asean insiders series

SEPTEMBER 2020

Personal Data Protection in ASEAN

ZICO law

PERSONAL DATA PROTECTION IN ASEAN

The dark cloud of the COVID-19 pandemic has a silver lining - it has accelerated the pivot to digitalisation and tech solutions. Businesses in all industries across ASEAN are forced not just to adopt but also to react to digitalisation. An important element of this digital revolution, is unquestionably, data. Machines, equipment, devices and platforms are increasingly being networked to communicate with each other, and fueled with a substantial amount of data. Without data, this digital revolution will come to a grinding halt. Poor data stewardship poses heightened risks against a person's fundamental right of privacy. Data breach incidents, whether due to security lapses or irresponsible processing of data, can cause irreparable harm to the reputation of a business. As interest in ESG (Environmental, Social and Governance) investing continues to grow, investors also are also placing heightened scrutiny on a company's data privacy and security controls.

This underscores the need to have robust laws and clear compliance guidelines to protect personal data and privacy.

The development of data protection regulation in ASEAN has so far been uneven. Until recently, Singapore, Malaysia and the Philippines were the only countries with personal data protection laws. The latest country in ASEAN to enact data protection laws is Thailand, with the Parliament passing the Personal Data Protection Act in early 2019. Indonesia has been mulling over it and had a draft legislation which has yet to make its way through the legislative process.

The coming into force of the European Union's General Data Protection Regulations ("**EU GDPR**") on 25 May 2018 has introduced even higher standards, stricter laws and tougher sanctions in the EU with extra-territorial application. The EU GDPR regulates the usage of data of its citizens by companies in terms of data, privacy, security and transparency not only in its region but also companies or organisations worldwide that process or hold data of EU residents. As ASEAN trades heavily with Europe, it is becoming important for businesses to comply with the regulations. Because of the EU GDPR, many of the ASEAN countries are reviewing their own data protection laws and may develop a similar regulatory framework to protect their citizens and enable local businesses to operate globally through some sort of comity in regulatory approach.

Malaysia may be reviewing its Personal Data Protection Act 2010 to ensure that it is streamlined with the EU GDPR. Singapore's Personal Data Protection Act 2012 shares many of the EU GDPR principles, in that they both require customer consent for all communications regarding data collection, data processing or disclosure of data. As part of an ongoing review, a discussion paper was issued to introduce the right to data portability, which gives users greater control over the movement of their information across service providers. Philippines Data Privacy Act came into effect in 2016 and regulators have issued recommendations to ensure compliance with data privacy laws. The Personal Data Protection Act recently passed in Thailand offers citizens similar protections to the EU GDPR. While the remaining countries in ASEAN may not have overarching regulatory frameworks for data protection, there are laws in specific sectors or for electronic media.

This publication provides a snapshot of the various aspects and considerations that are relevant to the protection of personal data across ASEAN.

Nadarashnaraj Sargunaraj
Partner
nadarashnaraj@zicolaw.com

Countries with general personal data protection laws

MALAYSIA	
Legislation	Personal Data Protection Act 2010 ("**PDPA**")
Regulator	Personal Data Protection Commissioner
Application	Applies to: • any person who processes and has control over or authorises the processing of, any personal data in respect of commercial transactions • data users using equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.
Privacy notice requirements	Data user must provide written notice to the data subject with: • a description of the personal data which is being processed • purposes for use of the data • source of the data • persons to whom the personal data may be disclosed • the choices of the data subject for limiting the processing of his personal data • whether it is obligatory or voluntary for the data subject to provide the data and the consequences if he does not provide it.
Consent requirements	• Consent can be in writing or electronic form and must be recorded by the data user. Consent shall be in the national language or English. • Burden is on the data user to prove that consent has been obtained. • Explicit consent is required to process sensitive personal data. • Consent can be withdrawn by written notice.
Security	Data users have an obligation to take 'practical' steps to protect personal data, which includes, developing and implementing a security policy.
Breach notification	Currently, they are no requirements to inform authorities and data subjects of any data breaches. However, news reports indicate that the law could be amended to introduce such requirement, modelled on the EU GDPR.
Cross-border transfer of data	A data user cannot transfer personal data to a place outside Malaysia unless: • it is on a whitelist specified by the Minister, or • where the exceptions apply
Marketing	The principles on notice and choice apply. In addition, a data subject may by written notice require that a data user not use or stop using his personal data for marketing purposes. He may also withdraw consent previously given.
Sectoral regulations and Code of Conduct	Codes of conduct apply in the following sectors: • aviation • banking and financial • insurance and takaful • utilities (electricity)
Right of data subject to request and access correction	A data subject shall be given access to his personal data held by a data user and be able to make corrections.
Registration	Registration is required for data users in the prescribed sectors: • communications • banking and financial institutions • insurance • health • tourism and hospitality • transportation • education • direct selling, services (legal, audit, accountancy, engineering, architecture) • real estate • utilities • pawnbroker • money lenders.
Data Protection Officers	Currently, not required to appoint a data protection officer.
Penalties	For a body corporate, any person who at the time of the commission of the offence was a director, chief executive officer, chief operating officer, manager, secretary or other similar officer responsible for the management of the body corporate can be charged severally or jointly in the same proceedings as the body corporate.

