DATA GOVERNANCE IN ASEAN: FROM RHETORIC TO REALITY

April 2020

EU-ASEAN BUSINESS COUNCIL

Table of Contents

Executive Summary

ASEAN'S DIGITAL SERVICES (US$)

$38bn

e-commerce

$13bn

ride-hailing

$14bn

digital media

$34bn online travel agencies

Google, Temasek, Bain & Company (2019) e-Conomy SEA 2019, Available online: https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf

The digital economy in Southeast Asia has been one of the region's success stories. In 2019, the region's internet economy crossed the US$100 billion mark, a three-fold growth in barely four years. With a growing young and tech-savvy population, increasing digitisation of industry and strong consumer demand for e-commerce, ASEAN has strong fundamentals to support the digital economy's long-term growth.

However, much more needs to be done to ensure that ASEAN can achieve the projected US$300 billion internet economy in 5 years, especially in the area of data governance. Data has arguably become the most important asset, essential to both the public and private sector as it has real, measurable value which is used across every sector. Whether directly, or by indirectly taking advantage of global-scale data infrastructure has enabled cross-border economic activity, allowing small businesses to tap into traditionally inaccessible markets.

Digitisation of economies and international trade improve efficiency and increase productivity, by increasing access to information and enables markets to function more efficiently.[1]Already, global data flows have grown 45 times in the past decade. By 2025, it's estimated that 463 exabytes of data will be created each day, globally – that is more than the production of 2 million DVDs per day.[2]

At a time when data is contributing more to economic growth, it is imperative for member states to build a strong foundation of progressive data governance policies that are business-friendly while promoting secure cross border data flows. The failure to do so, will result in more cybersecurity attacks and breeches.

The COVID-19 endemic has also put data governance in the spotlight. With more countries in the region in varying levels of physical lockdowns, millions more citizens are taking to digital tools such as online learning, video conferencing and telemedicine. This places ever greater importance on data security and privacy protection. ASEAN leaders are rightfully focusing on these issues with ASEAN's Data Management Framework.

In 2018, ASEAN endorsed the Framework on Digital Data Governance. This framework aims to strengthen digital data collection and management capabilities of businesses to create trust in businesses' data management practices.[3] This framework is aimed at promoting effective data governance which ensures that data is consistent, trustworthy and does not get misused.

As such, this publication from the EU-ASEAN Business Council (EU-ABC) offers recommendations about Data Management and Data Classification. First, the larger issues of Data Governance are covered so that the core topic is understood in context. A key tenant of data governance is data classification. The paper argues that it is crucial for ASEAN to develop a coherent, transparent and consistent data classification framework which can promote interoperability across sectors. This will facilitate data to flow easily, efficiently and securely within and across multiple sectors. However, data classification is just the first step as it only sets a broad

[1] Joshua P. Meltzer & Peter Lovelock (2018), Regulating for A Digital Economy Understanding the Importance Of Cross-Border Data Flows In Asia, Global Economy and Development Working Paper 113, Brookings Institution, Available online: https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf Accessed 2 January 2020

[2] Desjardins, J. (2019) How Much Data is Generated Each Day? Weforum. Available: https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

[3] ASEAN Telecommunications and Information Technology Ministers Meeting (2018)

governing framework. Standards underpin such frameworks and ASEAN leaders need to work towards implementing **harmonised standards to govern cross border data flows.** The Council recognises that the principles in the European General Data Protection Regulation (GDPR) have not only influenced data regimes globally but also reflect principles that are shared by many systems around the world, while not prescribing technical standards.

At the overall legal and regulatory level an important business objective is to avoid wherever possible multiple compliance with conflicting regimes. As such, when **GDPR and local law requirements are compatible, the cost of compliance (while benefitting from good data governance regimes) is reduced.** This paper does not advocate for local laws to transform and mirror the GDPR. Instead, the Council recommends the implementation of local laws which ensures a level of protection comparable and compatible with the GDPR, thereby making it easier for companies to navigate between different systems, globally and in particular in the ASEAN region.

Technical standards are the next step in progressing towards this compatibility and the use of ISO standards is recommended.

But what continues to remain crucial is that **ASEAN member states need to permit secure cross border flows according to rules which are harmonised as much as possible.** This will not only promote intra-ASEAN trade but also trade and investments with key dialogue partners including the EU. **The Council encourages governments to design legal frameworks that facilitate data transfers in the regular course of business, while ensuring that such transfers take place with appropriate privacy and data security safeguards.** Privacy and security concerns are unlikely to be achieved by data localisation, but instead by actively taking advantage of leading technologies and harmonised intra-ASEAN cross border rules.

Framework On Digital Data Governance, ASEAN Secretariat, Available: https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf Accessed 19 December 2019

Overview of Recommendations

DATA GOVERNANCE IN ASEAN

SECURE CROSS BORDER DATA FLOWS

Recognise that data is the lifeblood of the new economy and data localisation policies do not support its growth. Instead, ASEAN leaders need to take advantage of leading security technology to promote secure cross border data flows based on harmonised norms which are compatible with GDPR.

TO BE GDPR COMPATIBLE

ASEAN to develop data frameworks compatible with GDPR where some elements are adopted to local law. When GDPR and local law requirements are compatible, the cost of compliance (while benefitting from good data governance regimes) will be reduced and the benefits of using data will be enhanced.

INTEROPERABLE DATA CLASSIFICATION FRAMEWORK

Data should be classified using the same tiers and standards across different sectors as far as possible, while recognising that certain sectors may have special requirements.

ISO STANDARDS

GDPR does not prescribe technical standards and the use of ISO standards is recommended in a harmonised way across the ASEAN region.

