Endorsed

ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN)

FRAMEWORK ON DIGITAL DATA GOVERNANCE

Background and Overview

1. ASEAN as a regional group has been experiencing sustained economic growth. With the right elements in place such as good and robust infrastructure, sound and progressive policies and governance frameworks, ASEAN's potential for growth is tremendous. To achieve this growth, it would be critical to boost economic integration and technology adoption across all sectors in the ten ASEAN Member States[1] (referred to collectively as "ASEAN Member States" or individually as "ASEAN Member State").

2. Globally, there have been significant efforts to harmonise data standards, data governance or data protection frameworks, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, APEC Privacy Framework, EU General Data Protection Regulation (EU-GDPR) and Standards for Personal Data Protection for Ibero-American States. To keep pace, ASEAN needs to develop forward-looking and enabling frameworks and policies that facilitate the growth of the digital economy. There is also a need to strengthen the governance of digital data in ASEAN with a view to promoting the growth of trade and flow of data within and among ASEAN Member States in the digital economy. Progress on digital data management issues also vary considerably across ASEAN and there is significant opportunity to improve transparency on requirements and identify areas to enhance performance.[2]

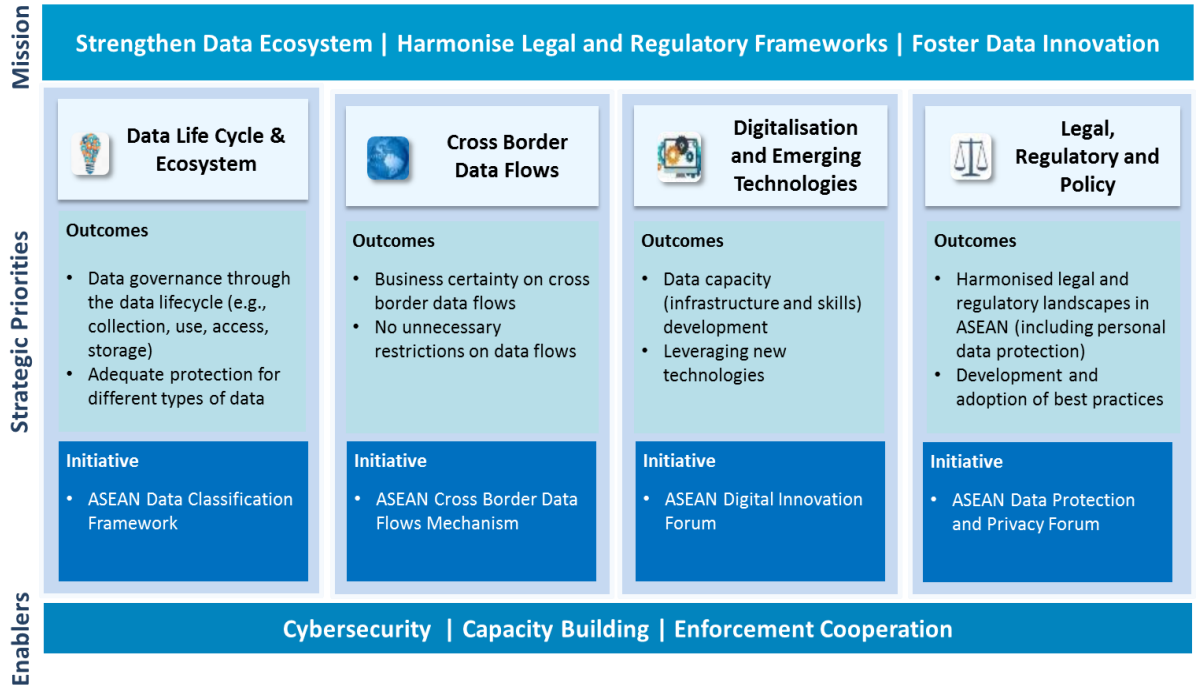
3. In this respect, the Heads of State of ASEAN Member States have jointly reaffirmed the importance of maintaining ASEAN centrality and unity in its community-building efforts, and have agreed on key deliverables for ASEAN such as Cybersecurity cooperation and personal data protection, and promoting innovation and e-commerce.[3] The Master Plan on ASEAN Connectivity 2025 has also identified the development of an ASEAN Framework on Digital Data Governance (referred to as the "Framework") as an initiative that is intended to enhance data management, facilitate harmonisation of data regulations among ASEAN Member States[4] and promote intra-ASEAN flows of data. This helps to ensure that ASEAN, collectively, realises the potential benefits, even with the recognition that the ten ASEAN Member States are currently at different levels of maturity.

