Deloitte.

Data and privacy protection in ASEAN

What does it mean for businesses in the region?

2018

Data and privacy protection in ASEAN – what does it mean for businesses in the region?

Written by Mr THIO Tse Gan, Cyber Risk Leader, Deloitte Southeast Asia

ASEAN has a population of 634 million, a combined GDP of US$2.55 trillion reported in 2016 and is currently the sixth largest economy in the world with total trade amounting to US$3.7 trillion. The region's forecasted annual growth of five per cent sets expectations that it will become the fourth largest economy by 2030. These numbers portray a region that is full of potential. The ASEAN Economic Community (AEC), established in 2015 will allow businesses to capitalize on opportunities in the region as an integrated market with a market reach of over 600 million instead of 10 fragmented economies and lesser impact.

With the AEC in motion, the region is now working towards a new vision - ASEAN 2025: Forging Ahead Together. ASEAN 2025 is a forward looking roadmap that articulates ASEAN goals and aspirations to realise further consolidation, integration and stronger cohesiveness as a community – collectively working towards becoming "politically cohesive, economically integrated, and socially responsible".

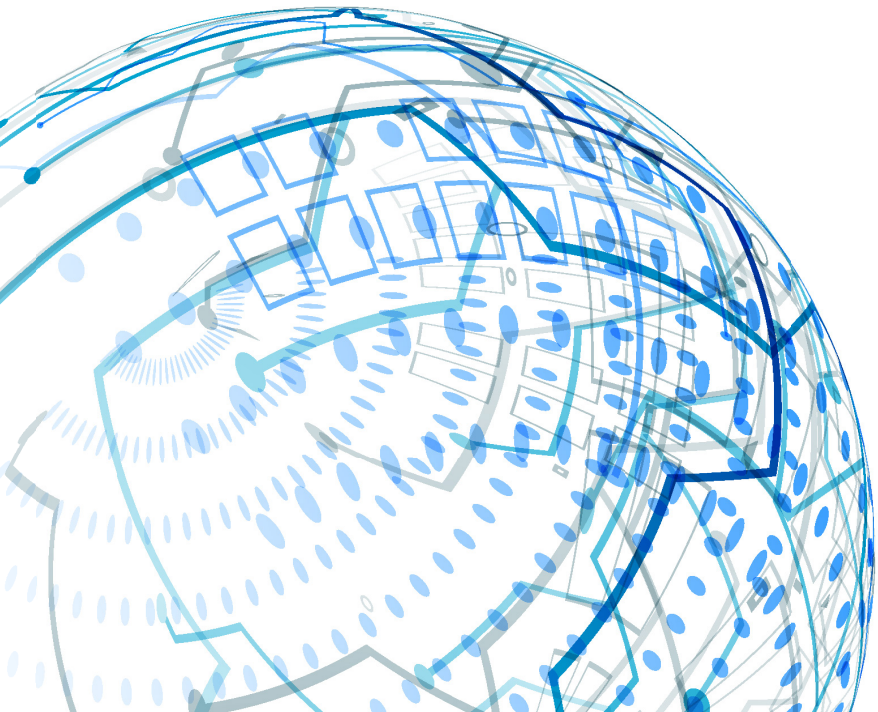
Digital technology has been recognised as being key in achieving this bold 2025 vision. An estimated $5.3 trillion[1] of global trade pass through ASEAN's waterways each year, and Internet and mobile penetration is one of the highest in the world - at about 80 percent of population using the internet and 100 percent ownership of mobile phones. This goes to show that the people in ASEAN are nearly ready to embrace the new economy[2].

In September 2016, a Master Plan on ASEAN Connectivity 2025 (MPAC 2025) was developed to address this digital technology aspect of the 2025 vision focusing on five strategic areas: sustainable infrastructure, digital innovation, seamless logistics, regulatory excellence and people mobility.

At individual government levels, the interest in harnessing digital technology is clear. Malaysia has set up the world's first Digital Free Trade Zone in 2017; Thailand has a multi-year blueprint to develop digital capabilities in all sectors of the economy, while Indonesia is focusing its attention on helping its SMEs digitise their operations. Singapore has a Smart City initiative and Vietnam has been busy investing in digital infrastructure[3].

Opportunities abound for Southeast Asia in digital technology. To put it in context, Southeast Asia is the world's fastest growing Internet region with nearly four million new users coming online every month over the next five years. This translates into a user base of 480 million by 2020. There are over 700 million active mobile connections in Southeast Asia. Online spending is expected to reach US$ 200 billion by 2025. This means that there will be a flourishing digital economy if every one of the 480 million unique users and 700 mobile devices[4] are secure and cross-border transactions are not hijacked by hackers.