Detailed Recommendations

Promote Cross Border Data Flows

- **ASEAN member states need to permit cross border flows, according to rules which are harmonised as much as possible.** EU-ABC respects the need for special treatment of sensitive data but does not support data localisation. Instead, the Council encourages government to design legal frameworks that facilitate data transfers in the regular course of business, while ensuring that transfers take place with appropiate privacy and data security safeguards.
- **ASEAN member states permit secure flows of data across borders under harmonised norms, compatible with GDPR.**

Data Management

- **ASEAN to develop a coherent, transparent and consistent data classification framework which can promote interoperability across sectors.** This will facilitate data to flow easily, efficiently and securely within and across multiple sectors.
- **Setting Standards - Act Local, Think Global:** This hybrid Data Governance approach does not encourage ASEAN Member States to transform local law to become identical with GDPR. A case in point is Thailand, with its Personal Data Protection law coming into force partly in May 2019 and fully by May 2020. By September 2018, the revised draft approximated essential elements of the GDPR, including its provisions relating to the territorial scope of application. The council advocates for **ASEAN states to implement laws with comparable standards which are compatible with GDPR.**
- **Mandate companies to adhere to international standards:** GDPR does not prescribe specific technical standards and the use of ISO standards is recommended. Such consistent standards can help structure and categorise shared data sets.This will help businesses, especially SMEs build trust with different partners and stakeholders in the region.

1. Delivering Trusted Data in ASEAN

The world is experiencing an unprecedented increase in global data flows. Underpinned by the fourth industrial revolution, and the realisation that every sector (manufacturing, services, agriculture) relies on the ability to collect, use and disclose data according to predicable norms. Technology and regulatory advances such as heightened global connectivity and cloud services have enabled significant increases in cross-border economic activity, allowing all user groups: individuals, MSMEs, start-ups, corporates, government and civil society to gain access to global and previously untapped markets[4] and to interact, communicate and learn.

In turn, the impact of cross-border data flows on world GDP has surpassed that of global goods trade[5]. Over the last decade, global data flows (measured in zettabytes) has grown 45 times and projections suggest that cross-border data flows will further increase at a rate of 26% annually through to 2021[6]. By 2025, it is estimated that 463 exabytes of data will be created each day globally – that's the equivalent of 212,765,957 DVDs per day [7]. This growth in data flows contrasts the growth of traditional value flows of physical goods and services, which have barely managed to grow at the pace of worldwide nominal GDP[8]. By 2025, global data flows could account for $11 trillion of global GDP[9]. This means that cross border data flows are contributing more to economic growth and ASEAN is strongly following this trend.

Southeast Asia's internet economy continues to thrive and expand, soaring to US$100 billion for the first time in 2019, more than tripling in size over the last four years[10]. Driven by a rise in a tech-savvy middle-class population with greater access to the internet, Southeast Asians spend more time on the internet than do citizens in other parts of the world, including the United States[11]. In 2019, ASEAN's internet penetration rate stood at 65%. The region also has the third-largest number of mobile-phone users in the world and the fourth largest number of Internet and Facebook users[12]. The rate at which these users are coming online is also among the highest in the world, making ASEAN one of the most data-rich regions in the

[4] Joshua P. Meltzer & Peter Lovelock (2018), Regulating for A Digital Economy Understanding the Importance Of Cross-Border Data Flows In Asia, Global Economy and Development Working Paper 113, Brookings Institution, Available online: https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf Accessed 2 January 2020

[5] McKinsey Global Institute (2016), Digital Globalisation: The New Era of Global Flows, Available online: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx Accessed 2 January 2020 . MGI is relevantly 2016 – see use made of these materials in mid 2016 pp 16-17 https://pronto-core-cdn.prontomarketing.com/2/wp-content/uploads/sites/1871/2016/06/JFCCT-FORUM-BOOKLET-v1.9-1.pdf and also in 2018 https://pronto-core-cdn.prontomarketing.com/2/wp-content/uploads/sites/1871/2018/11/BOOKLET-DATA-PRIVACY-v-1.8-Rev-3a.pdf - see p.12

[6] ibid

[7] https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

[8] GSMA (2018) Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation Available online: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf Accessed 2 January 2020

[9] Crowell (2018) Benefits of APEC Cross-Border Privacy Rules Protecting Information, Driving Growth. Enabling Innovation, Available: https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf, Accessed 19 march 2010

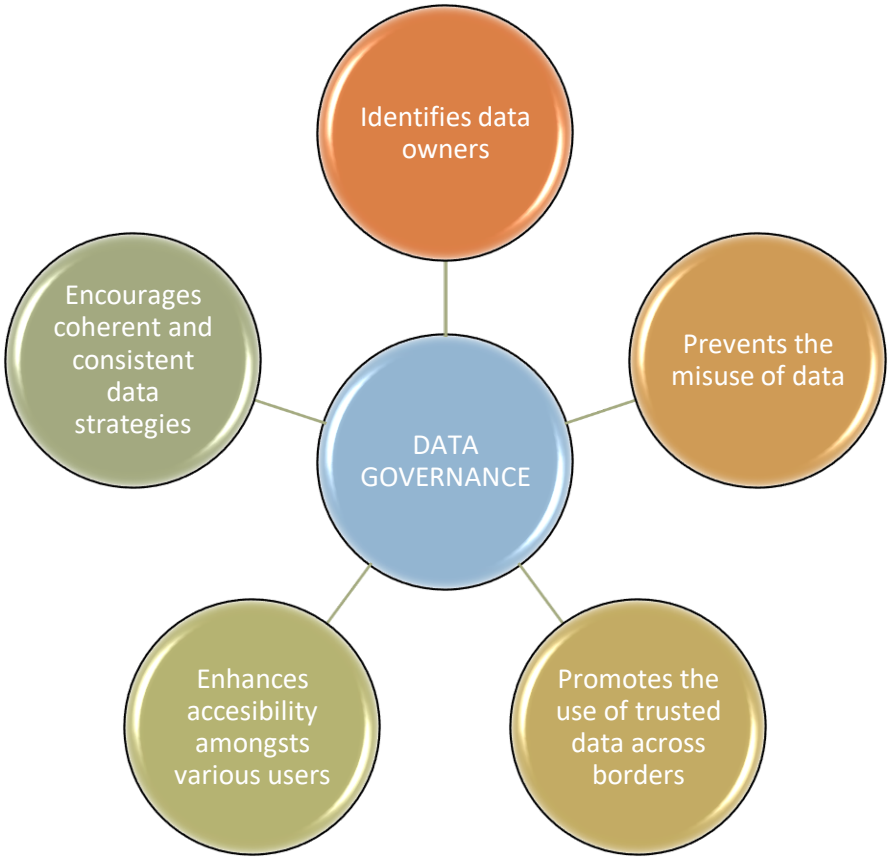
[10] Google, Temasek, Bain & Company (2019) e-Conomy SEA 2019, Available online: https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf Accessed 19 December 2019