[1] The term ASEAN Member States refers to Brunei Darussalam, the Kingdom of Cambodia, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand, and the Socialist Republic of Viet Nam.
[2] Master Plan on ASEAN Connectivity 2025 Project Concept – Concept Note Initiative 7 – Establish an ASEAN Digital Data Governance Framework, 15 August 2017.
[3] Chairman's Statement of the 32nd ASEAN Summit, Singapore, 28 April 2018.
[4] Building on the ASEAN Framework on Personal Data Protection adopted in 2016.

Objectives

4. This Framework sets out the strategic priorities, principles and initiatives to guide ASEAN Member States in their policy and regulatory approaches towards digital data governance (which include both personal and non-personal data) in the digital economy. These are summarised in Figure 1.

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



Scope of the Framework

5. The Framework identifies four strategic priorities of digital data governance that support the ASEAN digital economy, namely:

   (a) Data Life Cycle and Ecosystem;
   (b) Cross Border Data Flows;
   (c) Digitalisation and Emerging Technologies; and
   (d) Legal,Regulatory and Policy.

6. The Framework also identifies four initiatives that can be undertaken in support of the four strategic priorities, which are:

   (a) ASEAN Data Classification Framework;
   (b) ASEAN Cross Border Data Flows Mechanism;
   (c) ASEAN Digital Innovation Forum; and
   (d) ASEAN Data Protection and Privacy Forum.

7. This Framework will not apply to:

   (a) Measures adopted by an ASEAN Member State to exempt any areas, persons or sectors from the application of the Principles identified under the Framework; and

   (b) Matters relating to national sovereignty, national security, public safety, and all government activities deemed suitable by an ASEAN Member State to be exempted.

ASEAN Guiding Principles on Data Governance for the Digital Economy ("Principles")

8. The Principles for each strategic priority aim to provide ASEAN Member States with guidance to develop data governance for the digital ecosystem based on each ASEAN Member State's level of readiness and development.

9. Each ASEAN Member State will endeavour to take into account and implement within their domestic laws and regulations the Principles in accordance with this Framework. Where relevant, each ASEAN Member State should also encourage organisations to consider or incorporate these Principles when developing policies and practices.

Strategic Priority 1: Data Life Cycle and Ecosystem

10. The Principles on the data life cycle and ecosystem highlight the importance of data governance at every stage of the data life cycle and how that can contribute to the overall integrity and usability of data. The data life cycle follows the various stages of data management – from the point when the data is generated or collected for specific functions or purposes, to the data being used (e.g. processed and analysed), including when the data is in transit or at rest and through to the final point where the data is eventually deleted.

A. Principle on Data Integrity and Trustworthiness

11. The Principle on data integrity and trustworthiness recognises that access to accurate and reliable data is critical, especially when the data is used to analyse and support business decisions such as product development, service delivery or market expansion. This would include:

   (i) Tracking and documenting data sources to account for when data is procured externally or generated internally;

   (ii) Ensuring data accuracy, where practicable, over the entire data life cycle by implementing good data management practices, including managed data collection and creation, proper data recording and processing such that it does not affect the data quality, review and update internal databases to ensure data is up-to-date especially when the data is used to make a decision about individuals, and incorporate safeguards for data storage; and

(iii) Promoting interoperability of standards by ensuring that data provided is in a structured, commonly used and machine-readable format.

B. Principle on Data Use and Access Control

12. The Principle on data use and access control promotes accountability in data processing, which is a key component in data governance. This would include:

(i) Using and/or processing data only for purposes that are reasonable and appropriate; and which are not contrary to laws or national policies;

(ii) Assigning different access controls and levels of authorisations to personnel for access to different types or classifications of data; and

(iii) Ensuring that access to data should be adequate, relevant, and transparent.

C. Principle on Data Security

13. The Principle on data security establishes the need to safeguard data, and any storage centres the data sits within, as well as the systems and platforms that handle the data. This would include:

(i) Taking appropriate measures, including technical, procedural and physical measures, to ensure that they protect the confidentiality, integrity and availability of any data in their possession, or control against risks such as loss or unauthorised access, use, modification, disclosure, or destruction; and

(ii) Addressing data breaches promptly and effectively, by containing the breach and implementing mitigating measures to rectify the breach and where relevant, in accordance with national policies on data breach notifications.

