EABC (European Association for Business & Commerce) also known as The European Chamber of Commerce Thailand www.eabc-thailand.org is pleased have the opportunity to respond, through the EU ASEAN Business Council (EU-ABC) on the Study on the ASEAN Digital Economy Framework Agreement (DEFA) – Mapping Study and Gap Analysis – issued 4 April 2023. EABC is joined by the Joint Foreign Chambers of Commerce in Thailand (JFCCT www.jfcct.org) in this endeavour.

A. Key points

1. There are many ASEAN instruments in the digital area, we see a DEFA as an opportunity to consolidate essential and some missing terms into a mandatory and binding agreement. It need not be so comprehensive as to take years to finalise and must avoid unnecessary administrative burdens. A multinational agreement must mandate inclusion in an AMS domestic (or 'municipal') legislation. If it is overly prescriptive rather than relying on fundamental rules and guidelines it won't succeed. A review of existing instruments is thus needed – DEFA should replace some and complement or provide a higher framework for others. In particular consider what if any an on-going role for DIFAP would be. Common language is lacking in Digital FAs.

2. That approach should still recognise that the ten AMS represent a range in economic development. On any given topic today, there is a range of policy and legislative responses. A DEFA should move the dial towards harmonisation but not kill the goose.

3. Market access in services is on a trend which tends to default to a de facto Mode 3 for services (Commercial presence) through requirements in certain developing regulations. It should not, such a trend is a barrier to effective digital trade. Modes 1 and 2 (in particular 1) need to be valid for digital trade. *See more in Part C, below*

4. Free flow of data – based on the DFFT (Data Free Flow with Trust) concept. Cross border payments and making them effective requires a public and private sector effort based on common goals. Information-rich file formats (using ISO standards) are needed. There are many other use cases for cross border flows of data. *See more in Part C, below*

5. Conceptually, a good understanding about data and what WTO and other jurisprudence suggest it is (a service). Free flow of data (digital pieces), including payments is essential to support trade. Data is also an asset class in its own right.

6. Digital ID, authentication, Digital signatures development varies greatly amongst AMS. DEFA should set a path to optimise compatibility at a minimum for authentication. This requires a public and private sector effort. *See more in Part C, below*

7. Digital government development cannot be ignored. For a DEFA to be effective, an approach to digital government needs guidelines towards digitalisation: elements such as interoperability amongst agencies, single-sign on etc are needed.

8. Far greater multi-national efforts in Cybersecurity and battling cybercrime are needed. ENISA and US reports show that Ransomware is the #1 Cyberthreat. *See more in Part C, below*

9. DEFA should support good business practices and reasonable consumer protection. Climate impact is an emerging area.

10. Regulation in developing areas such as Metaverse and AI (Ethical AI, Generative AI) needs Guidelines and bases without over-prescription at this stage. These should be tech neutral. Digital assets such as cryptocurrencies should have agreed Guidelines as a minimum.

11. IP protection is essential for innovation and predictable business. We do not advocate a separate IPR regime but note its importance. There are challenges to Copyright and Data Protection brought about by the easy ability in AI and Social Media to create content. *See more in Part C, below*