[11] World Bank Group (2019) The Digital Economy in Southeast Asia : Strengthening the Foundations for Future Growth, World Bank, Washington, D.C, Available online: http://documents.worldbank.org/curated/en/389415587082677736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf Accessed 15 December 2019

[12] Vinayak HV, Fraser Thompson, and Oliver Tonby (2015) Understanding ASEAN: Seven things you need to know, McKinsey & Company, Available: https://www.mckinsey.com/industries/public-sector/our-insights/understanding-asean-seven-things-you-need-to-know Accessed 22 January 2020

world[13]. With the large volume of data reshaping ASEAN's consumer and trade patterns, data governance has become more important.

The EU-ABC uses 'Data Governance' to describe the norms, principles and rules governing various types of data. At a macro level (amongst economies), it is about cross-border data flows. At a micro level (in the enterprise, but also relevant to individual economies), it would be to ensure that high data quality exists throughout the lifecycle of the data. Thus it covers availability, usability, consistency, data integrity and data security and who is accountable to do what to ensure these things[14]. Transparent data governance frameworks and practices support better overall regulation and make it easier for businesses, especially MSMEs to understand what is happening to data and potential risks (e.g. leaks, potentially wrong business assessments, or cyber attacks).



Politically, data governance has also become more important with headline-grabbing data breaches, and cybersecurity attacks. Studies also show that gradually, more economies in Southeast Asia are being used as launchpads for cyberattacks, due to relatively weak security infrastructure where numerous computers can be infected easily for large-scale attacks[15]. ASEAN has become a 'prime target' for cyberattacks with Malaysia, Indonesia and Vietnam as hotspots for the launch of malware attacks[16].

In the name of national interest and security, some ASEAN leaders have resorted to data localisation measures. Data localisation requires the local storage and processing of data. Some regulators believe keeping data within borders will be more secure (see Annex), but it will lead to a reduction in economic competitiveness. Data localisation has been estimated to lead to declining investment in Indonesia and Vietnam, with exports from Indonesia expected

[13] Vidhya Ganesan (2018) How data-rich ASEAN can leverage this resource, Business Times, Available: https://www.businesstimes.com.sg/opinion/how-data-rich-asean-can-leverage-this-resource Accessed 22 January 2020

[14] Various sources – one is TechTarget which relies on industry consensus https://searchdatamanagement.techtarget.com/definition/data-governance

[15] AT Kearney (2019) Cybersecurity in ASEAN: An Urgent Call to Action, Available online: https://www.atkearney.com/documents/20152/989824/Cybersecurity+in+ASEAN.pdf/2e0fb55c-8a50-b1e3-4954-2c5c573dd121, Accessed 19 December 2019

[16] ibid

to fall by 1.7 percent[17]. Overall, data localisation inhibits innovation and cuts off access to (cloud based) digital services for smaller economies.

However, this needs to be considered EU-ABC recommends that policies should be centred on creating a regulatory structure which allows for innovation and growth with sufficient checks and balances to safeguard personal data but that unduly restricting cross border movement will be anti-innovative[18]. That said, just about all economies have restrictions on off-premises transfer of data in areas such as financial services, medical records and sometimes in national security matters.

Understanding the need to address these issues, ASEAN has put 'Digital Data Governance' in the spotlight. In 2018, ASEAN leaders signed the ASEAN Framework on Digital Data Governance[19]. 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.

In support of these principles, this paper will:

- Discuss EU-ASEAN growing trade relations and recommend that it is in ASEAN's interest to implement data privacy rules which are compatible with international norms e.g. GDPR
- Evaluate the different frameworks and agreements governing ASEAN's digital ecosystem and identify the opportunities and challenges in achieving these commitments.
- Provide an in-depth analysis on how ASEAN can address the above-mentioned gaps by harmonising with European data governance and management standards.
- Provide recommendations on how ASEAN can develop a coherent and consistent set of interoperable data classification standards.

[17] Meltzer, J. P., & Lovelock, P. (2018). Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia. *Global Economy and Development Working Paper*, *113*. Available: https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf

[18] Lee Chen Chen & Shangari Kiruppalini (2018) Red flags from Facebook data breach for ASEAN, The Straits Times, Available: https://www.straitstimes.com/opinion/red-flags-from-facebook-data-breach-for-asean Accessed 19 December 2019

[19] ASEAN Telecommunications And Information Technology Ministers Meeting (2018) Framework On Digital Data Governance, ASEAN Secretariat, Available: https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf Accessed 19 December 2019

2.ASEAN'S Privacy Regulations: Being GDPR Compatible for Business Fluidity

The European Union (EU) has been a strong supporter of ASEAN's economic development. The EU has consistently been the region's top investor with total investments amounting to US$30 billion in 2018. ASEAN has also exported over US$150 billion worth of goods and services to the EU, making the region ASEAN's second largest trade partner after China[20]. To deepen relations between the two economic blocs, the EU and ASEAN have agreed to take new steps towards resuming talks for a region-to-region agreement in March 2017 [21].

However, in some export-driven economies in ASEAN data protection standards are rather undeveloped as compared to key trading partners, such as Japan or the EU. Some countries are modernising their data protection framework (Thailand, Indonesia, Philippines, Malaysia, Singapore are reinforcing their data protection systems or implementing new ones). ASEAN is also working towards its own regional guidelines through the ASEAN Framework on Digital Data Governance.

More could be done to support the region, while ensuring more convergence with global standards. As the recent example of the EU-Japan cross-border data flows arrangement shows, this convergences in data protection standards pays off: it enabled the EU and Japan to put in place the world's largest area of free and secure data flows, thereby expanding the benefits of the free trade agreement agreed between the two parties .