SINGAPORE	
Legislation	Personal Data Protection Act 2012 (No. 26 of 2012)* ("**PDPA**") ** To be read together with the various guidelines issued by the PDPC*
Regulator	Personal Data Protection Commission ("**PDPC**")
Application	Applies to all organisations (including any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under the laws of Singapore or resident or having a place of business in Singapore) that carries out activities involving personal data in Singapore, unless they fall within the category of organisations expressly excluded from the application of the PDPA. Excluded organisations: • individuals acting in a personal or domestic capacity; • employees acting in the course of his or her employment with an organisation; • public agencies; and • organisations in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.
Privacy notice requirements	Organisations must obtain consent before collecting, using or disclosing personal data and must: • use personal data only for limited purposes of which the individual has been notified • provide the individual access to and correct errors in his personal data • protect personal data in its possession • cease to retain personal data when no longer necessary • not transfer personal data outside of Singapore (except in accordance with the PDPA).
Consent requirements	• Consent should be written or in electronic form. • Consent can be withdrawn at anytime by an individual upon reasonable notice to the organisation.
Security	An organisation must make security arrangements reasonable and appropriate in the circumstances to protect personal data and prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
Breach notification	Under the PDPC's Guide to Managing Data Breaches 2.0 ("**PDPC Breach Guide**"), organisations are advised to notify the PDPC and/or affected individuals of data breaches that is of a significant scale (i.e. the data breach involves personal data of 500 or more individuals) or is likely to result in significant harm or impact to the individuals to whom the information relates. These breach notification requirements closely mirror those under the Personal Data Protection (Amendment) Bill 2020 ("**PDP Bill**"), which introduces a mandatory data breach notification regime.
Cross-border transfer of data	An organisation may transfer personal data overseas if: • it complies with the PDPA while the transferred personal data remains in its possession; and • the recipient is bound by legally enforceable obligations to provide protection comparable to that under the PDPA.
Marketing	The "Do Not Call (DNC) Registry" allows individuals to opt out of certain marketing messages being sent to his or her Singapore telephone numbers.
Sectoral regulations and Code of Conduct	PDPC has published advisory guidelines specific to the following sectors: • telecommunications • real estate agencies • education • healthcare • social services • transport services (in-vehicle recordings) • management corporations The following regulated industries also have specific data protection rules: • banking • healthcare • life insurers
Right of data subject to request and access correction	Individuals have the right to request access to their data and for corrections to be made to it.
Registration	No requirements for registration.
Data Protection Officers	An organisation is required to designate a data protection officer.
Penalties	For persons in breach of the PDPA, fines not exceeding SGD5,000 - SGD10,000 or imprisonment of up to 12 months, or both, depending on the offence. For organisations in breach of the PDPA, fines not exceeding SGD50,000 - SGD100,000. Officers and members of an organisation in breach of the PDPA may be held liable for breaches of that organisation.