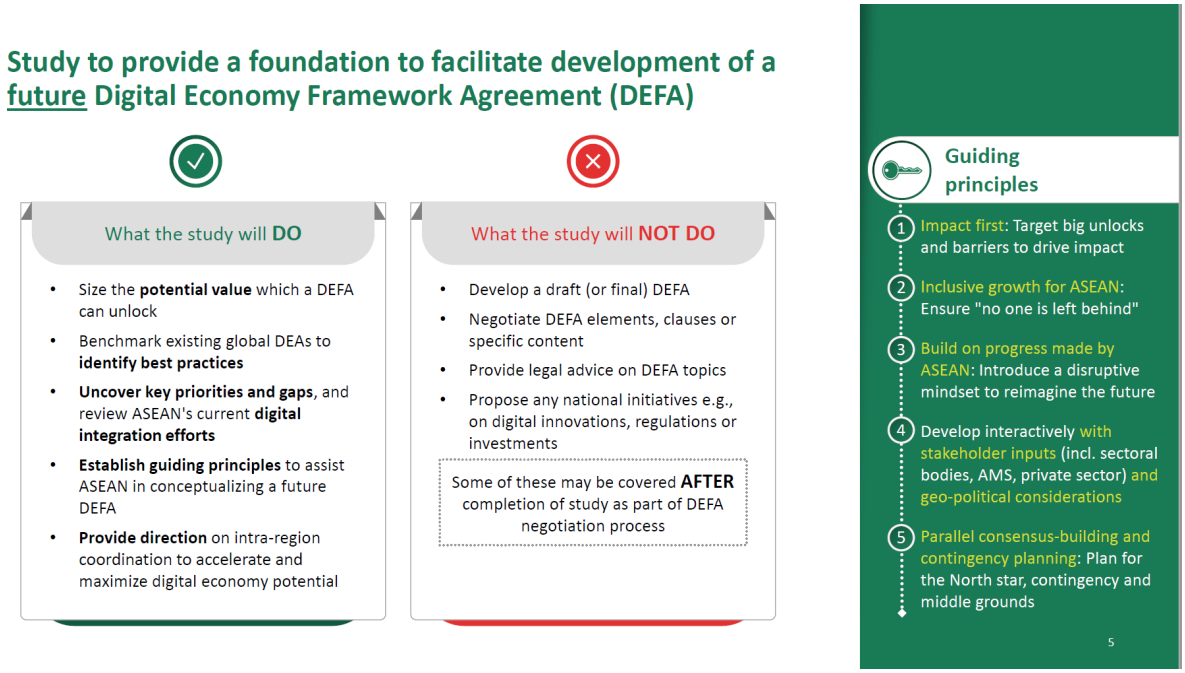
12. Harmonisation on data protection approach. There is already an ASEAN instrument. Cross border disclosures are an essential part as is Data Localisation. The GDPR has a test about data adequacy, so does the Thailand PDPA. DEFA should support minimal standards about this. There is misunderstanding about data localisation. *See more in Part C, below*

13. In a regional context, digital skills development requires freer flow of skills. We also recommend support for the concept of Digital Nomads to unlock barriers to upskilling and wider availability of skills. *See more in Part C, below*

14. The soft and hard infrastructure which enables digital economies needs greater investment. Telecoms sector (which underpins the Digital Economy) regulation is included in GATS and regional FTAs but market access effectiveness varies. Under-investment in hard infrastructure should be examined to identify those areas which have provided reasonable investment and those where more is needed. Our definition of Digital Economy (see Annex) recognises the role of the telecoms sector.

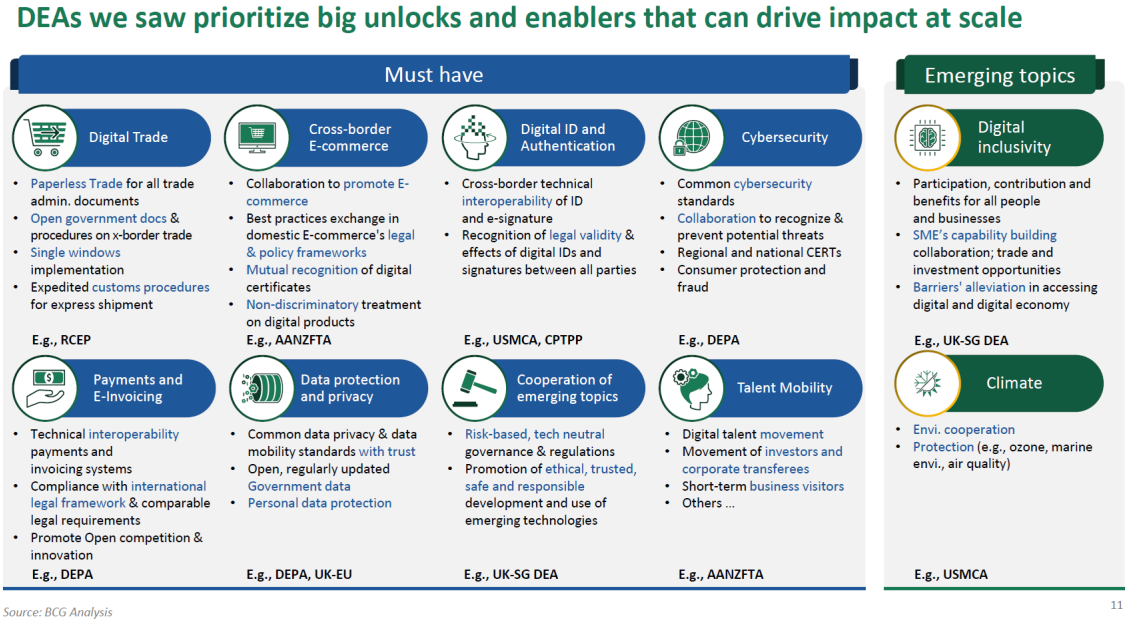
We expand on certain of these in Part C below (3,4,6,8,11,12,13) .