The implementation of the European Union's General Data Protection Regulation (GDPR) in May 2018 has also introduced a modern data protection law with comprehensive (cross-sectoral) coverage and a broad scope of application[22]. GDPR applies to data processed by (1) organisations that are based in the EU, or **(2) organisations based outside the EU, that specifically target or monitor EU citizens.** The GDPR has several key elements that have contributed to global regulatory convergence in terms of data privacy, control, processing and cross-border data flows. As such, ASEAN businesses and their subcontractors will in any case have to apply GDPR regulations if they are offering goods or services to individuals residing in the EU or in other cases where the GDPR applies, in additional to compliance with relevant local laws (see Annex A).

Moreover, the EU has endorsed horizontal provisions for cross-border data flows and personal data protection in trade negotiations[23]. While these provisions have the objective to facilitate data flows and combat localisation measures, they preserve the ability of each Party to condition the flow of personal data upon the respect of certain guarantees of and safeguards. Depending on the level of data protection in ASEAN, there might be opportunities to complement bilateral trade agreements and the potential EU-ASEAN FTA with adequacy decisions under the GDPR that would expand the benefits of the trade agreements/FTA. As such, there is an urgency for businesses in Southeast Asia to incorporate GDPR to their day-to-day operations or risking losing out in US$17 trillion economy[24].

[20] Eurostat (2017) EU-ASEAN cooperation - key trade and investment statistics, Available: https://ec.europa.eu/eurostat/statistics-explained/index.php/EU-ASEAN_cooperation_-_key_trade_and_investment_statistics Accessed 27 January 2020
[21] ibid
[22] GDPR Art 3
[23] European Commission (2018) European Commission endorses provisions for data flows and data protection in EU trade agreements, available: https://ec.europa.eu/luxembourg/news/european-commission-endorses-provisions-data-flows-and-data-protection-eu-trade-agreements_fr Accessed 27 January 2020
[23] ibid
[24] European Commission (2018) Facts and Figures, Available: https://europa.eu/european-union/about-eu/figures/economy_en Accessed 27 January 2020

With companies such as Apple adopting GDPR standards globally, the GDPR is slowly becoming the global standard for privacy and data governance[25], promoting a degree of harmonisation and global convergence. Already, the GDPR is being used as the 'blueprint' for widespread data privacy law reform around the world, from Argentina to New Zealand, and Kenya to Thailand[26] (refer to figure 1). To be clear, EU-ABC is not recommending the adoption in local law of a GDPR equivalent but to implement laws with similar standards and compatibility.

Figure 1: ASEAN's GDPR Uptake

https://asialawportal.com/2019/07/19/asean-insiders-series-2019-personal-data-protection/

[25] Alan Beattie (2020) The Brussels Effect, by Anu Bradford, The Financial Times, Available: https://www.ft.com/content/82219772-3eaa-11ea-b232-000f4477fbca Accessed 27 January 2020

[26] Svantesson, D. J. B. (2019). Internet & Jurisdiction Global Status Report 2019. Available:https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf

3. ASEAN's Digital Ecosystem

ASEAN is the fastest growing Internet market in the world. With 125,000 new users coming onto the Internet every day, the ASEAN digital economy is projected to grow significantly, adding an estimated US$1 trillion to regional GDP over the next ten years [27].

But many significant roadblocks stand in the way of realising this potential. According to the Global Digitisation Index which measures a country's ability to reap the benefits of the digital economy, countries in Southeast Asia are in varying stages of development. Out of 100 countries surveyed, Singapore clinched the seventh position and Malaysia the 29th whereas Indonesia, Thailand and the Philippines did not make it to the top 50[28]. This disparity is caused by weak and unreliable telecommunications networks in rural Southeast Asia, which is stifling digitally enabled growth.

ASEAN has laid out important policy measures and frameworks, including, amongst others, the AEC Blueprint 2025, Masterplan on ASEAN Connectivity 2025, and the e-ASEAN Framework Agreement, to address these roadblocks and level the playing field. The table below highlights the various initiatives ASEAN has developed to bridge the digital divide in the region.

ASEAN's Digital Potential in Numbers

Brunei Population: 436.7 thousand
- Mobile Subscription: 566 thousand
- Smartphone Users: 131.9%

Cambodia Population: 16.4M
- Mobile Subscription: 19.5M
- Smartphone users: 119.5%

Indonesia Population: 268.2M
- Mobile Subscription: 355.5M
- Smartphone Users: 119.8%

Laos Population: 7M
- Mobile Subscription: 3.7M
- Smartphone Users: 51.9%

Malaysia Population: 32M
- Mobile Subscription: 40.2M
- Smartphone Users: 134.5%

Myanmar Population: 53.4M
- Mobile Subscription: 61.1M
- Smartphone Users: 113.8%

Philippines Population: 107M
- Mobile Subscription: 124.2M
- Smartphone Users: 110.4%

Singapore Population: 5.6M
- Mobile Subscription: 8.37M
- Smartphone Users: 145.7%

Thailand Population: 70M
- Mobile Subscription: 92.3M
- Smartphone Users: 180.2%

Vietnam Population: 96M
- Mobile Subscription: 143M
- Smartphone Users: 147.2%

[27] Singapore Business Federation (2019) Digitize ASEAN 2019 to Spur Closer Collaboration to Propel ASEAN's Digital Economy, Available: https://www.sbf.org.sg/digitize-asean-2019-to-spur-closer-collaboration-to-propel-asean-s-digital-economy Accessed 15 January 2020

[28] Noelia Cámara and David Tuesta (2017) DiGiX: The Digitization Index, Working Paper, BBVA Research, Available: ,file:///C:/Users/advoc/Downloads/03_DiGiX_methodology.pdf Accessed 15 January 2020