PHILIPPINES	
Legislation	• Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012 ("**DPA**") • Implementing Rules and Regulations of the DPA ("**IRR**")
Regulator	National Privacy Commission
Application	• The DPA and its IRR apply to the processing of personal data by any natural and juridical person in the government or private sector. • Both the DPA and IRR have extraterritorial application.
Privacy notice requirements	• The data subject must be aware of the nature, purpose and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. • Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
Consent requirements	• Consent shall be in writing, either by electronic or recorded means. It may also be given on behalf of the data subject by an authorised agent. • Where sensitive personal information is being processed, notice and consent should be obtained prior to processing. • Data subjects are allowed to withdraw their consent.
Security	Personal information controllers and processors are required to implement reasonable and appropriate organisational, physical, and technical security measures for the protection of personal data. Steps should be in place to ensure that any natural person acting under their authority and has access to the data, does not process them except upon their instructions, or as required by law.
Breach notification	• The National Privacy Commission is to be informed within 72 hours upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. • Affected data subjects shall also be notified within 72 hours of the breach.
Cross-border transfer of data	The DPA does not restrict the transfer of personal data outside the Philippines.
Marketing	Where data is to be processed for direct marketing, the data subject must be provided with specific information regarding the purpose and extent of processing. Where the direct marketing activity involves data sharing to a third party, both DPA and IRR require a data sharing agreement.
Sectoral regulations and Code of Conduct	There are no specific sectoral regulations or Codes of Conducts on personal data. However, in light of the COVID-19 pandemic, the National Privacy Commission, together with the Department of Health, has issued a joint memorandum applicable to the use of telemedicine.
Right of data subject to request and access correction	The data subject has the right to request access to their data and to dispute any inaccuracies in the personal data. The personal information controller has to correct the inaccuracies, unless the request is vexatious or otherwise unreasonable.
Registration	There are no requirements for data users to be registered. However, registration with the National Privacy Commission is required where: • the personal data processing systems operating in the Philippines involve accessing or requiring sensitive personal information of at least 1,000 individuals • the personal information controller or information processor, that employs fewer than 250 persons but carries out processing that is likely to: o pose a risk to the rights and freedoms of data subjects o the processing is not occasional, or o the processing includes sensitive personal information of at least 1,000 individuals. Notification should be made to the National Privacy Commission if the processing of personal information involves the use of automated operations, and when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject.
Data Protection Officers	The DPA requires persons involved in the processing of personal data to appoint a data protection officer.
Penalties	Penalties are criminal and civil in nature: • In cases where a data subject files a complaint for violation of his or her rights as a data subject, and for any injury suffered as a result of the processing of his or her personal data, the National Privacy Commission may also impose civil liability upon the violator and award indemnity to the data subject based on the New Civil Code. • In case of criminal acts, if the offender is a corporation, partnership, or any juridical person, the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime, shall be recommended for prosecution by the National Privacy Commission based on substantial evidence.