We note the aims of the study and what it is not intended to do:



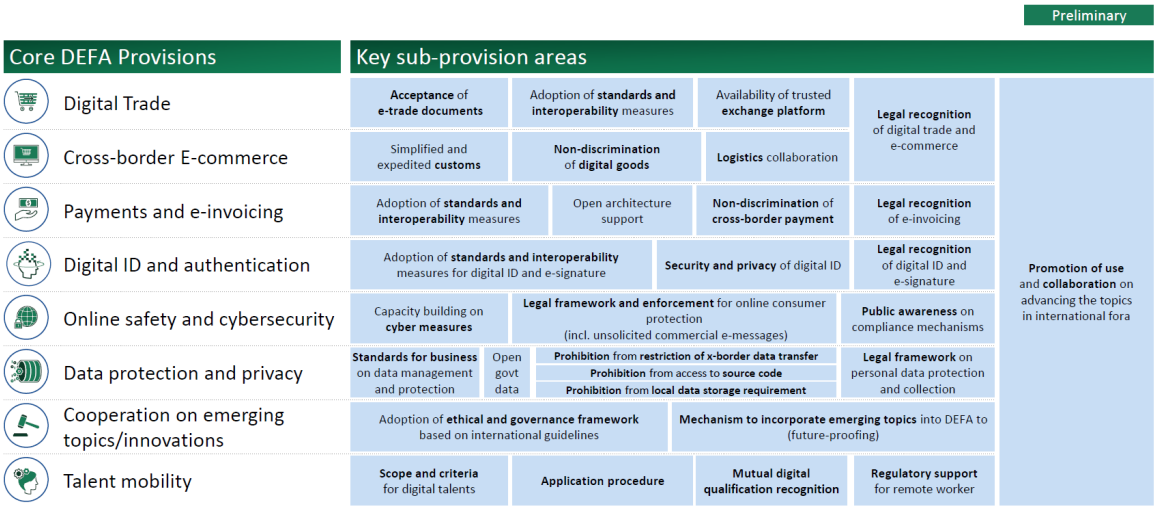
B. BCG identification of topics

The BCG review of existing DFAs is useful to prompt areas where DEFA needs to make a difference.



We note how these eight topics form a basis for proposed DEFA topics.

Discussion Question: What are important key elements to drive Northstar DEFA?



Our analysis is largely in line but with some additional points and some different emphases.

C. Further details on selected topics (see part A for numbering)

3. Market access in services

This is on a trend which tends to default to a de facto Mode 3 for services (Commercial presence) through requirements in certain developing regulations. It should not, such a trend is a barrier to effective digital trade. Modes 1 and 2 (in particular 1) need to be valid for digital trade.

Regulation of Digital Platforms where business is done in an economy, varies around AMS from none, to light touch with a Guideline, to a heavy regulation in Thailand (gazetted December 2022) which borrows heavily from the EU Digital Services Act, but with much reporting and control. It will be expensive to comply with. The proposal to require representatives for example would have made the requirement tantamount to Mode 3 delivery.

This is one example. Mode 1 should be supported. Principles of good business and consumer protection are well appreciated.

4. Free flow of data

Based on the DFFT (Data Free Flow with Trust) concept. Cross border payments and making them effective requires a public and private sector effort based on common goals. Information-rich file formats (using ISO standards) are needed. There are many other use cases for cross border flows of data.

In "MOVING FORWARD ON DATA FREE FLOW WITH TRUST: NEW EVIDENCE AND ANALYSIS OF BUSINESS EXPERIENCES"' April 2023[1], an extract from the Executive Summary puts it well:

> "Businesses indicate that they attach fundamental importance to the protection of personal data and privacy, for the protection of the rights of individuals, of sensitive business data, and as an economic asset and competitive advantage. At the same time, they also highlight that while privacy and data protection frameworks aimed at generating trust and facilitating data flows build on commonalities and elements of convergence, challenges remain on how to fully "operationalise" them globally to ease compliance and facilitate cross-border data flows.'

Thus international regulatory co-operation on data protection/privacy is needed, in addition to co-operation on data flows for interoperability.

