech for Good Institute as we deliver on our mission to shape technology for the long-term benefit of humanity.

Johanna Weaver
Founding Director
ANU Tech Policy Design Centre
December 2023

Acknowledgments

The Tech for Good Institute would like to thank Australia National University's Tech Policy Design Centre (TPDC) for the conceptual framework of this paper. The Institute would also like to express our gratitude to our partners who provided inputs and feedback for this paper:

- Johanna Weaver, Tech Policy Design Centre
- Ibrahim Kholilul Rohman, Indonesia Financial Group Progress
- Farlina Said, Institute of Strategic and International Studies
- Benjamin Ang, Center of Excellence for National Security
- Thitirat Thipsamritkul, Thammasat University
- Nguyen Minh Thao, Central Institute for Economic Management

The Tech for Good Institute is also grateful to Grab for supporting TFGI's mission of leveraging the promise of technology and the digital economy for inclusive, equitable, and sustainable growth in Southeast Asia. Funders do not determine research findings nor the insights and recommendations of research.

Disclaimer

The information in this paper is provided on an "as is" basis. This paper is not to be considered as a recommendation for investments in any industry. This document is produced by the Tech for Good Institute and has been prepared solely for information purposes over a limited time period to provide a perspective on the region. The Institute and any of its affiliates or any third party involved make no representation or warranty, either expressed or implied, as to the accuracy or completeness of the information in the paper, and no responsibility or liability whatsoever is accepted by any person of the Institute, its affiliates, and its respective officers, employees or agents.

About the Tech for Good Institute

The Tech for Good Institute is a non-profit organisation working to advance the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia.

With a population twice the size of the US and strong demographics, Southeast Asia's digital economy is evolving rapidly. At the same time, the region's trajectory will be unique, shaped by its diverse cultural, social, political, and economic contexts.

The Tech for Good Institute serves as a platform for research, conversations, and collaborations focused on Southeast Asia while maintaining global connections. Our work is centred on issues at the intersection of technology, society, and the economy, and is intrinsically linked to the region's development. Through research, effective outreach, and evidence-based recommendations, we seek to understand and inform policy with rigour, balance, and perspective.

The Institute was founded by Grab to advance the vision of a thriving and innovative Southeast Asia for all. We welcome opportunities for partnership and support, financial or in-kind, from organisations and individuals committed to fostering responsible innovation and digital progress for sustainable growth in the region.

More information about the Institute can be accessed at www.techforgoodinstitute.org.



Executive Summary

➤ Regulation of the tech ecosystem in Southeast Asia reflects different approaches.

Governments are recognising the importance of updating laws and regulations to address the challenges of emerging technologies and the innovative business models they enable. The mandate of governing the digital economy is usually spread across different agencies in each of the SEA-6 countries, with Thailand pursuing a more integrated approach.

➤ While there are different approaches to governing the digital ecosystem in the SEA-6, there are common goals that are evident across countries.

Common areas of focus include:

1. Preserving competition for innovation
2. Protecting consumers
3. Safeguarding personal data to foster trust, and
4. Enhancing cybersecurity

This is reflective of a common goal of balancing digital innovation and protecting the public's interest.

➤ Existing regulators in SEA-6 economies are seeing their regulatory roles expand.

With new technologies and innovative business models, the mandate of regulators now includes areas traditionally not within their purview. For example, the rise of e-commerce has added new policy areas for trade ministries and central banks. Transport franchising regulators have also seen an expansion of their mandate to include ride-hailing services and transport-sharing services. In some cases, reorganisation within and between ministries has been necessary to adapt to the changing landscape of the digital economy.

➤ New regulators with fresh mandates are also being established.

Digitalisation has introduced new challenges unique to the digital economy. For example, data protection agencies have been created to respond to the need for safeguarding personal data in our new digital reality. Cybersecurity agencies are also being formed to protect critical technologies and information systems, address cyber threats, foster trust in the ecosystem, and enable a more resilient digital ecosystem.

➤ With rapid technological developments, coordination of tech policy is key to enabling a responsive regulatory environment.

Technology and business innovation moves faster than traditional policymaking. To keep pace with the impact of digital transformation, tech policy coordination is needed among government agencies, between public and private sectors, and across countries.



1. Tech Regulators in Southeast Asia's Digital Economy

Southeast Asia is a diverse region with a rapidly growing tech ecosystem. The state and rate of digital evolution varies significantly across Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam (collectively known as "SEA-6").¹

In recent years, regulators in SEA-6 have been working to update laws and regulations to address the challenges emerging from tech innovation and the new business models it enables, while driving economic growth through digital transformation. As with the jurisdictions reviewed under the Tending the Tech Ecosystem report by Tech Policy Design Centre,² the responsibility for tech regulation is spread across different agencies in each of the SEA-6 countries.

Common objectives centre around:

- Preserving competition for innovation;
- Protecting consumers and small businesses;
- Protecting personal data, and;
- Enhancing cybersecurity.

This paper focuses on tech regulators in the digital space, defined as "government officials, departmental units and independent statutory authorities that are empowered to administer and enforce tech regulation, or more specifically to: grant approvals (including registration and licensing); monitor compliance; and enforce the regulations."³

Governments play many roles in developing a safe, trusted and vibrant digital tech ecosystem of which regulation is but one. Other vital efforts such as promoting emerging industries, encouraging investment, showcasing best practices and developing talent are just as important, but are not part of this focused review.

Definition of terms for the purposes of this paper are adopted from the ANU Tech Policy Design Centre's report on [Tending the Tech Ecosystem: who should be the tech-regulator\(s\)?](#).

Table 1. Definition of Terms

| Term | Definition |
|------------------------|---|
| Regulation | An intentional form of intervention [...] in the economic activities of a target population with the aim of achieving a public policy objective or set of objectives. The intervention can be direct and/or indirect, the activities can be economic and/or non-economic, and the regulatee may be a public or private-sector actor. ⁴ |
| Regulators | Government officials, departmental units and independent statutory authorities that are empowered by legislation to administer and enforce regulation, or more specifically to: grant approvals (including registration and licensing); monitor compliance; and enforce laws. ⁵ |
| Tech Sector | <p>Includes:</p> <ul style="list-style-type: none"> • Companies and individuals whose core business is to develop digital technologies, including infrastructure, hardware, software, products, platforms and services (or a combination of some or all of those elements); and • Companies and individuals whose core business is to develop digital technologies to deliver previously analogue products and services (for example: fintech, healthtech and agritech companies). |
| Tech-ecosystem | <p>Is broadly defined to include:</p> <ul style="list-style-type: none"> • The tech sector, its employees and financiers; • Manufacturers, retailers, installers and repairers of digital technologies; • End users of digital technologies (government, enterprises or individuals); • Entities (other than companies and individuals for whom it is a core business) that develop digital technologies, study the impact of digital technologies or support the tech sector's talent pipeline; • Entities (public or private) that design and implement tech regulation; and • Tech regulators. |
| Tech Regulation | An intentional form of intervention in the tech ecosystem with the aim of achieving a public policy objective or set of objectives. The intervention can be direct and/or indirect, the activities can be economic and/or non-economic, and the regulated party may be a public or private sector actor. |
| Tech Regulator | Government officials, departmental units and independent statutory authorities that are empowered to administer and enforce tech regulation, or more specifically to grant approvals (including registration and licensing), monitor compliance and enforce regulations. |



2. Country Overviews

The country overviews present the evolving roles of tech regulators, starting with regulators charged with the common mandates of competition and consumer protection, personal data protection and cybersecurity. The overviews conclude with regulators focused on specific sectors or industries.

➤ INDONESIA COMPETITION COMMISSION (Komisi Pengawas Persaingan Usaha; abbreviated as “KPPU”)

Institutional Form: Independent agency

Responsible Minister: N.A given independence. KPPU executive leadership consists of nine Commissioners, including Chairman and Vice Chairman. They are elected by the Parliament with recommendation from the President for a five-year term.

Principal Instrument(s): Law Number 5 Year 1999 Concerning The Prohibition of Monopolistic Practices and Unfair Business Competition

Mandate: KPPU has three main tasks from the competition law. It enforces the law, provides advice on competition policy and reviews mergers and acquisitions. KPPU also has the power to undertake market studies and review government policies to determine whether they are consistent with fair competition. Under Law Number 20 of 2008, in conjunction with Government Regulation Number 7 of 2021, KPPU has the authority to oversee and enforce the law concerning partnerships between large enterprises and Micro, Small, and Medium Enterprises (MSME).

Major Reports, Inquiries and Related Initiatives:

- Digital Platform Regulation (2019)
- The Digital Economy in Indonesia (2017)
- Official Textbook on Competition Law, Second Edition (2017)
- Regulation of The Supreme Court of The Republic of Indonesia Number 3 Year 2021
- Law Number 57 Year 2010 Concerning Merger or Consolidation of Business Entities and Acquisition of Shares of Companies which may cause Monopolistic Practices and Unfair Business Competition
- Law Number 4 Year 2019 Regarding Procedures for the Supervision and Handling of Partnership Cases
- Commission Regulation Number 1 Year 2019 regarding Case Handling Procedures
- Commission Regulation Number 3 Year 2019 on Review of Merger or Consolidation of Business Entities and Acquisition of Shares of Companies

MINISTRY OF TRADE (Kementerian Perdagangan)

Institutional Form: Government ministry

Responsible Minister: Minister of Trade

Principal Instrument(s): Regulation No. 50 of 2020 on Provisions on Business Licensing, Advertising, Guidance, and Supervision of Businesses in Trade Through Electronic System, Government Regulation No. 80 of 2019 on Trade Through Electronic System, Law No. 7 of 2014 on Trade

Mandate: The Ministry of Trade directs the formulation of policies related to development of trade in Indonesia, which encompass the following areas:

- Formulation, establishment, and implementation of policies in the areas of domestic trade strengthening and development, consumer protection and trade order, foreign trade, enhancement of market access for goods and services in international forums, national export development, as well as the development, nurturing, and supervision of commodity futures trading, warehouse receipt systems, and commodity auction markets.
- Coordination of task implementation, nurturing, and administrative support to all organisational elements within the Ministry of Trade.
- Management of state-owned goods or assets that fall under the responsibility of the Ministry of Trade.
- Oversight of task implementation within the scope of the Ministry of Trade.
- Execution of technical guidance and supervision regarding policy implementation in the fields of domestic trade strengthening and development, consumer protection and trade order, foreign trade, national export development, nurturing warehouse receipt systems, and commodity auction markets.
- Provision of substantive support to all elements within the Ministry of Trade.