THAILAND

Legislation	• On 27 May 2019 the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") was gazetted with the effective date of coming into operation set as 27 May 2020. Due to COVID-19 however, a royal decree was issued which defers the enforcement of the PDPA until 1 June 2021. • Under tort, the Civil and Commercial Code (as amended) ("**CCC**") is still applicable for the collection, use, disclosure or transfer of personal data in case such act causes damage to a data subject. • Certain sectoral legislation such as telecommunications, banking and financial institutions does regulate the collection and use of personal data. The provisions of the PDPA will apply additionally.
Regulator	Personal Data Protection Committee ("**PDPC**")
Application	• The PDPA applies to a person who has power to make decision regarding the collection, use, or disclosure of the personal data ("**Data Controller**") or a person who operates in relation to the collection, use and disclosure of personal data pursuant to the orders given by or on behalf of a Data Controller ("**Data Processor**"). • The PDPA has extraterritorial reach and applies to Data Controller or Data Processor outside of Thailand who collects, uses or discloses personal data of data subjects who are in Thailand, where the Data Controller or Data Processor: o offers goods or services to a data subject in Thailand; or o monitors behaviours of a data subjects which occur in Thailand.
Privacy notice requirements	Generally, the Data Controller must notify the data subject of: • the data to be collected • objectives of the data collection • use or disclosure, data retention period • types of persons to whom the collected data may be disclosed • whether it is obligatory or voluntary for the data subject to provide the data and the consequences if he/she does not provide • rights of the data subject.
Consent requirements	• Explicit consent in writing or via an electronic system is required , unless it cannot be done by its nature. • The data subject must be informed of the purpose of the collection, use, or disclosure of the personal data when there is a request for consent. The request for consent must be presented in a manner which is clearly distinguishable from other matters, in an easily accessible and intelligible form and statements, using clear and plain language, and is not deceptive or misleading to the data subject. • Explicit consent is required for collection of sensitive personal data though there are exceptions in certain situations. • Consent can be withdrawn upon notice by the data subject.
Security	Appropriate security measures is required to prevent unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data, and such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety. The security shall also be in accordance with the minimum standard specified and announced by the PDPC.
Breach notification	• The Data Processor must notify the Data Controller of any data breach. • The Data Controller must notify the Office of PDPC without delay and within 72 hours of a data breach that might affect personal rights and freedom after its awareness of the same. • The Data Controller must also notify the data subject of a data breach that poses a high risk of affecting personal rights and freedom and the remedial measures.
Cross-border transfer of data	Personal data can be transferred to other countries or international organisations that have adequate personal data protection standards unless exemptions apply.
Marketing	Marketing is allowed to the extent that it must not unreasonably affect the rights and freedom of the data subject or it is done for public interest. The data subject can oppose the collection, use or disclosure of personal data for direct marketing at any time.
Sectoral regulations and Code of Conduct	There are specific laws and regulations governing personal data in some sectors such as banking and finance, telecommunication.
Right of data subject to request and access correction	Data subjects have the right to request access to their personal data and make corrections to it.
Registration	There are no requirements for data users to be registered.
Data Protection Officers	Data protection officers are required to be appointed in certain cases where there is collection, use or disclosure of sensitive data, or massive amount of personal data.
Penalties	• Civil compensation and punitive damages, criminal penalties and administrative fine will be imposed on the violator. • Directors and managers responsible for a juristic person will be subject to criminal liability.

Countries with personal data protection laws that are specific to sectors or medium

INDONESIA

Indonesia has no general data protection laws. However, there are certain regulations concerning the use of electronic data (collectively "**EIT Regulations**"):

- Law No. 11 of 2008 on Information and Electronic Transaction as amended with Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Information and Electronic Transaction;
- Government Regulation No.82 of 2012 on Electronic System and Transaction Operation and its implementing legislation, Minister of Communication and Informatics Regulation No.20 of 2016 on Personal Data Protection in an Electronic System; and
- Government Regulation No. 71 of 2019 on the Implementation of Electronic System and Transaction.

The EIT Regulations are applicable to those who use electronic information and transactions both in and outside of Indonesia, but have relationship with Indonesian jurisdiction, and detrimental to the interest of Indonesia.