Initiative under Strategic Priority 1: ASEAN Data Classification Framework

14. Data governance principles on data life cycle and ecosystem may differ depending on, among other things, the types of data. The level of protection required and accorded under the Principles may apply the same approach and considerations. For example, certain types of data (e.g. sensitive personal data) require higher levels of protection, such as by having stricter access controls or more stringent handling and disclosure requirements compared to data that is publicly available.

15. To afford data the necessary and adequate level of protection, it will be useful to have a common data classification framework, which sets out broad categories of data, descriptions of what each category entails and development of security requirements for each data classification level.

16. The data classification framework is not meant to be an exhaustive or binding list of data categories. Each category of data will include recommended measures or protections that should apply to that specific category of data. These include steps that can be taken to allow data to be processed, shared or transferred across country borders. The factors that could be considered for the development of the data classification framework include data sensitivity, risk assessment, protection impact management, storage and storage standards, or applicable industry regulations and standards.

Strategic Priority 2: Cross Border Data Flows

17. Data is regarded as the lifeblood of the digital economy, driven by increasing technology adoption and digitalisation. As the region moves towards a borderless, interconnected environment, the Principle on cross border data flows is intended to guide governments, businesses and consumers in the region as they navigate their way through managing data flows in this new phase of digital transformation and integration.

18. Data flows should be accompanied by assurances that safeguards are in place to protect and secure the information regardless where the data goes. These safeguards should be harmonised to prevent the development of fragmented regulatory regimes, which may negatively impact data flows and increase business compliance costs.

19. It should be emphasised that not all requirements imposed on cross border data flows are detrimental to the economy. Requirements may exist to ensure that there are safeguards to accord the necessary protection for the data being transferred. It is important for individual ASEAN Member States to review and minimise restrictions[5] to cross border data flows against the backdrop of its overall impact to data innovation and the goal of fostering a vibrant data ecosystem.

D. Principle on Cross Border Data Flows

20. The Principle on cross border data flows is intended to maximise the free flow of data within ASEAN to foster a vibrant data ecosystem but at the same time ensure that the data transferred is accorded the necessary protection. This would include:

(i) Facilitating cross-border data flows within ASEAN by developing clear and unambiguous requirements and/or criteria and/or circumstances in which data can be transferred from one ASEAN Member State to another;

(ii) Evaluating and ensuring that the requirements on cross border data flows within ASEAN are proportionate to the risks associated with

[5] Restrictions may come in the form of policies requiring organisations to store data within the country (e.g. data localisation), or regulatory conditions imposed before data can flow out of the country of origin (e.g. consent of the individual, for purposes of fulfiling contractual obligations).

transferring the data, taking reference from the data classification framework; and

(iii) Building trust by ensuring an adequate level of protection is accorded to the transferred data.

Initiative under Strategic Priority 2: ASEAN Cross Border Data Flow Mechanism

21. Increased data flows promote innovation and collaboration. However, for these benefits to materialise, businesses need regulatory certainty on who they may share data with, the types of data that may be shared, and how they may share such data. A cross border data flow mechanism within ASEAN is expected to facilitate such data flows between participating ASEAN Member States.

22. While specifics of the mechanism will need to be worked out, the mechanism will take into account the different levels of maturity and local laws present in the ASEAN Member State. ASEAN Member States may then assess their participation in the mechanism when they are ready to do so.

Strategic Priority 3: Digitalisation and Emerging Technologies

23. It is important for ASEAN Member States to identify and leverage emerging technologies and the latest trends, including the benefits these technologies can offer. Capacity building is an important part of this, and an economy will only be able to develop itself as a digital economy if it has access to well-developed infrastructure and a skilled workforce. These two elements often feed off each other to produce digital solutions and generate significant synergies, including in the promotion of cross-border data transfers.

E. Principle on Capacity Development

24. The Principle on capacity development advocates capacity building and equipping stakeholders with the necessary resources to evolve with the new trends and technologies. This would include:

(i) Undertaking regular stakeholder engagements and consultation sessions to assess and put in place basic and next-level support structures to develop and sustain the digital infrastructure in the short, medium and long-terms;

(ii) Facilitating universities and learning institutions in updating their curricula and pedagogic approaches in educational and vocational training to equip and empower the current and future workforce with relevant data and digital skills;

(iii) Encouraging organisations, especially micro, small and medium enterprises, to conduct regular on-the-job training for employees; and

(iv) Encouraging cooperation and aid on human capacity development, information exchanges between ASEAN Member States, as well as with

international organisations to reduce the digital divide between ASEAN Member States.