Major Reports, Inquiries and Related Initiatives:

- Annual Report 2022
- Ministry of Trade User Goods Report 2022
- Ministry of Trade Performance Report 2022
- Secretariat General Performance Report 2022

MINISTRY OF COMMUNICATION AND INFORMATICS (Kementerian Komunikasi dan Informatika; abbreviated as “Kominfo”)

Institutional Form: Government ministry

Responsible Minister: Minister of Communication and Informatics

Principal Instrument(s): Law No. 11 of 2008 on Electronic Information and Transactions (“ITE Law”) as amended with Law No. 19 of 2016 on the Amended of Law No. 11 of 2008 on Electronic Information and Transaction (“ITE Law Amendment”); Government Regulation No. 82 of 2012 on Electronic System and Transaction Operation and its implementing legislation, Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in an Electronic System; Minister of Communication and Informatics Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions; Law 27 of 2022 on Personal Data Protection; Regulation No. 5 of 2020 on Electronic System Organizers (ESO) in the Private Sector;

Mandate: Kominfo is responsible for communication, information affairs and internet censorship. Its responsibilities include policy formulation for resource and telecommunications management, informatics devices, postal and informatics services, and administration of public information and communication. Kominfo is also tasked with implementing and supervising policies in these areas, providing technical guidance, conducting research and development in communication and informatics, and offering substantive support to organisational elements within the ministry.

Major Reports, Inquiries and Related Initiatives:

- Annual Report 2022
- Performance Report 2022
- Public Service Survey Results Report 2020
- Public Information Services Report 2019

INDONESIAN FINANCIAL SERVICES AUTHORITY (Otoritas Jasa Keuangan; abbreviated as “OJK”)

Institutional Form: Independent government agency

Responsible Minister: OJK leadership consists of a Board of Commissioners appointed by Presidential Decree.

Principal Instrument(s): Law of the Republic of Indonesia Number 21 of 2011 on Financial Services Authority

Mandate: The Financial Services Authority (OJK) is mandated to ensure that all activities within the financial services sector are conducted in an orderly, fair, transparent, and accountable manner. It aims to create a financial system that grows sustainably and remains stable while protecting the interests of consumers and the public. OJK is responsible for implementing an integrated regulatory and supervisory system for all activities within the financial services sector, including supervising the financial services activities in the Banking sector, the Capital Market sector, and the Non-Bank Financial Industry (IKNB) sector.

Major Reports, Inquiries, and Related Initiatives:

- [Explanation about OJK Regulation on Consumer Protection in Financial Services Sector \(2012\)](#)
- [OJK Regulation on Consumer Protection in Financial Services Sector \(2012\)](#)
- [Securities brokerage is regulated under OJK Regulation No. 20/POJK.04/2016 on the Licensing of Securities Companies That Conduct Business Activities as Underwriters and Securities Brokers \(“POJK 20/2016”\)](#)
- [Crypto trading is regulated under Bappebti Regulation No. 8 of 2021 on Guidelines for the Implementation of Physical Market of Crypto Assets in Futures Exchange \(“Bappebti Regulation 8/2021”\)](#)
- [Equity crowdfunding operation is regulated under OJK Regulation No. 57/POJK.04/2020 on Securities Offering Through Information Technology-Based Crowdfunding Service, as amended by OJK Regulation No. 16/POJK.04/2021 \(“POJK 57/2020”\)](#)
- [P2P Lending is regulated under OJK Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending Services \(“POJK 77/2016”\)](#)
- [Digital banks are regulated under POJK 12/2021](#)
- [Aggregator activities are regulated under OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovation in the Financial Services Sector \(“POJK 13/2018”\)](#)
- [Digital Finance Innovation Road Map and Action Plan 2020-2024](#)

BANK INDONESIA

Institutional Form: Independent state institution

Responsible Minister: Bank Indonesia is led by its board of governors. The governor and senior deputy governor are nominated and appointed by the President, with approval from the House of Representatives.

Principal Instrument(s): [Act of the Republic of Indonesia Number 23 of 1999 Concerning Bank Indonesia](#), [Act of the Republic of Indonesia Number 7 of 1992 Concerning Banking as Amended by Act Number 10 of 1998](#), [Law of the Republic of Indonesia Number 15 Year 2002 Concerning the Crime of Money Laundering](#), [Law of Republic of Indonesia Number 24 Year 2004 Concerning Deposit Insurance Corporation](#), [Act of the Republic of Indonesia Number 3 of 2004 Concerning Amendment to Act of the Republic of Indonesia Number 23 of 1999 Concerning Bank Indonesia](#), [Act of the Republic of Indonesia Number 21 of 2008 Concerning Sharia \(Islamic\) Banking](#), [Act of the Republic of Indonesia Number 6 of 2009 Concerning Stipulation of Government Regulation in lieu of Act Number 2 of 2008 Concerning Second Amendment to the Act Number 23 of 1999 Concerning Bank Indonesia](#), [Act of the Republic of Indonesia Number 3 of 2011 Concerning Funds Transfer](#)

Mandate: Bank Indonesia carries a three-fold responsibility as monetary, regulatory and supervisory authority for banking and payment systems. As such, Bank Indonesia’s most important task is not only to safeguard monetary stability, but also financial system stability. [To achieve and maintain the stability of the Indonesian rupiah, Bank Indonesia manages the fields of Monetary, Payment Systems, and Financial System Stability.](#) [The management of these three areas is implemented through policies issued by Bank Indonesia and operated using various instruments relevant to each respective field.](#)

Major Reports, Inquiries, and Related Initiatives:

- Payment Service Providers (PJPs) are regulated under Bank Indonesia regulation No. 23/6/PBI/2021 on Payment Service Providers (“BI Regulation 23/2021”)

➤ NATIONAL CYBER AND CRYPTO AGENCY
(Badan Siber dan Sandi Negara; abbreviated as “BSSN”)

Institutional Form: Ministerial-level agency

Responsible Minister: Coordinating Minister for Political, Legal and Security Affairs

Principal Instrument(s): Presidential Decree No. 53 of 2017, Presidential Decree No 28 of 2021.

Mandate: BSSN is an agency of the government of Indonesia that mandates the implementation and consolidation of Indonesian cybersecurity and encryption elements.

Major Reports, Inquiries and Related Initiatives:

- Annual Monitoring Report 2021
- Security Guidance for Your Small Business
- Handle DOS Attack for Small and Medium Businesses
- Data Breach Incident Handling
- Beware of Ransomware Attack

➔ MALAYSIA COMPETITION COMMISSION (MyCC)

Institutional Form: Government agency

Responsible Minister: Minister of Domestic Trade and Costs of Living

Principal Instrument(s): Competition Commission Act (2010), Competition Act (2010)

Mandate: MyCC's main role is to protect the competitive process for the benefit of businesses, consumers and the economy. It carries out functions, such as to implement and enforce the provisions of the Competition Act 2010, issue guidelines in relation to the implementation and enforcement of the competition laws, act as an advocate for competition matters, carry out general studies in relation to issues connected with competition in the Malaysian economy or particular sectors of the Malaysian economy, and inform and educate the public regarding the ways in which competition may benefit consumers and the economy of Malaysia.

Major Reports, Inquiries, and Related Initiatives:

- Strategic Plan 2021-2025
- Handbook for General Public Competition Act 2010

➔ MINISTRY OF DOMESTIC TRADE AND COSTS OF LIVING (KPDN)

Institutional Form: Government ministry

Responsible Minister: Minister of Domestic Trade and Costs of Living

Principal Instrument(s): Consumer Protection Act 1999, Consumer Protection (Electronic Trade Transactions) Regulations 2012, Supply Control (Amendment) Act 2015, Hire Purchase (Amendment) Act 2010, Weights and Measures (Amendment) Act 2017, Direct Selling and Anti-Pyramid Schemes Act 1993, Consumer Protection (Amendment) Act 2017, Optical Disc Act 2000 (act 606), Trade Description (Amendment) Act 2022, Price Control and Anti-Profiteering (Amendment) Act 2017, Companies Act 2016, Interest Schemes Act 2016, Business Registration (Amendment) Act 2015, Trade Marks Act 2019, Patents (Amendment) Act 2022, Integrated Circuit Layout Design Act of 2000, Copyright (Amendment) Act 2022, Geographical Indications Act 2022, Malaysian Intellectual Property Corporation (Amendment) Act 2018, Trade Descriptions (Definition of Halal) Order 2011

Mandate: The Ministry of Domestic Trade and Costs of Living (KPDN) formulates policies, strategies and reviews matters pertaining to the development of domestic trade which is inclusive of regulating matters pertaining to companies and businesses (based on related acts) as well as administering the intellectual property protection system. The Ministry is organised by domestic trade development and consumer empowerment; and also includes agencies such as the Intellectual Property Organisation Malaysia (MyIPO) and MyCC.

Major Reports, Inquiries, and Related Initiatives:

- [Guidelines for Foreign Participation in Distributive Trade Services in Malaysia \(Amendment\) 2020](#)
- [National Intellectual Property Policy](#)
- [Fair Trade Practices Policy](#)
- [National Consumer Policy](#)
- [Client Charter Performance Report \(January 2023\)](#)
- [Guidelines In Conducting Electronic Transactions For Consumers June 2016 \(BM document\)](#)

MINISTRY OF DIGITAL

Institutional Form: Government ministry

Responsible Minister: Minister of Digital

Principal Instrument(s): Pending (as of January 2024)

Mandate: The Ministry of Digital was announced in December 2023, separating from its preceding agency, the Ministry of Communications and Digital. The Ministry of Digital guides and supervises Malaysia's initiatives related to digitalisation and digital transformation on a national scale.