Privacy Notice, Consent and Registration	• Written notice is required for any actions related to the acquisition, collection, processing, analysis, storage, appearance, announcement, transfer and distribution of personal data. • The data subject must be provided with the option to allow or not allow third parties to obtain or collect the personal data. • A written consent in Bahasa Indonesia is required in order to acquire, collect, process, analyse, transfer, and distribute personal data. The consent may be made in bilingual format, but Bahasa Indonesia shall be one of the language. • Processing of personal data must obtain a valid consent from the personal data owner for the purposes that have been conveyed to the owner. • While there are no provisions for withdrawal of consent, the EIT Regulations allows for data owner to demand data user to erase the personal data, except regulated otherwise by the prevailing laws and regulations. In this regard, the data owner is entitled of two types of rights which are: o Right to Erasure, on which individuals may ask an electronic system provider to delete irrelevant electronic information or electronic documents (including personal data obtained and processed without their consent); and o Right to Delisting, on which an individual may ask an electronic system provider to delist irrelevant electronic information or electronic documents from an Internet search engine through a court order. • Data used for public services and private purposes must be registered with the Minister of Communication and Informatics. The registration must be conducted before the electronic system is used to process electronic data, including personal data.
Security	• Obligations of data users include: o maintaining the confidentiality of the personal data acquired, collected, processed, and analysed o protecting personal data along with the documents containing such personal data from misuse o being liable in case of personal data misuse o issuing an internal regulation on protection of personal data in compliance with the laws and regulations o providing audit trail of the whole electronic system it manages. • If the data is used for public purposes, the holder of the data has an additional obligation to have the data centre/server and disaster recovery centre located in Indonesia unless the storage technology is unavailable in Indonesia.
Breach	There are no requirements to notify the authority of data breaches. However, the electronic system provider shall inform the data owner in written or electronic form within 14 days of the breach along with reasons for the breach.
Cross-Border Transfer and Marketing	• Although there are no restrictions, the following procedures apply to transfer personal data overseas: o coordinate with Minister of Communication and Informatics or officer/agency authorised for such matters; and o comply with the prevailing laws on cross-border data transfer (however to date Indonesia does not have any laws on cross-border transfers of data). • Written consent is required for the processing of personal data for marketing purposes.
Sectoral Regulations	In addition, there are also sectoral regulations that may relate to data protection: • Telecommunications Sector - Law No. 36 of 1999 regarding Telecommunications provides that any person is prohibited from tapping information transmitted through any telecommunications services operator has to keep confidential any information transmitted or received through its network. • Public Information Sector - Law No. 14 f 2008 regarding Disclosure of Public Information provides that public bodies may not disclose any information relating to personal rights. • Banking and Capital Market Sectors - data privacy is regulated under Law 7 of 1992 as amended by Law 10 of 1998 on Banking and Law 9 of 1995 on Capital Markets (applies to both individuals and corporate data) and Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology (prior approval from the Bank Indonesia needs to be obtained prior to customer data transfer, by way of establishing a data centre or data processing outside of Indonesia).

Sectoral Regulations	• Finance Sector - Financial Services Authority Regulation No.1/POJK.07/2013 on Financial Consumer Protection stipulates that the disclosure of the customer personal data to any third party is prohibited to the financial service business actors unless written consent had been obtained or the disclosure is required by law. Further, financial services business actor must obtain approval from the data owner for the data obtained from third parties used to carry out its activities. • Health Sector - protections against the medical records of the patient is regulated under Law No. 26 of 2009 on Health and Minister of Health Regulation No. 269/Menkes/Per/III.2008 on Medical Records (every person is entitled to the confidentiality of their health conditions that have been disclosed to the healthcare provider). • Trading Sector - Government Regulation No. 80 of 2019 on Trade through Electronic Systems stipulates that every business actor who engages in the electronic trading activity must meet the standard criteria for recording the data of their customers electronically. In addition, the customer has the right to request the revocation of the customer's data in the event the customer chooses to quit, unsubscribe, or not utilise the business actor's trading electronic platform.
Data Protection Officers	No exact provision to appoint, however the EIT Regulations provide that a data user must have internal policies of personal data protection and provide details of a contact person, which can be contacted by a data owner regarding management of his data.
Penalties	Penalties range from fines of up to IDR12 billion and/or imprisonment of up to 12 years and/or administrative sanctions (warnings, administrative penalty, suspension of activities, announcement on the relevant website and dismissal from the registration list).

LAOS

Law on Electronic Data Protection No. 25/NA dated 12 November 2017 ("**Law on Electronic Data Protection**") applies to a domestic or foreign individual, juristic person or incorporated body, who lives and operate in Lao PDR. The law is also applicable to foreign data users if they conduct business or have operations in Lao PDR.

Registration and Consent	• While there are no specific requirement for data users to be registered, data processing shall be within a registered business scope of the data controller/processor, who is an incorporated entity. • Data collectors need to identify the objective, details of data collection, identity of the data controller and the rights of the data subject. Data subjects may refuse to give permission for the use, disclosure, and transfer of data. Data subjects are to be notified with regards to any amendment or deletion of their data. • Prior consent is needed for the collection, use, disclosure and transfer of data.
Security and Breach	• Data controllers are required to adopt appropriate security measures to prevent unauthorised or unlawful access to personal data. • Where there is a data breach, data controllers are required to notify the relevant authority of the date, time, place, form and characteristic of data breach, and impact and source of data breach.
Cross-Border Transfer and Marketing	The Law on Electronic Data Protection does not provide any provisions on cross-border transfers of data or processing of personal data for marketing purposes.
Sectoral regulations	There are codes of conduct applicable to the banking and credit information system.
Data Protection Officers	Data controller has the obligation to establish an internal department/appoint and officer to supervise protection of the data.
Penalties	Civil, criminal and administrative penalties, including: • warning and re-education • disciplinary action in case of offences committed by government officials • fine of LAK15 million in case of engagement in prohibited action which does not constitute criminal offence • potential civil liability for incurred damage • the application of criminal sanctions based on the seriousness of the wrongful act.