Although published some years ago (2016) this McKinsey Global Institute graphic illustrates a wide range of use cases for data:

Digitization is transforming business models in ways that enable more cross-border activity

Cross-border implications of digitization		Flow type: Data	Goods	Services	Finance	FDI
Remote monitoring	Remote tracking	●	●			
	Remote maintenance	●	●			
Supply-chain management	Remote inventory management	●	●			
	Supplier management	●	●			
Access to global markets	Cross-border access to customers	●		●	●	
	Cross-border access to labor	●		●		
	Cross-border access to finance	●			●	
Business operations and strategy	Centralized back-office operations	●		●		
	Cross-border digital payments	●			●	
	Real-time communications and collaboration	●		●		
	Data sharing and analytics-driven decision making	●	●	●	●	●

SOURCE: McKinsey Global Institute analysis

[1] OECD DIGITAL ECONOMY PAPERS April 2023 No. 353; prepared by the Working Party on Data Governance and Privacy (WPDGP), based on the responses to a survey about businesses' perspectives on the importance of cross-border data flows and trust, and related compliance challenges as more laws and regulations applicable to data flows are adopted globally. DFFT= Data Free Flow with Trust.
https://www.oecd-ilibrary.org/docserver/1afab147-en.pdf?expires=1682824093&id=id&accname=guest&checksum=2126A3BB53139EFA7B108E21EF734474

We deal with the privacy concerns in another part. Elements of what are needed in this part are:

- Regulatory support for free flow
- Cybersecurity standards and enforceability; international cybercrime co-operation
- Rich information file fomats eg ISO 20022

6.Digital ID, authentication, Digital signatures development
This aries greatly amongst AMS. DEFA should set a path to optimise compatibility at a minimum for authentication. This requires a public and private sector effort.

Digital IDs and IDaaS from identification providers is emerging. To support regional objectives, recognition and harmonisation will be needed. Imposing a single standard at this stage may be a stretch too far, but should not be ruled out.

Each economy has its own taxonomy. This should cover citizen ID, foreigner ID and entity ID. Singapore for example has NRIC for individuals (local and PR or long term pass holder) FIN (Foreign Identification Number) and UEN (Unique Entity Number) for entities.
Digital signature take up lags due to inadequate policy support in some cases and poor usage by the government sector and private sector. Government agencies and the private sector (eg banks) in all economies require hard copy, wet signature in many cases where they do not need to.

8. Cybersecurity
Far greater multi-national efforts in Cybersecurity and battling cybercrime are needed. ENISA and US reports show that Ransomware is the #1 Cyberthreat.

A change of mindset is needed. While by analogy we recognise and respect Copyright violation being a criminal offence (see the FBI warning shown at the start of movies), we laud the skills of hackers. White hat hackers are needed, black hat hackers are hard to prosecute.

Efforts to combat Ransomware are largely failing. Trust will not be reached without a change. Just like the FBI warning, consider a criminal offence warning at IT conferences about black hat hacking.

11.IP protection
Essential for innovation and predictable business. We do not advocate a separate IPR regime but note its importance. There are challenges to Copyright and Data Protection brought about by the easy ability in AI and Social Media to create content.

AI (eg generative AI) and social media make content creation easy. Copyright and Data Protection do not offer adequate protection. How will DEFA cover this ? - changes to those regimes or a new legal regime?

12. Data protection and privacy

Harmonisation on data protection approach. There is already an ASEAN instrument. Cross border disclosures are an essential part as is Data Localisation. The GDPR has a test about data adequacy, so does the Thailand PDPA. DEFA should support minimal standards about this. There is misunderstanding about data localisation.

Cross border disclosure includes much development and ASEAN intent. The ASEAN Framework on Personal Data Protection is weak on cross border disclosures. Data adequacy is a useful approach.

Most FTAs are anti data localisation. The general consensus now seems to be (regardless of whether or not the context is FTA) that localisation (and the more extreme measure, nationalisation) is anti free trade, and even, anti-innovation.

A 2016 publication being a survey of practices in FTA[2] 'Free Trade Agreements and data privacy: Future perils of Faustian bargains; notes:

"Countries negotiating new bilateral or multilateral trade agreements, particularly but not exclusively the USA, are likely to attempt to include requirements that the parties do not include any significant data export restrictions, or 'data localisation' provisions in their laws. This chapter surveys the variety of ways in which FTAs have affected data privacy by considering a range of examples,.."

And in para 1.2 in that paper the author's view:
"…the only role that privacy rights should play in Free Trade Agreements is a negative one: as explicit exceptions confirming that other FTA provisions have nothing to do with limiting the protection of privacy (or other human rights)."

There have been data leaks and many AMS have sector specific legislation (separate to a PDPA or equivalent eg in financial services, medical records and national security data) which prohibits certain disclosures and even requires it to be kept on premises in certain cases.

Most frequently in an FTA setting, data localisation is seen as favouring privacy (at the expense of free trade). The big privacy issue in the FTA setting is that increased (cross-border) flow of personal data comes with increased risks to privacy.

[2] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732386 – Prof Graham Greenleaf, in a publication edited by Prof Dan Svantesson. 2016

What is the right balance and how can this be managed?