Prior to the establishment of the Ministry of Digital, the Malaysian Communications and Multimedia Commission regulates the communications and multimedia industry in Malaysia, particularly to govern the private players in Malaysia's communications and multimedia industry. The Commission led technology adoption objectives aimed at establishing Malaysia as a hub for communications and multimedia information and content services while regulating through the [Act 588](#) as a core instrument.

Major Reports, Inquiries and Related Initiatives:

Pending clear guidelines on specific mandate and regulatory areas (as of January 2024). For existing information, please refer to the Ministry of Communications [page](#).

MALAYSIAN PERSONAL DATA PROTECTION DEPARTMENT (PDPD)

Institutional Form: Government agency

Responsible Minister: Minister of Communications and Digital Malaysia

Principal Instrument(s): Personal Data Protection Act (2010)

Mandate: PDPC's role is to enforce and regulate personal data protection in Malaysia. The Personal Data Protection Act (PDPA) focuses on processing personal data in commercial transactions and avoiding any misuse of personal data.

Major Reports, Inquiries, and Related Initiatives:

- The Personal Data Protection Code of Practice For Licences Under the Communications and Multimedia Act 1998
- The Personal Data Protection Code of Practice For The Banking and Financial Sector

BANK NEGARA MALAYSIA (BNM)

Institutional Form: Statutory body

Responsible Minister: Independent

Principal Instrument(s): Central Bank of Malaysia Act (2009), Financial Services Act (2013), Islamic Financial Services Act (2013), Insurance Act (1996), Development Financial Institutions Act (2002), Money Services Business Act (2011), Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act (2001), Currency Act (2020)

Mandate: The role of BNM is to promote monetary and financial stability. This is aimed at providing a conducive environment for the sustainable growth of the Malaysian economy. Bank Negara Malaysia has played a significant developmental role in developing the financial system infrastructure in advancing the financial inclusion agenda. This is to ensure all economic sectors and segments of the society have access to financial services. The roles of the Bank are supported by 39 departments/units covering the following seven functional areas.

Major Reports, Inquiries, and Related Initiatives:

- Cloud Technology Risk Assessment Guideline (CTRAG) - Appendix to Risk Management in Technology (RMiT) Policy Document (2022)
- Management of Customer Information and Permitted Disclosures (2021)
- Licensing Framework for Digital Banks (2020)
- Electronic Know-Your-Customer (e-KYC) (2020)
- Risk Management in Technology (RMiT) (2020)
- Publishing Open Data using Open API (2019)
- Payment Cards Framework (2022)

MINISTRY OF HEALTH MALAYSIA

Institutional Form: Government ministry

Responsible Minister: Minister of Health

Principle Instrument: [Telemedicine Act 1997](#), [Poisons Act 1952](#)

Mandate: Malaysia's Ministry of Health oversees regulations in Malaysia related to health, which includes delivering health-related services online (telemedicine) or dispensing medication. The Ministry's Pharmacy Enforcement Division has issued notices to e-commerce platforms demanding the removal of links that advertise illegal pharmaceutical products, inclusive of those that may be counterfeit.

Major Reports, Inquiries and Related Initiatives:

- [Action Plan Towards The Elimination of Cervical Cancer in Malaysia 2021 - 2030](#)
- [National Strategic Plan for Ending AIDS 2016 - 2030](#)
- [Health Facts 2022](#)
- [Health Indicators 2022](#)
- [Health White Paper for Malaysia](#)
- [Strategic Plan 2021 - 2025](#)
- [Yearly Report 2021](#)

NATIONAL CYBER SECURITY AGENCY

Institutional form: Government agency

Responsible Minister: Prime Minister's Department

Principle instrument: [National Security Council Directive No.26](#), [Cyber Security Bill \(drafted\)](#)

Mandate: NACSA was established under the National Security Council to coordinate and develop cyber security policies that would strengthen Malaysia's resilience, which includes national-level policies and strategies. The addition of the digital economy as a critical national information infrastructure in Malaysia's National Cyber Security Strategy, places the digital economy sector among ten other sectors as a priority for protection by NACSA.

Major Reports, Inquiries, and Related Initiatives:

- [Malaysia National Cyber Security Strategy 2020-2024](#)

COMMERCIAL CRIME INVESTIGATION DEPARTMENT

Institutional Form: Enforcement body

Responsible Minister: Royal Malaysia Police

Principle Instrument: Police Act 1967, Moneylenders Act 1951, Criminal Procedure Code, Computer Crimes Act 1997, Anti-Money Laundering and Anti-Terrorism Financing Act 2001, Communications and Multimedia Act 1998

Mandate: The Commercial Crimes Department has investigative divisions such as those for Computer, Internet and Intellectual Property Crimes Investigation, the Police Cyber Investigation and Response Center, as well as the Telecommunication Crime Investigative Division. The purview of governance covers misinformation, fraud, scams, cyber-enabled crime as well as intellectual property.

Major Reports, Inquiries and Related Initiatives:

- Electronic Service for Verification

➤ PHILIPPINE COMPETITION COMMISSION (PCC)

Institutional Form: Government agency

Responsible Minister: Chairperson of the Commission

Principal Instrument(s): [Philippines Competition Act \(2015\)](#)

Mandate: The PCC was established as the country's competition authority to implement the national competition policy while attaining the objectives and purposes of the Act. Aside from the PCC, the Office for Competition (OFC), which is under the Department of Justice, is also responsible for the enforcement of the Act by conducting preliminary investigation and undertaking prosecution of all criminal offences arising under the Philippine Competition Act and other competition-related laws. The OFC organises and allocates resources as may be required therefore to effectively pursue such a mandate.

Major Reports, Inquiries, and Related Initiatives:

- [Philippine Competition Commission Annual Report 2022](#)
- [Implementing Rules and Regulations \(IRR\) of the Philippine Competition Act](#)

➤ DEPARTMENT OF TRADE AND INDUSTRY (DTI)

Institutional Form: Government agency

Responsible Minister: Secretary of Trade and Industry

Principal Instrument(s): [Executive Order No. 133, s. 1987](#)

Mandate: DTI is a prime mover of consumer welfare. It is committed to protecting the rights and interests of the consumers and is also committed to developing policies and programs aimed at sustaining the growth and development of the Philippine economy. Besides overseeing the effective implementation and enforcement of trade regulation and fair trade laws, the DTI provides protection for consumers through consumer education and information dissemination programs.

Major Reports, Inquiries, and Related Initiatives:

- [DTI Compendium of Laws and Policies](#)
- [Philippine e-Commerce Roadmap 2022](#)

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT)

Institutional Form: Government agency

Responsible Minister: Secretary of Information and Communications Technology

Principal Instrument(s): [Republic Act No. 10844 \(2016\)](#)

Mandate: DICT is the primary policy, planning, coordinating, implementing and administrative entity of the Executive Branch of the government. It plans, develops and promotes the national ICT development agenda.

Major Reports, Inquiries, and Related Initiatives:

- [E-Government Masterplan 2022](#)
- [National Broadband Plan](#)
- [National Cybersecurity Plan 2022](#)
- [National Competency Standard for e-Center Knowledge Workers](#)

NATIONAL PRIVACY COMMISSION (NPC)

Institutional Form: Independent body attached to the Department of Information and Communication Technology for policy coordination purposes

Responsible Minister: Privacy Commissioner

Principal Instrument(s): [Republic Act No. 10173 \(2012\)](#)

Mandate: NPC is the country's privacy watchdog. It is an independent body mandated to administer and implement the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection.

Major Reports, Inquiries, and Related Initiatives:

- [NPC Advisories and Circulars \(2023\)](#)
- [NPC Privacy Toolkit \(Third Edition\), 2018](#)

NATIONAL TELECOMMUNICATIONS COMMISSION (NTC)

Institutional Form: Government agency attached under the Department of Information and Communications Technology

Responsible Minister: NTC Commissioner

Principal Instrument(s): [Republic Act No. 10844 \(2016\)](#)

Mandate: The National Telecommunications Commission (NTC) is primarily responsible for the regulation and quasi-judicial functions relative to the supervision, adjudication and control of the country's radio communications, telecommunications and broadcast, including cable television (CATV) facilities and services throughout the Philippines.

Major Reports, Inquiries, and Related Initiatives:

- [NTC Annual Report 2020](#)

BANGKO SENTRAL NG PILIPINAS (BSP)

Institutional Form: Independent monetary authority

Responsible Minister: Governor of the Bangko Sentral ng Pilipinas

Principal Instrument(s): Republic Act No. 7653 (1993),

Mandate: BSP is the central bank of the Republic of the Philippines. The BSP took over from the Central Bank of Philippines, which was established on 3 January 1949, as the country's central monetary authority. The BSP enjoys fiscal and administrative autonomy from the National Government in the pursuit of its mandated responsibilities.

Major Reports, Inquiries, and Related Initiatives:

- BSP Annual Report 2022
- BSP Digital Payments Transformation Roadmap 2020-2023

CYBERCRIME INVESTIGATION AND COORDINATING CENTER (CICC)

Institutional Form: Government agency attached to the Department of Information and Communications Technology

Responsible Minister: Executive Director of the CICC

Principal Instrument(s): Republic Act 10175 (2012),

Mandate: CICC is responsible for all functions related to cybersecurity including the formulation of the Philippines National Cybersecurity Plan, establishment of the National Computer Emergency Response Team (CERT), and the facilitation of international cooperation on intelligence regarding cybersecurity matters.

Major Reports, Inquiries, and Related Initiatives:

- CICC Accomplishment Report September 2020 - September 2021

➤ COMPETITION AND CONSUMER COMMISSION OF SINGAPORE (CCCS)

Institutional Form: Statutory board

Responsible Minister: Minister for Trade and Industry

Principal Instrument(s): Competition Act (2004, amended 2020), Consumer Protection (Fair Trading) Act (2003, amended 2020)

Mandate: The CCCS is Singapore's competition regulator. It investigates and enforces against practices that have an adverse effect on competition and protects consumers against unfair trade practices in Singapore. The CCCS also advises the government and other public authorities on national needs and policies related to competition matters, and represents Singapore with respect to competition matters in the international arena.