VIETNAM

Currently, there is no general personal data protection law in Vietnam. Personal data protection however is sparsely regulated in several laws such as:

- Law on Protection of Consumers' Rights 2010
- Law on Cyber Information Security 2015
- Law on Information Technology 2016
- Law on Cyber Security 2018

In general, Vietnamese law on personal data protection applies to Vietnamese agencies, organisations and individuals, and foreign organisations and individuals directly involved in or related to cyber information security activities in Vietnam. The law also has extraterritorial reach in that it applies to data users outside of Vietnam.

Privacy Notice, Registration & Consent	• Notification is required of the form, scope, place and purpose of collecting, processing and using of personal data and data users are required to obtain consent prior to the collection. Data subjects can opt to withdraw their consent, unless prescribed by the law. • Registration for data users depends on the specific sectors that data operators operate in. Foreign enterprises providing telecommunication services, internet services and value-added services in Vietnam's cyberspace that collect, analyse or process personal data are required to open branches or representative offices in Vietnam.
Security and Breach	• Data users are obliged to take appropriate management and technical measures to protect personal data and to comply with standards and technical regulations on security of cyber information. • In the event of a breach, both the authority and data subjects must be notified.
Cross-Border Transfer and Marketing	There are no restrictions to cross-border transfers of data and on processing personal data for marketing purposes. However, written consent is required for the processing of personal data for marketing purposes.
Sectoral regulations	Sectoral regulations apply banking and finance, e-commerce, insurance, information technology, telecommunications, media and consumer protection.
Penalties	Administrative, civil and criminal sanctions may apply for infringement of an individual's privacy. Depending on the circumstances of the case, officers of a body corporate may be severally liable for breaches of the law.

CAMBODIA

- There are proposals to draft laws relating to Trade Secrets, State Secrets and Cyber Law. However, these laws have yet to be drafted. Currently, there is no specific personal data protection law in the Kingdom of Cambodia. The legal framework may however be found in general law (Civil Code and Criminal Code) and in specific laws regulating the entity undertaking such acts.
- Some provisions of personal data, confidentiality and right to privacy have been embedded in the following laws:
  - Cambodian Constitution 1993
  - Cambodian Civil Code 2007
  - Cambodian Criminal Code 2009
  - Labour Law 1997
  - Law on Banking and Financial Institutions 1999
  - Prakas on Credit Reporting dated 24 May 2011
  - Law on Press 1995
  - Sub-decree on the Code of Medical Ethics dated 28 August 2003
  - Law on Electronic Commerce 2019
- The laws above are applicable to banks, financial institutions, the press, medical professionals, Cambodian citizens and persons residing in the Kingdom of Cambodia.
- Penalties for contravention of the laws above include:
  - Cambodian Civil Code: civil claim for damages, injunction.
  - Cambodian Criminal Code: According to Article 314, any person who reveals confidential information regarding the profession, function or mission to unauthorised persons shall be punished by an imprisonment of between one month to one year and a fine of between KHR100,000 to KHR2 million.
  - Law on Electronic Commerce 2019: imprisonment between one to two years and a fine from KHR2 million to KHR4 million for contravention of Article 32(1) on storing private information electronically.
  - Labour Law 1997: fine of 10 to 30 days of the base daily wage for breaching confidentiality during period of suspension, termination of the employment contract without prior notice for breaching professional confidentiality.
  - Law on Negotiable Instruments and Payment Transactions: damages for breach of an obligation of secrecy and non-disclosure of information which is not limited to monetary losses and may include compensation for proven distress, embarrassment or inconvenience.
  - Prakas on Credit Reporting: administrative fine of KHR5 million to KHR250 million as well as disciplinary sanctions or penalties.
  - Sub-Decree on Code of Medical Ethics: disciplinary punishments by the Regional Medical Council with participation of the disciplinary unit of the National Medical Council. In this case, the Regional Medical Council's president shall enforce the decision.
  - Law on Press: civil action for damages may be filed by individuals whose rights under this article are violated by the press.