Initiative under Strategic Priority 3: ASEAN Digital Innovation Forum

25. Given the pace at which technological innovation and advancement is occurring, some firms in traditional sectors, small and medium enterprises, and even government agencies grapple with keeping abreast of the latest technological developments and emerging technologies. As technologies have the potential to help businesses streamline their operations and drive growth, productivity and innovation, there is significant value in knowledge sharing and transfer between technology firms, ASEAN Member States that have adopted such technologies, with other ASEAN Member States.

26. ASEAN should establish a digital innovation forum to create avenues for businesses of all sizes from ASEAN to share the latest technological developments. The forum functions as an avenue for effective dissemination of information on emerging digital trends and the relevant regulatory issues. Such forums can also include hands-on workshops for participants to experiment with the latest technological solutions, and to motivate them to adopt new technologies. Ideally, these forums would encourage collaboration between technology firms and other private and public sector organisations, promote data-driven innovation and improve awareness on key issues such as cybersecurity in ASEAN.

Strategic Priority 4: Legal,Regulatory and Policy

27. A harmonised legal and regulatory digital data environment within ASEAN plays a vital role in generating business confidence and stimulating economic growth. While there are a few key pieces of legislation that form the foundation of digital economies, a particular area of focus is on the development and harmonisation of personal data protection regulations, building on the ASEAN Framework on Personal Data Protection.

F. Principle on Personal Data Protection and Privacy Regulation

28. The Principle on personal data protection and privacy regulation establishes the need for harmonisation of personal data protection regulations within ASEAN. ASEAN Member States should endeavour to work towards establishing personal data protection regulations in their respective countries.

29. In the absence of country-specific personal data protection regulation, any policies established sectorally may refer to the Principles set out in the ASEAN Framework on Personal Data Protection, including Consent, Notification and Purpose, Accuracy of Personal Data, Security Safeguards, Access and Correction, Transfers to Another Country or Territory, Retention and Accountability.

G. Principle on Accountability

30. The Principle on accountability requires the development and implementation of data protection and data management policies and guidelines. This would include:

(i) Data protection and data management policies that are clearly documented and communicated with relevant stakeholders; and

(ii) Continuous review of data protection and data management policies to take into account relevant emerging technologies and trends, and to make amendments as necessary to maintain currency.

H. Principle on Development and Adoption of Best Practices

31. The Principle on development and adoption of best practices recognises the non-binding nature of the Framework, and encourages ASEAN Member States to promote adherence with these principles. ASEAN Member States should endeavour to encourage domestic adoption of measures that give effects to the Principles in this Framework.

Initiative under Strategic Priority 4: ASEAN Data Protection and Privacy Forum

32. ASEAN Member States can establish an annual ASEAN Data Protection and Privacy Forum to facilitate knowledge sharing and discuss the implementation details of the four proposed initiatives under this Framework, whether the ASEAN Member State has an established data protection authority or otherwise.

33. The ASEAN Data Protection Forum can facilitate the sharing of knowledge and operational know-how by policy makers and regulators, which will help ASEAN Member States that do not have a personal data protection authority in setting up their respective authorities. It can also discuss, among other things, issues such as enforcement cooperation, considerations when dealing with multiple stakeholders in data protection enforcement cooperation.

Effect of the Framework

34. This Framework is non-binding, and does not create rights or obligations under domestic or international law for the ASEAN Member States.

Implementing the Framework

35. To facilitate the implementation of this Framework, including the proposed initiatives, ASEAN Member States should endeavour to provide regular bi-annual updates on their progress of implementing the Framework at the working group level. This will enable ASEAN Member States to monitor their development with respect to this Framework.

36. Thereafter, following the establishment of the annual ASEAN Data Protection Forum, ASEAN Member States may provide milestone updates at this Forum.

Amendments

37. This Framework may be reviewed periodicially, and amended at any time to incorporate new developments or changes, by mutual agreement amongst all ASEAN Member States.

ADOPTED AT Bali, Indonesia, this sixth day of December in the year two thousands and eigthteen in one (1) original copy in the English language.