Major Reports, Inquiries, and Related Initiatives:

- Competition Act (2004)
- Consumer Protection (Fair Trading) Act (2003)

➤ ENTERPRISE SINGAPORE (ESG)

Institutional Form: Statutory board

Responsible Minister: Minister for Trade and Industry

Principal Instrument(s): Enterprise Singapore Board Act (2018, amended 2020)

Mandate: Enterprise Singapore provides support for businesses in Singapore, as well as serving as the national standards and accreditation authority. It oversees the Singapore Standards Council (SSC), which is responsible for implementing the Singapore Standardisation Programme, governing industry standards in a range of key sectors, including biomedical and information technology. The SSC also comprises several Coordinating Committees that contribute to Singapore's Cybersecurity and Smart Nation Initiative.

Major Reports, Inquiries, and Related Initiatives:

- Singapore Standards

INTELLECTUAL PROPERTY OFFICE OF SINGAPORE (IPOS)

Institutional Form: Statutory board

Responsible Minister: Minister for Law

Principal Instrument(s): Intellectual Property Office of Singapore Act (2001, amended 2020), Intellectual Property (Amendment) Act (2022), Copyright Act (2021)

Mandate: The IPOS administers intellectual property rights in Singapore. Recent amendments to the Intellectual Property (Amendment) Act improved the intellectual property registration process. Specific to technology, the IPOS introduced the SG IP Fast Track Programme in 2020 to accelerate patent applications across technology fields within 6 months from filing. The IPOS is implementing its Singapore IP Strategy (SIPS) 2030, aiming to strengthen Singapore's position as a regional innovation hub and improve business and employment opportunities.

Major Reports, Inquiries, and Related Initiatives:

- Singapore IP Strategy 2030
- Intellectual Property (Amendment) Act (2022)
- Copyright Act (2021)

SINGAPORE CUSTOMS

Institutional Form: Government department

Responsible Minister: Minister for Finance

Principal Instrument(s): Customs Act (1960), Trade Marks Act (1998), Geographical Indications Act (2014), Copyright Act (2021), Strategic Goods (Control) Act (2002)

Mandate: Singapore Customs is primarily responsible for trade facilitation and revenue enforcement. Its duties include the border enforcement of intellectual property rights, as well as regulating and controlling the transfer and brokering of dual-use technologies under the Strategic Goods (Control) Act, such as computers designed for information security functions like cryptography. The Strategic Goods (Control) Regulations support the implementation of the Act, including permit procedures for legitimate activities and the conditions for approval, revocation or suspension of permits.

Major Reports, Inquiries, and Related Initiatives:

- Strategic Goods (Control) Order (2023)
- Strategic Goods (Control) Regulations (2006)
- Strategic Goods (Control) Act (2002) (2020 Revised Edition)

MINISTRY OF COMMUNICATIONS AND INFORMATION

Institutional Form: Government ministry

Responsible Minister: Minister for Communications and Information

Principal Instrument(s): [Broadcasting Act \(1994, amended 2023\)](#), [Online Safety \(Miscellaneous Amendment\) Act 2022](#), [Public Entertainments Act \(1958, revised 2021\)](#)

Mandate: The Ministry of Communications and Information (MCI) oversees the development of the state's national library, national archives and public libraries; government's information and public communication policies; as well as media sectors and infocomm technology. MCI leads the development of Singapore's digital economy, digital readiness and inclusion, regulation of digital infrastructure and data, online regulation, and cyber security.

Major Reports, Inquiries, and Related Initiatives:

- [Digital Connectivity Blueprint \(2023\)](#)
- [Digital Media and Information Literacy Framework \(2019\)](#)
- [Digital Readiness Blueprint \(2018\)](#)

SMART NATION GROUP

Institutional Form: Agency part of the Prime Minister's Office and administered by the Ministry of Communications and Information

Responsible Minister: Chairman of the Smart Nation and Digital Government Group Ministerial Committee (SNDGG)

Principal Instrument(s): N/A

Mandate: The Smart Nation Group is responsible for Singapore's digital transformation initiatives and leads the development of the country's Smart Nation strategies. The group oversees the development and application of digital technologies and capabilities across Singapore. In addition, the group promotes digital inclusivity, while regulating data and online activities, and strengthening digital security. The group was recently formed in October 2023 with the merger of SNDGG and MCI's digital development functions.

Major Reports, Inquiries, and Related Initiatives:

- [Digital Government Blueprint \(2018\) \(2020 Revised Edition\)](#)
- [Smart Nation: The Way Forward \(2018\)](#)

Institutional Form: Statutory board

Responsible Minister: Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): Protection from Online Falsehoods and Manipulation Act (2019), Info-Communications Media Development Authority Act (2016, amended 2020), Personal Data Protection Act (2012), Electronic Transactions Act (2010), Telecommunications Act (1999), Broadcasting Act (1994, amended 2023)

Mandate: The IMDA develops and regulates the infocomm and media sectors in a holistic way, through an emphasis on talent, research, innovation, and enterprise. As a statutory board in the Singapore government, it seeks to deepen regulatory capabilities for a converged infocomm media. As part of its mandate, IMDA enforces the Telecommunications Act that regulates the licensing of telecom systems and services and grants of spectrum rights, among other matters. It also enforces the Electronic Transactions Act (amended in 2021) that covers matters such as electronic records, signatures, and contracts. As part of its broader remit, the IMDA issued an updated Model Artificial Intelligence Governance Framework that provides guidance to private-sector organisations on ethical and governance issues when deploying artificial intelligence solutions. An Advisory Council on the Ethical Use of AI and Data was set up in 2018 to advise the Government on issues arising from commercial deployment of artificial intelligence that may require policy or regulatory intervention. Members comprise international industry leaders in artificial intelligence, advocates of social and consumer interests, and leaders of local companies who are keen to make use of artificial intelligence.

Major Reports, Inquiries, and Related Initiatives:

- Code of Practice for Online Safety (2023)
- National AI Strategy (2023)
- Broadcasting Act 1994, Part 10A [added by Act 38 of 2022 wef 01/02/2023]
- Electronic Transactions Act (2021)
- Model Artificial Intelligence Governance Framework (2020)
- Digital Economy Framework for Action (2018)
- Services and Digital Economy Technology Roadmap (2018)

INFOCOMM MEDIA DEVELOPMENT AUTHORITY, PERSONAL DATA PROTECTION COMMISSION (PDPC)

Institutional Form: Commission within a statutory board, the Infocomm Media Development Authority

Responsible Minister: Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): Info-Communications Media Development Authority Act (2016, amended 2020), Personal Data Protection Act (2012, amended 2020)

Mandate: The PDPC regulates the collection, use, disclosure, and protection of personal data used by organisations, including online personal data.

Major Reports, Inquiries, and Related Initiatives:

- Personal Data Protection Act (2012, amended 2020)

INFOCOMM MEDIA DEVELOPMENT AUTHORITY, PROTECTION FROM ONLINE FALSEHOODS AND MANIPULATION ACT OFFICE (POFMA)

Institutional Form: Office within a statutory board

Responsible Minister: Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): Protection from Online Falsehoods and Manipulation Act (2019)

Mandate: The POFMA is part of Singapore's whole-of-government approach to counter the proliferation of online falsehoods. The POFMA issued codes of practices to provide guidance to internet intermediaries and digital advertising intermediaries about systems and processes to prevent and counter the misuse of online accounts. The POFMA works to improve the transparency of political advertising and 'de-prioritise' online falsehoods by providing a list of prescribed intermediaries subject to the codes of practice.

Major Reports, Inquiries, and Related Initiatives:

- Code of Practice for Giving Prominence to Credible Online Sources of Information (2019)
- Code of Practice for Transparency of Online Political Advertisements (2019)
- Code of Practice for Preventing and Countering Abuse of Online Accounts (2019)
- Protection from Online Falsehoods and Manipulation Act (2019)

MONETARY AUTHORITY OF SINGAPORE (MAS)

Institutional Form: Statutory board

Responsible Minister: Minister for Finance

Principal Instrument(s): Monetary Authority of Singapore Act (1970)

Mandate: The MAS is Singapore's central bank and integrated financial regulator. Its key functions include issuing currency, monetary policy and supervision of financial services. In the digital space, it develops guidance on digital banking, digital and cryptocurrencies, and banking cyber security. The MAS issued an Internet Banking Framework in 2000, and an Eligibility Criteria and Requirements for Digital Banks in 2019. In 2016, the MAS launched a FinTech Regulatory Sandbox framework to encourage and enable experimentation of technology innovation to deliver financial products and services.

Major Reports, Inquiries, and Related Initiatives:

- FAQs on MAS FinTech Regulatory Sandbox Framework (2021)
- The Future of Money, Finance and the Internet – Speech by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Singapore FinTech Festival on 9 November 2021
- A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context (2021)
- Revised Technology Risk Management Guidelines (2021)
- Eligibility Criteria and Requirements for Digital Banks (2019)

HEALTH SCIENCES AUTHORITY (HSA)

Institutional Form: Statutory board

Responsible Minister: The Minister for Health

Principal Instrument(s): Health Products Act (2007)

Mandate: The HSA is responsible for the regulation of health products, issuing licences for medical devices to be produced or distributed in Singapore. Its mandate has been expanded to oversee emerging technologies in digital health, such as telemedicine and the use of artificial intelligence in healthcare, contributing to the Artificial Intelligence in Healthcare Guidelines (AIHGle – pronounced “agile”) in 2021.