[1]https://www.jpmorgan.com/country/US/EN/cib/investment-banking/trade-asean-future
[2]https://www.straitstimes.com/business/invest/compelling-case-for-investing-in-asean-region
[3]https://www.straitstimes.com/opinion/asean-needs-to-fix-its-digital-divide
[4]https://www.businesstimes.com.sg/asean-business/aseans-digital-economy-key-to-unlocking-growth



Addressing the risks

From a cyber risk perspective, the importance of data security and privacy cannot be further emphasised in the face of such staggering numbers and potential socio-economic impact. 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[5].

In April 2017, the ASEAN leaders issued a statement on cyber security cooperation in addition to ongoing efforts to foster regional cyber security cooperation such as the ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), the ASEAN Ministerial Conference on Cybersecurity (AMCC) and the ASEAN Cyber Capacity Programme (ACCP). An outcome from these platforms is Singapore setting aside S$10 million for the ACCP to build technical capability among incident responders and operations in the region[6].

Here is a glance at the data and privacy laws of the 10 ASEAN members so far:

- Brunei Darussalam – There is no comprehensive law on data protection at the moment but the country has been guided by a Data Protection Policy since 2014. This policy covers personal data (in electronic or manual form) maintained by government agencies and educational institutions.
- Cambodia – The Ministry of Post & Telecommunication ICT License (Article 27) states that "all ICT & Telecommunication operators and all relevant person must protect personal information, security, and safety of using their ICT & Telecommunication System "
- Indonesia – The Ministry of Information and Communication Regulation No.20/2016 details more comprehensive regulation on Personal Data Protection. Law No. 11 of 2008 regarding Information and Electronic Transaction and Government Regulation No. 82 of 2012 regarding the Provision of Systems and Electronic Transactions ("PP 82/2012") has also been enhanced.
- Lao PDR – There are no plans by the Lao People's Democratic Republic to legislate a statute on privacy and data protection but the Law on Protection of Electronic Data (2017) and the Law on Prevention and Combating Cyber Crime (2015) relate to the protection of personal information.
- Malaysia – Malaysia is currently enforcing the Personal Data Protection Act 2010 (PDPA) through its Personal Data Protection Department.

- Myanmar – In March 2017, Myanmar promulgated a 4-page law entitled Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017). According to the unofficial translation of the law[7] by the Myanmar Center for Responsible Business (MCRB), the law explicitly prohibits interception of a citizen's electronic communications, private correspondences and, physical privacy, unless otherwise warranted by an "order".
- Singapore – The Personal Data Protection Act 2012 (PDPA) has been in force since 2014, and is being implemented by the Personal Data Protection Commission.
- Thailand – The Notification of the Electronic Transaction Committee on Policies and Practices for the Protection of Personal Information of Government Agencies BE 2553 (2010) and the Information Act for Public Sector BE 2540 (1997) protect its citizens' personal information that are being processed by state agencies. The Personal Data Protection Act is under development and expected to be published soon.
- Vietnam – The most comprehensive legal framework on data protection is the Law on Cyber Information Security (Law No. 86/2015/QH13) (the "LCIS").
- Philippines - The Data Privacy Act was passed in 2012, "to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth." (Republic Act. No. 10173, Ch. 1, Sec. 2). This privacy law also established a National Privacy Commission to enforce and oversee it as well as giving it rule making power. Final implementation rules and regulations came into force in September 2016, given the Privacy Act specificity.

[5]http://asean.org/storage/2012/05/TELMIN-16-JMS-Final-cleared.pdf
[6]https://www.opengovasia.com/articles/asean-leaders-issue-statement-on-cybersecurity-cooperation
[7]http://www.myanmar-responsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf

While ASEAN continues to build momentum to protect the data and privacy of its more than 600 million citizens, the European Union, a similar regional organisation construct, has passed the General Data Protection Regulation (GDPR) made effective on 25 May 2018. The GDPR provides a set of standardised data protection laws across its 28 member countries for EU so that citizens can understand how their data is used. The GDPR not only gives EU citizens control over their personal data, it also simplifies the regulatory environment for international businesses by unifying the regulation within the EU. Herein lies the difference between the EU and ASEAN - while the EU has a parliament with the power to legislate, ASEAN has the ASEAN Inter-Parliamentary Assembly with the power of persuasion. Nonetheless, the GDPR is great news for ASEAN in many ways in terms of data and privacy protection. Celebrating 40 years of ASEAN-EU relations last year, the EU is ASEAN's second largest trading partner and the largest provider of Foreign Direct Investments. Most significant of all is the estimated seven million EU citizens that travel to ASEAN countries each year[8]. This means that many organisations within the ASEAN would be required to be compliant with the GDPR. In addition, the EU and ASEAN launched two flagship programmes in April 2018 on policy dialogue and regional economic integration with an overall budget of EUR 61 million to support the ASEAN integration process. These translate to a great deal of support for ASEAN to protect its digital economy.