Table 1: List of Digital Policy Measures/Framework in ASEAN

Policy	Key Points	Issues to note
Framework on Digital Data Governance (2018)[29]	At the ASEAN TELMIN meeting in December 2018, the Ministers endorsed the ASEAN Framework on Digital Data Governance. The Ministers tasked the Senior Officials to further develop and implement the four strategic priorities under the Framework to enhance digital capability and cooperation among ASEAN Member States. 1. Data Life Cycle & Ecosystem (adequate protection for different types of data) ➢ **Deliverable: ASEAN Data Management Framework.** 2. Cross Border Data Flows (No unnecessary restriction on data flows) ➢ **Deliverable: The ASEAN Cross-Border Data Flows Mechanism** 3. Digitalisation and Emerging Technologies (building data capacity) ➢ **Deliverable: The ASEAN Digital Innovation Forum** 4. Legal, Regulatory and Policy (harmonised legal regulatory landscape in ASEAN, including personal data protection) ➢ **Deliverable: The ASEAN Data Protection and Privacy Forum**	1. A step in the right direction for ASEAN, which highlights the importance of coordinating policy and regulatory measures to facilitate cross-border data flows. 2. However, the framework is non-binding and set outs broad guiding principles. 3. Light on specifics of what the standards will entail / what specific compliance measures would be necessary.

[29] ASEAN Telecommunications And Information Technology Ministers Meeting (2018) Framework On Digital Data Governance, ASEAN Secretariat, Available: https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf Accessed 19 December 2019

Policy	Key Points	Issues to note
ASEAN Agreement on Electronic Commerce (2018)[30]	Endorsed on 12 Nov 2018, on the side-lines of the 33rd ASEAN Summit and Related Meetings. It provides the starting point for new discussions on e-commerce and digital trade. 1. The agreement is meant to be monitored by the Senior Economic Officials (SEOM) and carried out by the ASEAN Coordinating Committee on Electronic Commerce (ACCEC) which will ensure coordination with other ASEAN entities. 2. Similar to the e-ASEAN framework in 2000, but with more detailed provisions regarding data localisation and cross-border data transfer issues. 3. Recognises technology neutrality 4. Includes a clause to review the agreement within three years	1. Most of the agreement remains at the level of cooperation, but ACCEC is charged with implementing proposals – a sign of accountability 2. Vietnam exempted itself from time delays in this document. While Cambodia, Lao PDR and Myanmar all received additional time for implementation of some provisions, Vietnam did not.
ASEAN Digital Integration Framework / Digital Integration Framework Action Plan 2019-2025[31]	This digital framework aims to accelerate a coordinated, regionally integrated digital economy. Priority Areas: 1. Facilitate seamless trade. 2. Protect data while supporting digital trade and innovation. 3. Enable seamless digital payments. 4. Broaden digital talent base 5. Foster entrepreneurship	1. Big-picture framework that integrates existing frameworks and plans like the Personal Data Protection framework, the ICT Masterplan 2020 etc. into a broader plan for digitalisation 2. Under Vietnamese 2020 Chairmanship, ASEAN is to develop a Digital Integration Index to monitor and improve the key areas under the Framework to advance an agenda of digital integration.

[30] ASEAN Coordinating Committee on Electronic Commerce (2018) ASEAN Agreement on E-commerce, ASEAN Secretariat, Available: https://static1.squarespace.com/static/5393d501e4b0643446abd228/t/5c99e02aeef1a10aa126c9a6/1553588313303/20190306035048.pdf Accessed 20 January 2020

[31] ASEAN Digital Integration Framework (2019), ASEAN Secretariat, Available: https://asean.org/storage/2019/01/ASEAN-Digital-Integration-Framework.pdf Accessed 15 January 2020

Policy	Key Points	Issues to note
Framework on Personal Data Protection 2016[32]	An ASEAN Framework on Personal Data Protection was adopted in November 2016, establishing a set of principles to guide the implementation of measures at both national and regional levels to promote and strengthen personal data protection in the region. Principles 1. **Consent, Notification and Purpose** An organisation should not collect, use or disclose personal data about an individual unless the individuals has been notified/given consent 2. **Accuracy of Personal Data** The personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal data is to be used or disclosed. 3. **Security Safeguards** The personal data should be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks. 4. **Access and Correction** Upon request by an individual, an organisation should provide the individual access to his/her personal data 5. **Transfers to Another Country or Territory** Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the	1. Framework does include exemption caveats (Paragraph 16) that are concerning. In other words, ASEAN Member States can unilaterally decide not to apply the Framework for almost any area or activity. 2. The challenge in creating the ASEAN wide Framework on Personal Data Protection is that not all member-states have privacy regimes in place or laws. 3. Singapore (Personal Data Protection Act 2012), Malaysia (Personal Data Protection Act 2010), Indonesia (Law of the Republic of Indonesia Number 11 of 2008), Philippines (Data Privacy Act of 2012) and Vietnam (Law on Protection of Consumers' Rights 2010). 4. Thailand Personal Data Protection Act 2019, while other states in the region such as Indonesia are in various stages of developing their own data protection and data privacy laws.

[32] ASEAN Telecommunications And Information Technology Ministers Meeting (2016) Framework On Personal Data Protection, ASEAN Secretariat, Accessed: https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf Accessed 10 January 2020

	overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles 6. **Retention** An organisation should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes. 7. **Accountability** An organisation should be accountable for complying with measures which give effect to the Principles.	
ASEAN ICT Master Plan 2016-2020 (drafted circa 2015)[33]	ASEAN ICT Masterplan 2020 was launched at the 15th ASEAN Telecommunications and IT Ministers (TELMIN) in Danang, Viet Nam in November 2015. It is being implemented in the period 2016-2020. The vision for the AIM 2020 is to propel ASEAN towards a digitally enabled economy that is secure, sustainable, and transformative; and to enable an innovative, inclusive and integrated ASEAN Community.	1. Sets out clear targets, initiatives, outcomes and timeline. 2. Build on the 2000-2015 Masterplans where ASEAN leaders have delivered on endorsing a Personal Data Protection framework.