Major Reports, Inquiries, and Related Initiatives:

- Artificial Intelligence in Healthcare Guidelines (2021)
- Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (2022)

SINGAPORE POLICE FORCE (SPF)

Institutional Form: Uniformed law enforcement agency

Responsible Minister: Minister for Home Affairs

Principal Instrument(s): [Foreign Interference \(Countermeasures\) Act \(2021\)](#), [Protection from Harassment Act \(2014, amended 2020\)](#), [Penal Code](#), [Computer Misuse Act \(1993, amended 2023\)](#)

Mandate: The SPF oversees Singapore's public law and order and law enforcement functions. It enforces relevant provisions of the Penal Code and the Computer Misuse Act, which criminalises unauthorised access or modification of computer material as well as other computer crimes. The SPF enforces the Protection from Harassment Act, which criminalises, among other things, cyber bullying, unlawful stalking and harassment within and outside of the workplace, and doxing. It also provides measures to address the spread of online falsehoods affecting people and established the Protection from Harassment Court (PHC). The SPF also enforces the Foreign Interference (Countermeasures) Act to prevent, detect, and disrupt the use of hostile information campaigns and local proxies by foreign entities that interfere in domestic politics, including using online technologies.

Major Reports, Inquiries, and Related Initiatives:

- [Foreign Interference \(Countermeasures\) Act \(2021\)](#)
- [Protection from Harassment Act \(2014\) \(2020 Revised Edition\)](#)
- [Computer Misuse Act \(1993\) \(2023 Revised Edition\)](#)

CYBER SECURITY AGENCY OF SINGAPORE (CSA)

Institutional Form: Government department

Responsible Minister: Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): [Cybersecurity Act \(2018\)](#)

Mandate: The CSA is responsible for cyber security strategy, operations, education, outreach and ecosystem development. The CSA administers the Cybersecurity Act and its chief executive serves as the Commissioner of Cybersecurity. Recent initiatives launched by the CSA as part of its mandate include the Singapore's Operational Technology Cybersecurity Masterplan 2019, the Cybersecurity Code of Practice for Critical Information Infrastructure and three certification schemes for providing security assurance for cyber security products, including the Cybersecurity Labelling Scheme for consumer smart devices.

Major Reports, Inquiries, and Related Initiatives:

- [Singapore Cybersecurity Landscape \(2022\)](#)
- [Cybersecurity Code of Practice for Critical Information Infrastructure \(2022\)](#)

TRADE COMPETITION COMMISSION OF THAILAND (TCCT)

Institutional Form: Independent administrative organisation

Responsible Minister: Minister of Commerce

Principal Instrument(s): Trade Competition Act B.R. 2560 (2017)

Mandate: TCCT, previously known as the Office of Trade Competition Commission (OTCC), is the competition regulator of Thailand. It serves as the primary mechanism in the supervision and enforcement of the Trade Competition Law. It is an independent regulatory agency with broader powers, including the authority to impose fines and penalties, and to approve or reject proposed mergers that could lead to a monopoly or undue market dominance against consumer interests. However, its authority does not extend to sectors with other regulatory laws in place such as telecommunications and energy.

Major Reports, Inquiries, and Related Initiatives:

- TCCT Guidelines on Merger, 26 September 2022
- TCCT Decision on unfair charges of advertising service on a delivery platform, 7 July 2022
- TCCT Decision on the deletion of shower soap product from online shopping platform, 21 April 2022
- TCCT Decision on the increase of commission fee in delivery platform, 3 March 2022
- TCCT Decision on the conditions of service in delivery platform that unfairly limit entrepreneur's rights, 27 January 2022
- TCCT Decision on the non-compete clause with a information technology service provider (research database), 24 February 2021
- TCCT Decision on the discriminatory trade conditions in delivery platform, 24 February 2021
- TCCT Decision on the deletion of the prohibited harmful products from online shopping platform, 14 October 2021

MINISTRY OF DIGITAL ECONOMY AND SOCIETY

Institutional Form: Government ministry

Responsible Minister: Minister of Digital Economy and Society

Principal Instrument(s): Royal Decree on Electronic Conferencing, B.E.2563 (2020), Digital Development for Economy and Society Act, B.E. 2560 (2017), Operation Protection Act of the Asia-Pacific Postal Union Headquarters B.E.2551 (2008), Operation Protection Act of the Asia-Pacific Space Cooperation Organisation, B.E. 2550 (2007), Postal Act, B.E. 2477 (1934), Radiocommunication Act, B.E. 2498 (1955), Computer Crime Act B.E. 2550 (2007), Statistic Act B.E. 2550 (2007), Digital Economy and Society Council of Thailand Act B.E. 2562 (2019), Electronic Transactions Development Agency Act B.E. 2562 (2019), Promotion and Development of the Quality of Life of Persons with Disabilities Act B.E. 2550 (2007), Cybersecurity Act B.E. 2562 (2019), Electronic Transaction Act B.E 2562 (2019)

Mandate: The Ministry of Digital Economy and Society was formerly known as the Ministry of Information and Communication Technology (MICT). The ministry assumed the responsibilities of MICT. It has broad mandates regarding digital development including telecommunication infrastructure, digital innovation promotion, integrated digital government and national statistics.

Major Reports, Inquiries, and Related Initiatives:

- Notification of the Council for Reform in the Democratic System with the King as Head of State No. 21 on the prohibition of wiretapping by telephone or any communication device (2006)
- Notification of the National Council for Peace and Order No. 26/2557 regarding the supervision and surveillance of the use of social media (2014)

ELECTRONIC TRANSACTION DEVELOPMENT AGENCY (ETDA)

Institutional Form: Public organisation

Responsible Minister: Minister of Digital Economy and Society

Principal Instrument(s): Electronic Transaction Act B.E 2562 (2019), Royal Decree on the Operation of Digital Platform Service Businesses that are Subject to Prior Notification, B.E. 2565 (2022), Royal Decree on the Regulation of Digital Identification and Authentication Service that Must be Licensed, B.E. 2565 (2022)

Mandate: ETDA has obligations to govern digital service businesses in order to create reliability and support the growth of digital economic and social activities, to promote and support electronic transactions and to cooperate with all sectors in order to push for integrated and connected electronic transactions. It became the regulator of digital ID business and digital platform service under the two royal decrees.

Major Reports, Inquiries, and Related Initiatives:

- Digital Platform Services regulation (assessment tools, registration guidelines, public hearing of subsidiary rules)
- Royal Decree on the Supervision of Regulated Digital Identification Authentication and Verification Service Businesses B.E. 2565 (2022)

SECURITIES AND EXCHANGE COMMISSION (SEC) OFFICE

Institutional Form: Independent administrative organisation

Responsible Minister: Minister of Finance

Principal Instrument(s): Emergency Decree on Digital Asset Businesses B.E. 2561

Mandate: SEC has mandates to supervise and to develop the Thai capital market by taking into consideration the changing dynamic and the involvement of SEC Board, Capital Market Supervisory Board, executives and employees of SEC as well as stakeholders in the capital market. SEC has issued the Emergency Decree on Digital Asset Businesses B.E. 2561 (2018) and related regulations to supervise fundraising, business operation and activities related to digital assets. It aims to respond to an increasing number of complaints and offences related to digital assets as well as other frauds and scams.

Major Reports, Inquiries, and Related Initiatives:

- Rules, guidelines and template in relation to digital asset business
- Summary of the Emergency Decree on Digital Asset Businesses B.E. 2561
- SEC Strategic Plan 2020 – 2022

NATIONAL BROADCAST AND TELECOMMUNICATION COMMISSION (NBTC) OFFICE

Institutional Form: Independent government organisation

Responsible Minister: Prime Minister

Principal Instrument(s): Act on the Organisation to Assign Radio frequency and to Regulate the Broadcasting and Telecommunications Services B.E. 2553 (2010)

Mandate: NBTC is the authority in spectrum management regarding licensing and regulating the broadcasting, television, radiocommunications, and telecommunications business operation.

Major Reports, Inquiries, and Related Initiatives:

- Notification of The National Broadcasting and Telecommunications Commission on the Second Broadcasting Master Plan B.E. 2563 – 2568 (2020 - 2025)
- Notification of the National Telecommunications Commission on Measures for Telecommunication Users' Rights to Privacy and Rights to Communicate through Telecommunication, 16 August 2550⁶

PERSONAL DATA PROTECTION COMMISSION (PDPC) OFFICE

Institutional Form: Independent administrative organisation

Responsible Minister: Minister of Digital Economy and Society

Principal Instrument(s): Personal Data Protection Act B.E. 2562 (2019) (PDPA)

Mandate: PDPC is responsible for planning the promotion and protection of personal data, prescribing guidelines and measures, and issuing various rules, codes and sub-regulations, among others. It appoints expert committees to consider complaints, investigate non-compliance and settle disputes. It has duties to provide advice and collaborate with other governmental agencies, especially those with the power to regulate personal data protection of specific sectors since PDPA adds new standards to apply together with their existing legislations.

Major Reports, Inquiries, and Related Initiatives:

- Notification of PDPC on Data Breach Notification, 6 December 2022
- Notification of PDPC on Record of Processing Activities, 20 June 2022
- Notification of PDPC on Exemption of Record of Processing Activities for SMEs, 20 June 2022
- Notification of PDPC on Security Measure, 20 June 2022
- Notification of PDPC on Administrative Fine imposed by Expert Committee, 20 June 2022
- Guidelines for Consent under PDPA
- Guidelines for Notice under PDPA
- PDPA Guide for Small Enterprises
- Guidelines for Risk Assessment and Data Breach Notification, 15 December 2022
- Practical Guide for Data Controller and Data Professor : Compilation of Answers to Requests for Consultation, 10 February 2023

BANK OF THAILAND (BOT)

Institutional Form: Independent administrative organisation

Responsible Minister: The Prime Minister

Principal Instrument(s): Financial Institutions Businesses Act, BE 2551 (2008)

Mandate: The BOT, which serves as Thailand's central bank, is responsible for a range of duties and obligations outlined in the Financial Institutions Businesses Act of 2008. Among these, the ones most pertinent to the field of fintech involve establishing or aiding in the creation of payment systems and electronic clearing systems, and overseeing the security and efficacy of such systems, which includes monitoring non-banking entities. This responsibility extends to areas such as e-payments, personal loans and nano finance businesses. Additionally, the BOT supervises, inspects and evaluates the financial status, performance and risk management protocols of financial institutions with the aim of promoting stability. This includes ensuring that traditional services like loans and deposits, as well as regulations governing e-banking and fintech used by both banks and non-banking entities, are in compliance.