Personal data are both crucial in trade (including cross-border trade) and protected (in some contexts as a fundamental human right) does not show an obvious solution.

Thus, while trade agreements often contain an anti-localisation provision, "it should be noted that such instruments typically also contain normal exceptions permitting data localisation in specific circumstances" [3]

One solution might be in seeing just how narrowly the protection of privacy can be read while still remaining effective. That is unless there is time for AMS to become convinced of the need for data localisation due to national security (/resilience) concerns.

"As data localisation may seek to protect data privacy in some cases, and undermine it in others, any assessment of the impact data localisation has on data privacy must be holistic and context-specific."[4]

Leaks, hacks and the increased concerns about undersea Internet cables being cut in case of conflicts will become a big driving force for data localisation (even if the data privacy concerns are overcome).

Thus we recommend:

- A need to justify any data localisation -eg about medical records, financial services records, national security, but not prohibit it.
- Data Nationalisation should not be allowed

13. Digital Skills

In a regional context, digital skills development requires freer flow of skills. We also recommend support for the concept of Digital Nomads to unlock barriers to upskilling and wider availability of skills.

A broad definition of Digital Literacy ('Digital Skills' might be better)

> "Digital literacy is the *a*bility to use, create and share digital content safely and responsibly. It is an overarching concept for a wide range of skills:
>
> i. *technology competency*, which is the use of digital technology;

[3] Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris, https://doi.org/10.1787/7fbaed62-en. Page 20

[4] Recommendation 4 of the OECD paper

ii. *information literacy*, which is the ability to locate, identify, retrieve, process and use digital information optimally; and

iii. *media literacy,* which enables us to comprehend, contextualise and critically evaluate information, as well as to create and communicate content effectively across digital media platforms.
iv. *cyber wellness*, includes taking personal responsibility to use the internet for the good of the community, and understanding the risks of online dangers and negative online behaviours.

(source imda.gov.sg)

A more narrow or traditional definition of Digital Literacy is about the ability to use computers, on-line tools and interact with others digitally.

EU – DigComp – Digital Competency for Citizens
• 1) **Information and data literacy**: Articulate information needs, Locate and retrieve digital information
• 2) **Communication and collaboration**: To interact, communicate and collaborate
• 3) **Digital content creation**: To create and edit digital content , integrate
• 4) **Safety**: To protect devices, content, personal data and privacy
• 5) **Problem solving**: To identify needs and problems and solve
https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

Digital Skills are enhanced by local economy training and education and by freer flow of skills.

This needs more than another MRA (Mutual Recognition Arrangement) but attention to visa and work permit regulation.

Many economies have Digital Nomad type visas now. Thailand does not have one. The only AMS with one is believed to be Malaysia. We will be pleased to supply more details,

29 April 2023

Annex: Our Definition of Digital Economy

Our definition of Digital Economy is based on a concept published by Analysys-Mason in 2015, adapted with A-Ms permission and updated by us in 2019.

> The 'digital economy' is all economic activity mediated by software and enabled by telecoms infrastructure.
>
> This includes core telecoms services such as voice, messaging, data, and video.
>
> The goods and services within the digital economy (whether used via consumer, business, government, civil society or wholesale deployment and whether delivered Machine-to-Machine, Machine-to-Person or Person-to-Person) can be broadly grouped as:
>
> ***intrinsically digital*** – streaming video, eBooks, computing services, Software-as-a-Service, social media, Internet of Things, Artificial Intelligence, Machine Learning, Virtual Reality services, games, various intelligent uses of Data to create value,
>
> ***substitutes for established equipment and services*** – virtual private communications networks, security services, virtualised PBXs, Platform-as-a-Service and services delivered on-line (e.g. accounting / other business processes, graphic design, software development, data analytics, knowledge-based outsourcing, eCommerce, banking and financial services, on-line payments, telemedicine; industry and home automation),
>
> ***marketing, sale, logistics, etc. of physical goods*** – (e.g. Amazon, eBay, Alibaba, Tarad.com, Lazada, Shoppee),
>
> ***marketing and sale of services*** which are not delivered on line (eg air services, taxi services, hotel bookings.
>
> Digital Economy is the means of enabling everyone's participation in and interaction with social and economic enterprise, and also includes the role played by governments in developing infrastructure and services.

The Digital Economy grows in three ways:

> (i) By the digitalisation of processes, services and products which have evolved from an analogue or off-line state, or have new digital equivalents
>
> (ii) By the entry of 'native' digital services, products or processes.
>
> (iii) By various digitalisation transformations and developments of organisations in the public and private sectors.