[33] ASEAN Telecommunications and IT Ministers (2015) The ASEAN ICT Masterplan 2020, ASEAN Secretariat, Available: https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf Accessed 5 Janury 2020

4.Data Classification – Just the First Step

Globally, governments have developed data privacy frameworks that can effectively protect the data of their citizens, while also allowing data to flow across borders in ways that support trade and innovation. These include the Organisation for Economic Cooperation and Development (OECD) Privacy Framework, the European Union's General Data Protection Regulation (GDPR) and the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR).

The OECD adopted the voluntary guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data in 1980 and revised in 2013 in response to growing concerns about information privacy and data protection in an increasingly interconnected world[34]. These guidelines apply to personal data both in the public or private domain. They are often regarded as the minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Developed by the 21 economies from AEPC, the CBPR system is a voluntary, principles-based framework which allows for the transfer of personal data across participating economies which have formally joined. The APEC Privacy Framework features nine high-level information privacy principles. These principles largely resemble those found in the OECD Guidelines. It does not displace or change a country's domestic laws and regulations. However, if there are no applicable domestic privacy protection requirements in a country, the CBPR system is intended to provide a minimum level of protection. Thus, the CPBR system attempts to solve the problem of non- or variable-adoption of the Privacy Framework within the APEC region by imposing a minimum standard for data privacy on all CBPR compliant data controllers[35].

Unlike the OECD guidelines and APEC's CBPR certification, GDPR has the status of enforceability and failure to comply, could result in fines. Examples of these companies which may be regulated by GDPR standards include[36]:

- E-commerce businesses that offer goods or services through their platforms to EU individuals (particularly if the website publishes the price of products or services in Euros or EU currencies);
- Hotels that operate websites that specifically target individuals in the EU (in European languages, with their room rates in Euros or EU currencies);
- Data analytic companies, insurance companies, social media platforms, gaming companies collecting data and monitoring or creating profiles of individuals in the EU;
- Organisations that use web-tracking, and are collecting data via cookies or social plug-ins from individuals in the EU;
- Organisations that receive EU personal data transferred from their European parent/holding companies.

As such, the following section of the report explores:

- How ASEAN can partially adopt and adapt European standards into personal data frameworks to promote compatibility with GDPR?

[34] OECD (2013) The OECD Privacy Framework, Available: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, Accessed 19 March 2020

[35] Crowell (2018) Benefits of APEC Cross-Border Privacy Rules Protecting Information, Driving Growth. Enabling Innovation, Available: https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf, Accessed 19 march 2010

[36] Singapore Legal Advise (2018) GDPR Compliance in Singapore: Is it Required and How to Comply, Available: https://singaporelegaladvice.com/law-articles/GDPR-Compliance-Singapore-Required/ Accessed 18 December 2019

- How ASEAN can use the ASEAN Framework on Digital Data Governance to develop an ASEAN wide approach on data classification, which applies to all companies, including MSMEs?

Data classification is broadly defined as the process of organising data by relevant categories so that it may be used and protected more efficiently [37]. The classification process makes data easier to locate and retrieve, while eliminating multiple processing of the same information. Data classification is especially important when it comes to risk management, compliance, and managing data security[38].

It is crucial that **ASEAN develops a coherent, transparent and consistent data classification framework to promote interoperability across sectors**. Classification should include an "outcomes-based" cyber risk management approach. Data should be classified using the same tiers and standards across different sectors as far as possible, while recognising that some certain sectors may have special approaches.

[37] Juliana De Groot (2015) What is Data Classification? A Data Classification Definition, Digital Guardian, Available: https://digitalguardian.com/blog/what-data-classification-data-classification-definition Accessed 18 December 2019
[38] Ibid

Table 2: Summary of how European Companies in ASEAN classify data

Confidential Data

- **Examples:** Commercially sensitive information, customer information (name, address, health information, income) financial data, personal data, and data protected by confidentiality agreements.

Access: Restricted to a minimum number of individuals on a need to know basis only. Non-disclosure agreements are required for access by external parties for business reasons.

Storage: Adequate safety and security measures for controlled environments must be in place when storing information, e.g. strict access restrictions, Multi-Factor Authentication, locked cabinets, password protection and encryption where appropriate, or other equivalent secure protection measures. Confidential information stored on removable media must be encrypted on the device. A clear desk policy applies for confidential information in physical format: it must be locked away when not in active and constant use.

Private Data

- **Examples:** Financial reports, marketing strategies, project plans, policies, business continuity plans.

Access: Restricted to company employees and authorised external workers for use within the company. Non-disclosure agreements are required for access by external parties for business reasons.

Storage: Internal and other non-public Business Information is stored, transmitted or processed within controlled environments where there are adequate security measures in place. Controlled environments include managed cabinets, digital services, devices as well as on premise, off-premise or outsourced environments under the company's purview.

Public Data

- **Examples:** Press releases, research publications, company addresses, continuity plans.
- **Access:** Unrestricted access for individuals.
- **Storage:** Public information posted electronically inside or outside of a company should be transmitted in a format and with technical safeguards that ensure its integrity and protect it from unauthorised or undetectable modification.

The classification presented above defines main categories from which the way data is handled in the within a company. However, data classification is just the first step of the data lifecycle. ***Data life cycle*** refers to the collection, storage, usage, disclosure and disposal of data. Data classification simply provides a filter and starting point of how data should be managed. ASEAN leaders need to do more to ensure data is protected at every stage of the data lifecycle. Ultimately, it is about the treatment and management of data.