Major Reports, Inquiries, and Related Initiatives:

- [Bank of Thailand Notification: No. SorNorChor. 16/2561, Re: Regulations, Procedures and Conditions on Application for License to Undertake Designated Payment Systems Business \(No. 2\)](#)
- [Payment System Act B.E 2560 \(2017\)](#)

 NATIONAL CYBER SECURITY COMMITTEE (NCSC) OFFICE

Institutional Form: Public organisation

Responsible Minister: Minister of Digital Economy and Society

Principal Instrument(s): [Cyber Security Act B.E. 2562 \(2019\)](#)

Mandate: NCSC has mandates to defend and address cyber threats, especially those related to the critical information infrastructures. It aims to become the centre of coordination for cybersecurity among governmental and private organisations.

Major Reports, Inquiries, and Related Initiatives:

- [Notification of NCSC on Cyberthreats Notification, 9 May 2023](#)
- [Website Security Guidelines](#)
- [Suggestions on Criteria of Critical Information Infrastructure](#)
- [Suggestions on Notification of Computer's Owner, Computer's Possessor and Computer System Administrator](#)
- [Suggestions on Cybersecurity Risk Assessment and Cybersecurity Inspection for Critical Information Infrastructure](#)

VIETNAM NATIONAL COMPETITION COMMISSION

Institutional Form: Government agency

Responsible Minister: Ministry of Industry and Trade

Principal Instrument(s): Vietnam Competition Law No. 23/2018/QH14,

Mandate: The Vietnam National Competition Commission is the only agency to enforce the Competition Law, with the function of adjudicating anti-competition practices and unfair competition cases. Exemption of anti-competitive agreements and deciding on whether economic concentration cases fall within the prohibited category.

Major Reports, Inquiries, and Related Initiatives:

- Decree No. 75/2019/ND-CP prescribing penalties for administrative violations against regulations on competition
- Decree No. 35/2020/ND-CP on detailed regulations of some provision of the Competition Law
- Law No. 59/2010/QH12 of the National Assembly on Protection of Consumer Rights
- Decree No. 99/2011/ND-CP of the Government detailing and guiding a number of articles of the Law on Protection of Consumer Rights

MINISTRY OF PLANNING AND INVESTMENT (MPI)

Institutional Form: Government ministry

Responsible Minister: Minister of Planning and Investment

Principal Instrument(s): Law No. 61/2020/QH14 on Investment

Mandate: The Ministry of Planning and Investment (MPI) is an agency of the Government, performing the state management of socio-economic development strategies and plans; domestic investment, foreign investment in Vietnam; development of enterprises; and state management of public services under the management of MPI. (Decree 89/2022/ND-CP)

Major Reports, Inquiries, and Related Initiatives:

- Decision No. 2289/QĐ-TTg dated December 31, 2020 of the Prime Minister promulgating the National Strategy on the Fourth Industrial Revolution to 2030
- Program on Digital Transformation for Businesses

MINISTRY OF INDUSTRY AND TRADE (MoIT)

Institutional Form: Government ministry

Responsible Minister: Minister of Industry and Trade

Principal Instrument(s):

- [Law No. 23/2018/QH14 on Competition](#)
- [Law No. 05/2017/QH14 on Foreign trade management](#)
- [Law No. 59/2010/QH12 on Protection of Consumer Rights](#)
- [Law No. 36/2005/QH11 on Commerce](#)
- [Decree No. 09/2018/ND-CP on guidelines for the law on commerce and the law on foreign trade management regarding exchange of goods and other activities directly related to exchange of goods of foreign investors and foreign-invested business entities in Vietnam](#)
- [Decree No. 52/2013/ND-CP dated May 16, 2013 on e-commerce](#)
- [Decree No. 85/2021/ND-CP amending and supplementing a number of articles of Decree No. 52/2013/ND-CP](#)
- [Law No.51/2005/QH11 on e-transaction](#)
- [Law No.36/2005/QH11 on commercial, Law No.61/2020/QH14 on investment \(“Law on Investment”\)](#)
- [Decree 52/2013/ND-CP on e-commerce, as amended by Decree 85/2021/ND-CP,](#)
- [Decree 09/2018/ND-CP \(“Decree 09”\)](#)

Mandate: The Ministry of Industry and Trade (MoIT) is an agency of the Government, performing the state management of industry and commerce, including the following sectors: high-tech industry (excluding information technology industry); domestic trade; import and export, border trade; e-commerce; competition, protection of consumer rights;... and state management of public services under the management of MoIT. (Decree 96/2022/ND-CP) MoIT is responsible for the advancement, promotion, governance, regulation, management and growth of the industry and trade. MoIT is the main governmental body that is responsible for e-commerce matters.

Major Reports, Inquiries, and Related Initiatives:

- [Vietnam Import-Export Report](#)
- [Developing the UK Market for the Textile and Garment Industry](#)
- [Implementing Rules of Origin in CPTPP – 3 Years Journey from the Effective Date of the Agreement](#)

MINISTRY OF INFORMATION AND COMMUNICATIONS (MIC)

Institutional Form: Government ministry

Responsible Minister: Minister of Information and Communications

Principal Instrument(s): [Law No. 20/2023/QH15 on E-transactions, Law No. 86/2015/QH13 on cyberinformation security, Law No. 41/2009/QH12 on telecommunications, Decree 25/2011/ND-CP on promulgating in detail some articles of telecommunications law, Law No. 67/2006/QH11 on information technology, Decree No. 85/2016/ND-CP on the security of information systems by classification](#)

Mandate: MIC is an agency of the Government, performing the function of state management of the press; publication; electronic information; telecommunication; information technology industry; IT applications; cyberinformation security; E-transactions; national digital transformation, etc. (Decree No. 48/2022/ND-CP).

Major Reports, Inquiries, and Related Initiatives:

- Decision No. 749/QD-TTg on approving Program on National digital transformation by 2025, towards 2030
- Decision No. 1619/QD-TTg on strengthening and renaming the national committee on E-government.
- Decision No. 24/QD-UBQGCDs, dated March 3, 2022, on operating regulations of the National Committee on digital transformation.
- Decree No. 15/2020/ND-CP on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and e-transactions

STATE BANK OF VIETNAM (SBV)

Institutional Form: Government ministry

Responsible Minister: Governor of the State Bank of Vietnam

Principal Instrument(s): Decree No. 101/2012/ND-CP dated November 22, 2012 of the Government on non-cash payment (amended and supplemented in Decree No. 80/2016/ND-CP dated June 1, 2016 and Decree No. 16/2019/ND-CP dated February 1, 2019), Decision 316/QD-TTg dated March 9, 2021 approving the pilot implementation of telecommunications accounts for payment of small value commodities and services (Mobile-Money), SBV - Decree 101/2012/ND-CP, Circular 39/2014/TT-NHNN, Official Letter No. 5228/NHNN/CSTT, Decree 101/2012/ND-CP, Official Letter No. 5747/2017/NHNN-PC

Mandate: SBV is a ministerial-level agency of the Government, the Central Bank of Vietnam; performing the function of state management of currency, banking activities and foreign exchange; performing the functions of the Central Bank in terms of money issuance, bank of credit institutions and provision of monetary services to the Government; state management of public services under the management of the State Bank SBV regulates banks and other credit institutions (i.e., finance companies, financial leasing companies, other non-bank credit institutions, microfinance institutions and People's Credit Funds). The SBV, through its headquarters in Hanoi and a network of provincial branches, performs the traditional role of a central bank and regulates the banking system in Vietnam, meaning it is in charge of granting licences for the establishment and operation of banks in Vietnam, issuing guidance for banking activities and supervising the banking system. (Decree No. 102/2022/ND-CP)

Major Reports, Inquiries, and Related Initiatives:

- Decision No. 149/QD-TTg dated January 22, 2020 of the Prime Minister approving the National Comprehensive Financial Strategy to 2025, with orientation to 2030
- Decision No. 1813/QD-TTg dated October 28, 2021 of the Prime Minister approving the project of developing non-cash payment in Vietnam for the period of 2021-2025.
- Resolution No. 100/NQ-CP dated September 6, 2021 of the Government approving the Proposal on drafting a Decree on Sandbox for Fintech activities in the banking sector.

MINISTRY OF PUBLIC SECURITY (MPS)

Institutional Form: Government ministry

Responsible Minister: Minister of Public Security

Principal Instrument(s): Law No. 24/2018/QH14 on Cyber Security, Law No. 86/2015/QH13, Law No. 35/2018/QH14 on Network Information Security Decree, No. 53/2022/ND-CP on Regulating in details some articles of the cybersecurity law, Decree No. 13/2023/ND-CP on the Protection of Personal Data, Law No. 67/2006/QH11, Law No. 21/2017/QH14 on Information Technology, Law No. 51/2005/QH11 on E-transactions, Law No. 59/2010/QH12, Law No.35/2018/QH14 on Protection of Consumers' Rights, Decree No. 13/2023/ND on the Protection of Personal Data

Mandate: MPS is a government agency responsible for ensuring public security and social order, national security and safety in Vietnam. The main functions of the MPS include maintaining security and order, preventing and combating crimes, protecting national security, managing immigration and border control, and ensuring safety for the public. The MPS also has several specialised agencies and departments, such as the Criminal Police Department, the Immigration Department and the Cyber Security Department, among others, which are responsible for specific areas of security and law enforcement, and state management of public services under the management of MPS. (Decree No. 01/2018/ND-CP).