What does this all mean to businesses in ASEAN?

Globalisation and digitalisation have become a double-edged sword as businesses attempt to comply with data protection regulations in a borderless internet world. As small projects and startups gather steam through large funding to disrupt industries, cyber security needs to be built into every business' DNA. Businesses should also set up checks and controls in order to be compliant to the growing lists of regulations around data protection and privacy.

No doubt regulations are not predictive and cannot address every new technological risk or weakness that can be exploited by cyber actors. The GDPR is a great reference tool for businesses to develop solid data protection programmes, thereby creating a robust ecosystem for the future digital economy.

[8]https://eeas.europa.eu/headquarters/headquarters-Homepage/30722/eu-asean-relations-factsheet_en

Start with asking if you know the answers to the following questions:

01. Where is your business operating today?
02. What data does your business collect?
03. Where does your data reside?
04. Where do your customers reside?
05. What are the data protection and privacy regulations in the countries of all the above?
06. What is your business roadmap in the next 5 years?

To help you consider your data protection and privacy:

1. New Data Subject Rights – especially data portability

The GDPR gives every individual the right to access their personal data on request, request a rectification to inaccurate data and object to the processing of their data and more. In this case, your company must have the ability to provide your customer with a copy of all the personal data that you have regarding them; and the ability to transfer that data to another data controller or service provider at their request.

This can lead to more competition as preferred services will have the advantage of retaining the customer's data. Thus, businesses need to rethink their business strategy in terms of customer experience to service value, and change their approach towards compliance by being customer-centric.

2. Extraterritorial applicability of the GDPR

The EU privacy rules now apply to businesses outside the EU, if these businesses process the data of individuals from the EU. For example, any organisation outside of the EU selling goods or services online to EU citizens will require their data to be processed.

Because this can apply to social networks and apps as well, the approach ensures the highest level of data protection.

3. Maintaining records of processing activities

A full overview of the processing activities that take place within an organisation is required and these activities are required to be documented accordingly. The breadth and depth of this requirement demands a proactive and collaborative approach from within organisations. To be successful, business units need to be involved in designing a process with clear roles and responsibilities, and a central register for the records. The added benefits as a result may be streamlined processes, better risk management and deeper business and operation insights.

4. Privacy by design and by default

Privacy by design mandates the consideration of privacy at the development process of any product or service. Privacy by default requires privacy to be a default setting allowing a customer to customise how much they would like to share with others.

This requirement is a good practice for the purpose of ensuring that the privacy of customers are always protected, which allows trust to be built up between customers and businesses.

5. Pseudonymisation and its use in profiling

Pseudonymisation uses a form of encryption to translate identifiable parts of personal data to unique artificial identifiers to prevent linking the data to the original identity of a person. Although it can still be traced to the data subject, not all pieces of the puzzle are in one place.

This form of data is suitable for a wide range of analysis and profiling, and is seen as less likely to negatively impact customers. This opens up the opportunity for your business to do market behaviour analyses to improve product offerings and promotions with less cause for concern because the data has been pseudonymised.

6. Security and breach notification

The responsibility of security not only falls on the controller but the processor as well. For example, if an online retailer (controller) collects data of customers and uses a service to store and process the data for billing an invoice (processor), both organisations are responsible for handling the personal data of these customers.

Contacts us:

SEA and Singapore
Thio Tse Gan
Executive Director,
SEA Cyber Risk Leader
+65 6216 3158
tgthio@deloitte.com

Edna Yap
Executive Director
+65 6531 5016
edyap@deloitte.com

Eric Lee
Executive Director
+65 6800 2100
ewklee@deloitte.com

Siah Weng Yew
Executive Director
+65 6216 3112
wysiah@deloitte.com

Leslie Moller
Director
+65 6800 2333
lesmoller@deloitte.com

Hisashi Ohta
Director
+65 6800 2555
hohta@deloitte.com

Indonesia
Sigit Kwa
Associate Director
+62 21 2992 3100 Ext. 33548
skwa@deloitte.com

Malaysia
Ho Siew Kei
Director
+603 7610 8040
sieho@deloitte.com

Philippines
Anna Marie Pabellon
Partner
+63 2 581 9038
apabellon@deloitte.com

Thailand
Parichart Jiravachara
Executive Director
+66 (0) 2034 0130
pjiravachara@deloitte.com

Pinyo Treepetcharaporn
Director
+66 (0) 2034 0000 Ext. 11946
ptreepetcharaporn@deloitte.com

Deloitte.