Countries with no personal data protection laws

MYANMAR

Currently, there is no specific data protection law in Myanmar. Personal data protection however is sparsely regulated in several laws such as:

- Law Protecting the Privacy and Security of Citizens (Union Parliament Law 5/2017) ("**PPSC Law 2017**") – applies to citizens of Myanmar and any person who commits unlawful acts, under section 8, to any citizen of Myanmar.
- Electronic Transactions Law 2004 to be read together with Pyudaungsu Hluttaw Law No. 6/2014 ("**ET Law 2004**") – applies to any person who commits an offence within Myanmar or from Myanmar to outside Myanmar, or from outside Myanmar to Myanmar via electronic transaction technology.

Penalties include:

- PPSC Law 2017: imprisonment for a minimum period of 6 months and up to 3 years.
- ET Law 2004: up to 5 years imprisonment.

BRUNEI

There are currently no general data protection laws in Brunei but the country has been guided by a Data Protection Policy since 2014. However only government bodies are subject to the provisions of the Data Protection Policy – the private sector remains exempt.

ZICO | law

ASEAN Data Protection Laws & Readiness for EU GDPR

General Application — **Sector Specific** — **No regulation**

Thailand

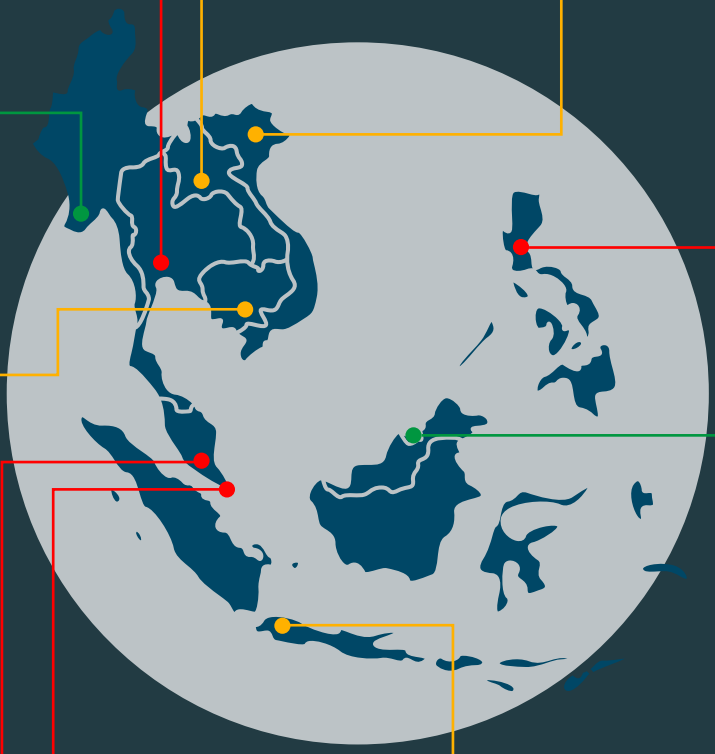
- Thailand's Personal Data Protection Act (PDPA) offers citizens similar protections to the EU GDPR. The PDPA will apply not only to companies located in Thailand, but also overseas companies which collect, use, or disclose personal data of any subjects in Thailand.

Laos

- No specific law on personal data protection in Lao PDR. However there is a law on electronic data protection.
- No indication that the country is prepared to adapt its existing laws to meet EU GDPR standards and obligations.

Vietnam

- No single comprehensive law to regulate personal data protection in Vietnam. Personal data protection regulations are scattered throughout different pieces of legislation.
- No indication that Vietnam is moving towards an singular data protection law comprising the policies of the EU GDPR.