Major Reports, Inquiries, and Related Initiatives:

- Decision 964/QD-TTg, dated August 10, 2022 of the Prime Minister approving the National Cybersecurity Strategy, proactively responding to challenges from cyberspace to 2025, with a vision to 2030.
- Decree No. 85/2016/ND-CP on the security of information systems by classification
- Decree No. 72/2013/ND-CP, Decree No. 27/2018/ND-CP, Decree No.150/2018/ND-CP of the Government, on management, provision and use of Internet services and online information
- Decree No. 15/2020/ND-CP on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions
- Decree No. 53/2022/ND-CP on Cyber Security (Prepared by MPS in coordination with other relevant ministries, ministerial-level agencies and bodies)



3. Regulatory Trends in Southeast Asia's Digital Economy

While the SEA-6 governments share some common goals in regulating their tech ecosystems, the country overviews demonstrate the diversity of approaches to regulating the rapidly changing landscape of the digital economy.

- **Preserving competition for innovation while protecting consumers and small businesses.** The Competition Commissions in SEA-6 have been charged with ensuring healthy, competitive markets. Market stability, however, often involves other specialist agencies. An example of this would be where regulatory authorities, such as the financial services authorities and central banks are entrusted with overseeing cryptocurrencies. In Malaysia, commercial activity in specific industries is regulated separately, namely communications, media, energy and aviation. The Malaysian Competition Act 2010 does not apply to commercial activity in these industries, which are governed by separate legislation such as the Communications and Multimedia Act 1998, Energy Commission Act 2001, Petroleum Development Act 1974 and Malaysian Aviation Commission Act 2015, respectively.
- **Protecting personal data to foster trust.** A law that governs the protection of personal data sets a minimum standard for safeguarding information about an individual who can be identified from that data or from other information accessible to a data controller or processor. This law includes a range of requirements related to the collection, use, disclosure and handling of personal data within a country. All SEA-6 countries have enacted laws to protect the data of their citizens, but not all have established separate agencies to implement these policies.

- **Enhancing cybersecurity.** Cybersecurity laws and codes have been implemented across SEA-6. The SEA-6 countries have a legal framework to create a cybersecurity plan to protect key national infrastructure. While Indonesia, Malaysia, Philippines and Singapore have specialist agencies overseeing cybersecurity, the Vietnamese Ministry of Public Security leads cybersecurity efforts under a broader remit of security. In Thailand, regulators vary by sector. For example, the Bank of Thailand regulates financial institutions and e-payment service providers, the Securities and Exchange Commission of Thailand regulates securities companies, and the National Broadcasting and Telecommunications Commission regulates telecommunication service companies.

Other common trends include the expansion of mandates for existing regulators and the emergence of new agencies.

3.1 Existing regulators are seeing their roles expand

The most obvious trend seen in this review of tech regulators across SEA-6 is the expansion of roles of existing regulators. Specific areas of the e-commerce legislation, for example, fall under the purview of the Ministry of Trade in Indonesia, Ministry of Domestic Trade and Cost of Living (KPDN)⁷ in Malaysia, the Department of Trade and Industry in the Philippines, and the Ministry of Industry and Trade in Vietnam. The expansion of roles for e-commerce regulators is a response to an evolution of the way commercial transactions are conducted — from traditional brick and mortar stores using cash transactions, to electronic transactions on the internet. As e-commerce grew in popularity, so did concerns about consumer protection, privacy and security.

Legislative changes to support effective regulation take time, since several laws may need to be updated or introduced. In Malaysia, for example, the KPDN oversees the Electronic Commerce Act 2006⁸, which stipulates that an electronic message in a commercial transaction is legally a valid contract. Yet, the Consumer Protection Act 1999, which falls under the purview of the same ministry, was initially not applicable to electronic transactions until the next year, when the 2007 amendment expanded the Act's scope to include "any trade transaction conducted through electronic means". The further introduction of the Consumer Protection (Electronic Trade Transactions) Regulations 2012⁹ by the same ministry helped to address the challenges and concerns surrounding the evolution of e-commerce activities in the country.

This expansion of role mirrors the general approach seen across most SEA-6 jurisdictions, in which existing laws are updated to fit the purpose for the digital age.

3.2 Specialist agencies emerge with fresh mandates

Apart from expanding the role of regulators to accommodate new business models and industries, new regulators may be formed. This is generally the case with data protection. Data protection regulation in the 20th century governed analogue applications, such as protecting the content of physical correspondence between individuals from leakage, or curtailing misuse of mailing lists from the postal services for marketing purposes.

In 1980, the Organisation for Economic Cooperation and Development (OECD) adopted the first internationally-agreed principles, namely the OECD Privacy Guidelines¹⁰ on data protection, which reflects the increasing use of computers to process business transactions. The guidelines serve as general guidance concerning the collection and the management of personal information, as digitalisation radically changed the way personal data is collected, processed and exploited.

Malaysia was the first country among SEA-6 to introduce its Personal Data Protection Act (PDPA) in 2010, followed by Singapore, Philippines and Thailand. In October 2022, Indonesia enacted the Personal Data Protection Law (PDP Law), with details of implementation expected in 2023.¹¹ Prior to PDP Law, personal data governance in Indonesia was under the purview of several agencies. A Data Protection Authority (DPA) under the Ministry of Communications and Informatics will be set up to enforce the new PDP Law. Meanwhile, in Vietnam, the Decree on Personal Data Protection (PDPD) submitted by the Ministry of Public Security (MPS) was issued in February 2023. It mirrors the EU's General Data Protection Regulation in different aspects and came into effect on 1 July 2023.

3.3 Increasing the need for coordination

While most SEA-6 governments entrust different aspects of tech regulation to several agencies, Thailand has taken a different approach. In 2016, the Thai government approved the establishment of the Ministry of Digital Economy and Society (MDES), replacing the Ministry of Information and Communication Technology. As the primary regulatory body responsible for Thailand's digital economy and its corresponding tech ecosystem, MDES' establishment signalled an intentional shift in the focus of the Thai government, from digital infrastructure development to the utilisation of digital technologies to benefit the country's overall socio-economic development.

Despite having a more centralised tech regulator charged with oversight over the digital economy and the impact of digital technologies on society at large, coordination across agencies is still necessary. Digital technologies are general purpose technologies and digitalisation will impact every industry vertical, including public services. The governance of new technologies and new business models require both digital and domain expertise, such as with the Bank of Thailand for e-payments and fintech, the Ministry of Transport for ride-hailing and the Ministry of Public Health for telemedicine, to name just three.

Another example of increasing need for coordination and streamlining processes can be observed in Singapore. In October 2023, Smart Nation and Digital Government Group (SNDGG) and the digital development initiatives of the Ministry of Communications and Information (MCI) were merged.¹² This marks a significant step in Singapore's intention to align and consolidate digital transformation efforts, which may be spread across various agencies. By combining SNDGG's oversight of the Smart Nation strategy and digital government services with MCI's leadership in digital economy development, regulation, and cybersecurity, the enlarged Smart Nation group is poised to comprehensively advance Singapore's digital agenda. This merger acknowledges the interconnected nature of digital initiatives and the goal of having more effective national and government digital strategies.

Hence, across SEA-6, increased coordination across agencies is more important than ever for tech regulation. In addition, various government agencies are charged with shaping different aspects of the tech ecosystem – from industry promotion, labour protection, talent development and digital skills development. Working together for learning and alignment is essential for the development of a sustainable, inclusive and equitable digital ecosystem.



4. Coordination Recommendations

Given the pace of change taking place in the digital economy, as well as the cross-cutting nature of the sector, greater coordination among stakeholders is vital to foster an enabling environment for innovation, while mitigating unintended consequences and emerging risk areas.

Coordination efforts between stakeholder groups involved in the digital economy that can be helpful in advancing the region's growth in this area include:

4.1 Between government agencies

The complexity, scale and ubiquity of digital technology requires close coordination between government agencies. Governments in the region can consider piloting near-term, soft coordination channels to serve as the de facto convening platforms for government agencies and departments to facilitate coordination, alignment, and where relevant, collaboration opportunities to address key areas of national concern.

Such channels could take the form of a multi-agency steering committee or programme office. An effective setup must be anchored on a set of principles to guide discussions, decision-making and recommending development processes that are co-chaired by senior public servants, to ensure that discussions involving policy trade-offs are tackled rigorously. As co-chairs, they will also have the discretion to determine if issues or recommendations require further escalation.

These coordinating mechanisms function best by bringing together diverse perspectives from public servants, technical experts, the private sector and the government of the day. This diversity will ensure both continuity of purpose and continuous sensemaking to build institutional knowledge and experience, while staying responsive to the dynamic and evolving opportunities and challenges.

An example of a “whole-of-government” coordination vehicle is MyDIGITAL Corporation in Malaysia, which has the mandate to coordinate and drive efforts across the government to advance the Malaysia Digital Economy Blueprint.¹³ In Singapore, a programme office model has been adopted in the form of the Smart Nation and Digital Government Office under the Prime Minister’s Office, to coordinate public sector efforts towards digital transformation.¹⁴

4.2 Between the public and private sector

As the pace of digitalisation and technology development continues to accelerate, open and collaborative lines of engagement between the public and private sector are vital. Digital economy companies drive innovation through research, developing and deploying new products and services. Many digital economy companies are also repositories of data, both operational and personally identifiable, at a scale often surpassing that are held by governments of its citizens.

Traditional modes of policymaking and governance are thus outpaced. Summarised as the “Collingridge Dilemma”, the impact of technology may not be known until it is widely adopted, but regulation or control is difficult once technologies, or the business models it enables, are entrenched.

While regulators have engagement mechanisms that seek private sector views on specific topics, consistent open dialogue is more important than ever. As suggested by the Tech Policy Design Centre, fora for effective exchange of knowledge and perspectives are ideally non-transactional and non-adversarial. Industry Associations, for example, have played a convening role for the private sector to engage its public sector counterparts across many industries. Other models, such as think tanks, non-profit organisations and self-regulatory organisations, have also demonstrated the ability to exercise oversight, encourage innovation and foster collaboration.