4.1 Technical Standards to Protect Data Through its Lifecycle

Below is a table outlining the different stages and ISO standards which companies can refer to when managing internal and external data. Although this report argues that GDPR is fast becoming a global standard for personal data protection, the Council recognises that it does not have sufficient technical obligations on data security and data management[39]. For example, the GDPR speaks frequently of 'privacy by design' without substantiating what it might actually look like in the day-to-day functioning of a company In this regard, **ISO standards can provide clear, comprehensive and transparent framework on how to minimise security risks that might lead to security incidents.**

[39] Middleton-Leal, M.(2018) GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?, Available https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/

Table 3: Suggested Data Management Steps & Standards

STEP	DETAILS	SUGGESTED STANDARDS
Identify Data Owners	Data Owners may sit somewhere else within the organisation either as a data producer or as a data consumer. Once identified, commence data classification process.	**Integrated framework based on international standards:** This approach provides a consistent, secure service which meets customer and regulatory requirements. • ISO/IEC 9001 Quality Management System • ISO/IEC 27001 Security Management System • ISO/IEC 22301 Business Continuity Management System • BS 10012 Personal Information Management System • ISO/IEC 20000 Service Management • ISO/IEC 27018: ISO 27018 Code of practice for personally Data protection • ISO/IEC 19845:2015 Universal data structuration Framework • ISO/IEC 29100 – Privacy Framework • ISO/IEC 29134 – Privacy impact assessment • ISO/IEC 27701- Privacy information management system.
Assess data vulnerabilities/risks	Perform a risk assessment and consider the vulnerabilities that are attributed to each Data Asset Potential security issues to consider: • data control • data encryption • blending of data with other customer data • mitigation process if a security breach does occur or if data is damaged or destroyed	
Audit logs	To maintain confidentiality and integrity of classified/restricted data a strict audit logging process is to be undertaken. This audit log must be carefully designed to ensure it can provide a 'trail of evidence' which can be used to investigate inappropriate or illegal access.	
Data Retention and Deletion	Hard drive degaussing exposes equipment to a powerful magnetic field, destroying hard drives or media tapes. Wiping hard drives useful for businesses that have off-lease equipment or hard drives for reuse. Manually deleting and manufacturer's reset.	

5.Towards A Data Centric ASEAN

In conclusion, the EU-ABC encourages a flexible and sector-wide approach in recommending some areas for consideration as ASEAN and its Member States may look to develop their data governance and data management frameworks:

1. Offer Clarity and Consistency to promote interoperability across sectors: Data should be classified using the same tiers and standards across different sectors. This will facilitate data to flow easily, efficiently and securely within and across sectors. Classification consistency will ultimately contribute to export and economic growth. Internationally, interoperable approaches can help unleash the economic and social potential of data while effectively protecting privacy, intellectual property.

2. Setting Standards - Act Local, Think Global: This hybrid Data Governance approach does not necessarily encourage ASEAN Member States to transform local law to become identical with GDPR. A case in point is Thailand, with its Personal Data Protection law coming into force partly in May 2019 and fully by May 2020. By September 2018, the revised draft approximated key elements of the GDPR, including its territorial scope provisions (Art 3 /s.5) and the requirement for representatives, something which will surely add to overhead. Besides, it advocates for ASEAN states to implement laws with similar standards and compatibility and contribute to convergence in data protection in the region and globally.

3. Promote cross border data flows: ASEAN member states permit secure flows of data across borders under harmonised norms, compatible with GDPR. This will avoid productivity loss to the detriment of the ASEAN competitiveness. Privacy and security will not be achieved by data localisation, but instead by putting in place common transfer tools (e.g. model contractual clauses) to facilitate free and secure transfers including for small and medium businesses, by actively maintaining data and taking advantage of such harmonised norms and the use of leading security technologies.

4. Using a Multi-Stakeholder Model (MSM) of governance: Such an approach is reflected in the various roles (e.g. data processor, data owner, data custodian) in data protection laws which use GDPR principles and concepts, and which support non-government user groups being part of oversight of data protection commissions and the like, and in well-developed Cybersecurity laws.

5. Mandate companies to adhere to international standards: Where businesses have not employed basic data governance principles, the EU-ABC encourages the use of international best practice standards e.g. ISO 27002/ BS 10012. Consistent standards can help structure and categorise shared information environments and data sets, including organising and labelling categories of data sets to support usability, findability and traceability. This will help businesses, especially SMEs build trust with different partners and stakeholders in the region.

6. Recognise that there are different types of data: There are multiple types of data which are collected and used, and their purpose and value differ substantially. Without recognising these different kinds of data, businesses will not be able to effectively address issues such as personal data protection or competition.

Annex A: Country Studies of Data Localisation in ASEAN Member States

All economies have some restrictions on sensitive data (e.g. medical records, financial records, national security information). Data Localisation is a set of requirements that any processing of data must be done in the subject economy and is not to be disclosed cross border. EU-ABC respects the needs for special treatment of sensitive data but does not support data localisation.

The following section gives an overview of data localisation policies and its stamping in the individual ASEAN Member States. Details concerning individual economies are briefly explained below.

Type I: Forced Local Data Storage[40]	*Type III: Some Restrictions on Data Transfers*	*No Data Localisation Laws*[41]
Vietnam	Malaysia	Cambodia
Brunei	Singapore	Laos
	Thailand	Myanmar
	Indonesia	Philippines

Brunei Darussalam

Negara Brunei Darussalam demands strict data localisation requirements, data to be saved and processed on servers within the borders of the country [42]. Companies must store information in the territory of Brunei[43].

Cambodia

A comprehensive policy on protection and processing of personal data does not exist. No forced data localisation laws are published within the Kingdom of Cambodia. Thus, foreign investors and IT providers do not have to follow specific requirements.

Indonesia

A new regulation in October 2019 replaced the old data localisation regulation. Private companies need not store their data locally; companies handling 'strategic electronic data' in eight sectors including food, transport, healthcare and defence may need to connect their data to an unspecified 'data centre' in the event of an incident that must be reported to the cyber security authority[44]. Another Personal Data Protection Bill is still being drafted[45]. As of 2018, there were proposals to

[40] Liu, H. W. (2018) Data Localisation and Digital Trade Barriers: ASEAN in Megaregionalism. ASEAN Law in the New Regional Economic Order: Global Trends and Shifting Paradigms, Cambridge University Press (Pasha L. Hsieh & Bryan Mercurio eds. 2019

[41] Graham Greenleaf (2014). Asian Data Privacy Laws: Trade & Human Rights Perspectives. Oxford University Press

[42] Albright Stonebridge Group (2015) Data Localisation: A Challenge to Global Commerce and the Free Flow of Information, Available online: https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf Accessed 20 December 2019

[43] Business Roundtable; (2012) Promoting Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements, Press Release, p. 5

[44] Daniel Pardede (2019) Indonesia: New Regulation on Electronic System and Transactions, Baker McKenzie ,Available: https://www.bakermckenzie.com/en/insight/publications/2019/10/new-regulation-electronic-system-and-transactions Accessed 20 December 2019

[45] Teresa Umali (2019) Indonesia drafts Personal Data Protection Act, OpenGov, Available: https://www.opengovasia.com/indonesia-drafts-personal-data-protection-act/ Accessed 20 December 2019

require that countries receiving data being transferred out of Indonesia must have data protection laws at least as strong as those in the proposed bill[46].