Philippines

- The National Privacy Commission has been pushing for data privacy compliance across different industries in the Philippines.
- In an effort to comply with the higher standards and obligations set by the EU GDPR, the Philippine Data Privacy Act of 2012 is now supplemented by rules and regulations mirroring EU GDPR policies.

Myanmar

- No specific law governing personal data

Cambodia

- Micro level efforts are being made across banks, law firms and insurance firms to comply with the EU GDPR in their company policies.
- No announcement of a nationalised effort to legislate personal data protection law.

Brunei

- No specific law governing personal data

Malaysia

- Malaysia recognizes EU GDPR's potential impact on companies across the globe and welcomes the higher standards that the EU GDPR provides.
- The Personal Data Protection Act 2010 is in the midst of being reviewed to incorporate elements from the GDPR.

Singapore

- Singapore is mooting for the inclusion of data portability in its Personal Data Protection Act 2012 (No. 26 of 2012) which aims to ease the data flow between service providers as well as to provide consumers with "greater control" over their own data.
- The Personal Data Protection (Amendment) Bill 2020 introduces a new data portability obligation.

Indonesia

- There is no general personal data protection law, however personal data in electronic systems are protected and legislated.
- Indonesia is currently in the midst of preparing a new law on the protection of personal data. The data protection bill was drafted back in June 2019, and was prepared by using EU GDPR as a reference. The data protection bill has been approved by Indonesia's President, Joko Widodo, and is currently discussed in the House of Representatives. Although it was uncertain of when the draft law will be passed into law, there are several indications from the statement given by the government officials that they expect the draft bill will be ratified and enacted in 2020.

ZICO LAW ASEAN NETWORK CONTACTS

Rozaiman Abdul Rahman
Managing Partner
ZICO R.A.R
rozaiman.ar@zicolaw.com
t. +673 223 2929

Matthew Rendall
Partner
SokSiphana&associates
matthew.rendall@zicolaw.com
t. +855 23 999 878

Afriyan Rachmad
Partner
Roosdiono & Partners
afriyan.rachmad@zicolaw.com
t. +6221 2978 3888

Jade Hwang Poh Geok
Partner
Roosdiono & Partners
poh.geok.hwang@zicolaw.com
t. +6221 2978 3888

Aristotle David
Managing Partner
ZICO Law Laos
aristotle.david@zicolaw.com
t. +856 21 410 033

Tuchakorn Kitcharoen
Senior Associate
ZICO Law Laos
tuchakorn.kitcharoen@zicolaw.com
t. +856 21 410 033

Nadarashnaraj Sargunaraj
Partner
Zaid Ibrahim & Co.
nadarashnaraj@zicolaw.com
t. +603 2087 9999

Geraldine Oh
Resident Partner
ZICO Law Myanmar
geraldine.oh@zicolaw.com
t. +95 1 538 362

Felix Sy
Managing Partner
Insights Philippines Legal Advisors
felix.sy@insights-law.com
t. +63 2 903 1290

Yap Lian Seng
Managing Director
ZICO Insights Law
lian.seng.yap@zicolaw.com
t. +65 6443 4920

Heng Jun Meng
Director
ZICO Insights Law
jun.meng.heng@zicolaw.com
t. +65 6443 4920

Nuttaphol Arammuang
Managing Partner
ZICO Law Thailand
nuttaphol.a@zicolaw.com
t. +66 2 6777 588

Archaree Suppakrucha
Partner
ZICO Law Thailand
archaree.suppakrucha@zicolaw.com
t. +66 2 6777 588

Tay Zi Li
Co-Executive Partner
ZICO Law Vietnam
zi.li.tay@zicolaw.com
t. +84 28 3915 1000

ZICO law

ZICO Law is a network of leading independent local law firms focused on ASEAN. With a presence in 18 cities in 10 out of 10 ASEAN countries, our 300 lawyers enable our clients to enjoy value-added legal services by leveraging on a combination of local expertise and regional insights.

ASEAN INSIDERS, by origin and passion

BRUNEI | CAMBODIA | INDONESIA | LAOS | MALAYSIA | MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM

www.zicolaw.com