4.3 Between governments in Southeast Asia

With the fastest growing internet market in the world and a digital economy projected to add an estimated US\$1 trillion to regional GDP over the next decade, the promise of the “Digital Decade” can only be realised if key regulations are aligned, as complex differing regulations across jurisdictions can make it difficult for companies to scale.¹⁵ Clear shared frameworks will not only lower the cost of compliance for digital economy companies, but it can also foster confidence that technology is being developed and deployed ethically, responsibly and consistently across countries. This may take the form of interoperability of finance and payment platforms, collaboration of companies in the digital economy, the sharing of digital economy governance frameworks or be in the form of digital economy partnership agreements.

Today, ASEAN serves as one of the several important vehicles to foster coordination among governments in the ASEAN Member States (AMS), which include the SEA-6. In 2015, the Association of Southeast Asian Nations (ASEAN) launched the ASEAN Economic Community¹⁶, which aimed to create a single market and production base within the region. The ASEAN Digital Masterplan 2025¹⁷ and the Bandar Seri Begawan Roadmap¹⁸ translates this ambition to the digital economy. The 3rd ASEAN Digital Ministers Meeting held in February 2023 expressed satisfaction with the developments in the second year of the ADM 2025. This progress has established a solid base for expediting the digital transformation of the region and working towards a digitally-integrated ASEAN oriented towards interoperability with the global economy. These echo the nine elements outlined within the ASEAN Digital Economy Framework Action (DEFA)¹⁹, which include: cross-border data flows and data protection, online safety and cybersecurity, payments and e-invoicing, digital ID and authentication, digital trade, cross-border e-commerce, cooperation on emerging topics, talent mobility and cooperation, and competition policy.

While DEFA negotiations are anticipated to take at least two years, there is momentum for coordination and cooperation, with tangible, implementable solutions. One example is the release of the ASEAN’s Model Contractual Clauses (MCCs)²⁰ to help small businesses gain access to opportunities in the digital economy across the region. The MCCs are template contractual terms and conditions that businesses may adopt in their legal agreements in cases where personal data is transferred across borders. The MCCs reduce negotiation and compliance costs, while ensuring personal data protection. It serves as a starting point for enterprises, including startups and MSMEs. The MCCs let businesses get on with business, even as it navigates the intricacies and challenges of cross-border data flows.

ASEAN has also been working to harmonise e-commerce regulations across the AMS. The countries in the region have correspondingly been developing and expanding their own e-commerce regulations. For example, Indonesia passed its first e-commerce law in 2016, establishing guidelines for e-commerce transactions, data protection and consumer protection.²¹ ASEAN has also played an instrumental role in realising the Regional Comprehensive Economic Partnership (RCEP) Agreement, which came into force in 2022. By providing an expanded regional market, bolstering protection of intellectual property and enhancing rules in services and e-commerce, RCEP supports the growth of the digital economy of Southeast Asia.

Examples of cooperation at the ASEAN-level are summarised in Table 2 below.

Table 2. Key Initiatives of ASEAN for Digital Integration

| Digital Economy Pillar | ASEAN Initiatives |
|-------------------------|--|
| Digital Infrastructure | <ul style="list-style-type: none"> • ASEAN Agreement on Electronic Commerce |
| E-commerce | <ul style="list-style-type: none"> • ASEAN Agreement on Electronic Commerce • RCEP (Chapter 12 covers three principles of e-commerce provisions, namely (1) data free flow, (2) prohibiting requirements for data localisation, and (3) prohibiting requirements for source codes) • Digital Economy Framework Agreement - in discussions |
| Data Protection | <ul style="list-style-type: none"> • ASEAN Framework on Personal Data Protection • Digital Economy Framework Agreement - in discussions |
| Cybersecurity | <ul style="list-style-type: none"> • ASEAN Cybersecurity Cooperation Strategy • Digital Economy Framework Agreement - in discussions |
| Entrepreneurship | <ul style="list-style-type: none"> • ASEAN Framework for Promoting the Growth of Digital Startups |
| Cross-border Data Flows | <ul style="list-style-type: none"> • ASEAN Data Management Framework and Model Contractual Clauses • Digital Economy Framework Agreement - in discussions |
| Artificial Intelligence | <ul style="list-style-type: none"> • ASEAN Guidelines on AI Ethics and Governance - in discussions |

Note: List not exhaustive.

Source: Tech for Good Institute (2023).

Given the diversity of ASEAN member states in digital maturity and digital governance approaches, region-wide initiatives are essential to work together to realise the full potential of the digital economy. It is crucial for ASEAN to prioritise coordination and cooperation without necessarily aiming for complete harmonisation, but rather agreeing on frameworks that would chart pathways for interoperability. These would be steps towards creating a responsive regulatory environment that would enable an inclusive, innovative and investable Southeast Asia.

References

| | |
|----|---|
| 1 | Chakravorti, B., Chaturvedi, R. S., Filipovic, C., & Brewer, G. (2020, December). Digital in the time of COVID: Trust in the Digital Economy and Its Evolution Across 90 Economies as the Planet Paused for a Pandemic. Digital Planet. Retrieved 1 February, 2023, from https://sites.tufts.edu/digitalplanet/files/2021/03/digital-intelligence-index.pdf |
| 2 | Weaver, J., & O'Connor, S. (2023, February). Cultivating Coordination: Research Report. ANU Tech Policy Design Centre. Retrieved 23 May 2023, from https://techpolicydesign.au/wp-content/uploads/2023/02/TPDC_Publication_NO.4_230224_LowRes.pdf |
| 3 | Weaver, J., & O'Connor, S. (2022, May). Tending the Tech-Ecosystem: Who should be the regulator(s)?. ANU Tech Policy Design Centre. Retrieved 23 May, 2023 from https://techpolicydesign.au/wp-content/uploads/2023/08/Web_TPDC_Tending-Tech-Ecosystem_NO.1_2022_2023-Cover-Update_V2.pdf |
| 4 | Freiberg, A. 2017. Regulation in Australia. The Federation Press, xxxviii. |
| 5 | Productivity Commission. (2013, September). Regulator Engagement with Small Business (p. 34). Australian Government Productivity Commission. Retrieved 14 April, 2022, from www.pc.gov.au/inquiries/completed/small-business/report/small-business.pdf |
| 6 | This subsidiary regulation was issued before the establishment of the current NBTC but remains in effect. On 9 June 2023, the current NBTC members agreed to update its contents to be consistent with new standards of protection under PDPA. (https://www.nbtc.go.th/News/Press-Center/60815.aspx) |
| 7 | Previously known as the Ministry of Domestic Trade and Consumer Affairs (KPDNHEP) |
| 8 | Malaysia Federal Legislation. (2006, August 31). Act 658: Electronic Commerce Act 2006). Laws of Malaysia. Retrieved 23 May 2023, from https://lom.agc.gov.my/ilims/upload/portal/akta/LOM/EN/Act%20658.pdf |
| 9 | Attorney General's Chambers. (2012, December 21). P.U. (A) 458, Consumer Protection (Electronic Trade Transactions) Regulations 2012. Federal Government Gazette. Retrieved 22 May 2023, from https://lom.agc.gov.my/act-view.php?type=pua&lang=Bl&no=P.U.%20(A)%20458/2012 |
| 10 | OECD. (n.d.). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD Legal Instruments. Retrieved 22 May 2023, from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 |
| 11 | Dorwart, H., Demetzou, K., Paulger, D., Thong, J. L. K., Matheson, L., & Perera, I. (2022, October 19). Indonesia's Personal Data Protection Bill: Overview, Key Takeaways, and Context. Future of Privacy Forum. Retrieved 22 March 2023, from https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/ |
| 12 | Smart Nation. (2023, September 12). Singapore government announces merger of Smart Nation and Digital Government Group (SNDGG) with Ministry of Communications and Information (MCI) functions to form an enlarged Smart Nation group. Retrieved 5 November 2023 from https://www.smartnation.gov.sg/media-hub/press-releases/12092023 |
| 13 | Economic Planning Unit, Prime Minister's Department. (2021, February). Malaysia Digital Economy Blueprint. Economic Planning Unit. Retrieved 21 February 2023, from https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf |
| 14 | Smart Nation and Digital Government Office. (2018, November). Smart Nation: The Way Forward. Smart Nation Singapore. Retrieved 22 May 2023, from https://www.smartnation.gov.sg/files/publications/smart-nation-strategy-nov2018.pdf |
| 15 | United Nations Conference on Trade and Development. (2021). Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. United Nations Publications. Retrieved 23 May 2023, from https://unctad.org/system/files/official-document/der2021_en.pdf |

| | |
|----|--|
| 16 | ASEAN Secretariat. (n.d.). ASEAN Economic Community, 2015 - progress and key achievement: a blueprint for growth. ASEAN. Retrieved 22 May 2023, from https://asean.org/book/asean-economic-community-2015-progress-and-key-achievement-a-blueprint-for-growth/ |
| 17 | ASEAN Secretariat. (2021, September). ASEAN Digital Masterplan 2025. ASEAN. Retrieved 22 May 2023, from https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf |
| 18 | Association of Southeast Asian Nations (ASEAN). (October 2021). Bandar Seri Begawan Roadmap on ASEAN Digital Transformation Agenda. Retrieved 22 May 2023 from https://asean.org/wp-content/uploads/2021/10/Bandar-Seri-Begawan-Roadmap-on-ASEAN-Digital-Transformation-Agenda_Endorsed.pdf |
| 19 | ASEAN Secretariat. (2023). Framework for Negotiating the ASEAN Digital Economy Framework Action. Retrieved from 5 November 2023 from https://asean.org/wp-content/uploads/2023/09/Framework-for-Negotiating-DEFA_ENDORSED_23rd-AECC-for-uploading.pdf |
| 20 | Association of Southeast Asian Nations (ASEAN). (January 2021). ASEAN Model Contractual Clauses for Cross-Border Data Flows. Retrieved 22 May 2023 from https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf |
| 21 | Global Regulation. Translation of Act No. 19 - Year 2016. Retrieved 22 May 2023, from https://www.global-regulation.com/translation/indonesia/8999766/act-no.-19-year-2016.html |