Lao PDR

Regarding the Lao People's Democratic Republic, there are recently no policies on data storing within the borders or forced localisation. But several policies are under revision focusing on new laws need to be introduced to enable future trade initiatives.

Malaysia

Malaysia has a whitelist of countries which can receive data coming out of Malaysia, including the EEA and countries recognised by the European Union under the Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) [47].

Myanmar

Currently, there are no laws concerning the data localisation topic available in Myanmar and no plans on draft regulations are published. Only legislations affecting certain personal data, but no comprehensive data privacy policy is in force.

Philippines

The Data Privacy Act of 2012 was signed in August 2012. The Act has similarities to the EU Data Protection Directive as well as the principles and requirements set out in the Asia-Pacific Economic Cooperation Privacy Framework. The law has much higher penalties and treatment for sensitive personal information but does not include prohibitions on cross border data transfers. The Philippine government uses this Act to protect the fundamental human right of privacy while ensuring the free flow of information to promote innovation and economic growth.

Singapore

Singapore's Personal Data Protection Act (2012) mandates that countries receiving data from Singapore have data protection standards at least as strong as Singapore's[48]. Organisations are required to take steps to ensure that the recipient is bound by legally enforceable obligations to provide a standard of protection that is comparable to that under the PDPA. This include contract, consent, binding corporate rules, certification, or any other legally binding instruments.

[46] Mark Innis (2019) Indonesia: Government Pushes Draft Data Protection Law, Baker McKenzie, Available: https://www.bakermckenzie.com/en/insight/publications/2018/05/government-pushes-draft-data Accessed 20 December 2019

[47] Malaysian Department Of Protection Of Personal Data (2017) Available: www.pdp.gov.my/images/pdf_folder/PUBLIC_CONSULTATION_PAPER_1-2017_.pdf Accessed 20 December 2019

[48] Singapore Statues Online (2012) Personal Data Protection Act 2012, Available: https://sso.agc.gov.sg/Act/PDPA2012#pr26- Accessed 20 December 2019

Thailand

Thailand passed a Personal Data Protection Act effective May 2019 and May 2020[49]. It requires that data disclosed cross border meet data protection standards at least as strong a standard as Thailand's or otherwise set by the relevant Thai agency[50]. It is similar to Singapore and the GDPR in that sense.

Vietnam

As of October 2019, only companies whose services have been used to violate Vietnamese law and fail to take measures to stop such violations will be subject to data localisation laws[51].

Note: All economies have restrictions on disclosure for certain sensitive data. Thus, financial information, medical records and sometimes national security data must be maintained on in-premises servers.

[49] Dhiraphol Suwanprateep, Pattaraphan Paiboon, Kritiyanee Buranatrevedhya and Jenjira Yanprasart (2019) The First Thailand Personal Data Protection Act Has Been Passed, Baker McKenzie, Available: https://globalcompliancenews.com/first-thailand-personal-data-protection-act-has-been-passed-20190401/ Accessed 20 December 2019

[51] Rajah & Tann LCT Lawyers (2019) Data localisation requirements narrowed in Vietnam's cybersecurity law, *The Business Times.* Available: https://www.businesstimes.com.sg/asean-business/data-localisation-requirements-narrowed-in-vietnams-cybersecurity-law Accessed 20 December 2019

About the EU-ASEAN Business Council

The EU-ASEAN Business Council (EU-ABC) is the primary voice for European business within the ASEAN region. It is formally recognised by the European Commission and accredited under Annex 2 of the ASEAN Charter as an entity associated with ASEAN.

Independent of both bodies, the Council has been established to help promote the interests of European businesses operating within ASEAN and to advocate for changes in policies and regulations which would help promote trade and investment between Europe and the ASEAN region. As such, the Council works on a sectorial and cross-industry basis to help improve the investment and trading conditions for European businesses in the ASEAN region through influencing policy and decision makers throughout the region and in the EU, as well as acting as a platform for the exchange of information and ideas amongst its members and regional players within the ASEAN region.

The EU-ABC conducts its activities through a series of advocacy groups focused on particular industry sectors and cross-industry issues. These groups, usually chaired by a multi-national corporation, draw on the views of the entire membership of the EU-ABC as well as the relevant committees from our European Chamber of Commerce membership, allowing the EU-ABC to reflect the views and concerns of European business in general. Groups cover, amongst other areas, Insurance, Automotive, Agri-Food & FMCG, IPR & Illicit Trade, Market Access & Non-Tariff Barriers to Trade, Customs & Trade Facilitation and Pharmaceuticals.

Executive Board

The EU-ABC is overseen by an elected Executive Board consisting of corporate leaders representing a range of important industry sectors and representatives of the European Chambers of Commerce in South East Asia.

Membership

The EU-ABC's membership consists of large European Multi-National Corporations and the eight European Chambers of Commerce from around South East Asia. As such, the EU-ABC represents a diverse range of European industries cutting across almost every commercial sphere from car manufacturing through to financial services and including Fast Moving Consumer Goods and high-end electronics and communications. Our members all have a common interest in enhancing trade, commerce and investment between Europe and ASEAN.

To find out more about the benefits of Membership and how to join the EU-ASEAN Business Council please either visit www.eu-asean.eu or write to info@eu-asean.eu .

Issued by the EU-ASEAN Business Council
April 2020

19/F Singapore Land Tower
50 Raffles Place
Singapore 048623

info@eu-asean.eu