

Recent Personal Data Protection Law Updates Within the ASEAN Region



G Vijay Kumar
Partner (Dispute Resolution)

**Technology, Media &
Telecommunications**

T: +603 6208 5870

E: ykg@lh-ag.com

The past two years have seen robust developments to personal data protection laws within the ASEAN region. This alert discusses some of the major developments and progressive steps taken by various ASEAN countries in seeking to align their respective personal data protection laws with what is perceived to be the gold standard for data protection laws, the European Union General Data Protection Regulation (**GDPR**).

Thailand

After much anticipation, the Personal Data Protection Act¹ was introduced in May 2019 (**Thai PDPA**), which largely adopted measures and standards similar to the GDPR. This includes requirements to appoint a data protection officer and to notify in the event of a data breach, as well as principles such as purpose limitation, lawfulness and fairness and data minimisation. The Thai PDPA also established the Personal Data Protection Commission, a regulator that will oversee and spearhead the enforcement of the Act.

The Thai PDPA has been partially enforced, with the main provisions on processing of personal data, rights of the data subject, complaints, civil liability and penalties only coming into force upon the expiry of a grace period, which was initially set to be one year from May 2019. However, the enforcement date of the remaining provisions of the Thai PDPA has been extended to 1 June 2021 in order to afford ample time for organisations to assimilate and incorporate the requirements under the Thai PDPA within their business practices, given the high standards contemplated therein.

Similar to the GDPR, the Thai PDPA has an extraterritorial effect. This raises the possibility of data controllers and processors not based in Thailand being subject to the requirements therein in respect of the processing of personal data of data subjects located in Thailand. Any contravention of the Thai PDPA may be punishable by administrative fines of up to THB5 million (approximately RM660,000) as well as criminal penalties.



Teo Wai Sum
Partner (Corporate Advisory)

**Technology, Media &
Telecommunications**

T: +603 6208 5805

E: tws@lh-ag.com



Eunice Chan Wei Lynn
Partner (Corporate Advisory)

**Technology, Media &
Telecommunications**

T: +603 6208 5872

E: cwl@lh-ag.com



CK Lung
Partner (Dispute Resolution)

**Technology, Media &
Telecommunications**

T: +603 6208 5948

E: ckl@lh-ag.com

¹

The Thailand Personal Data Protection Act, B.E. 2562 (2019), available at https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf

Vietnam

Previously, laws relating to personal data protection were found in various pieces of legislation such as the Civil Code, the Law on Cyber-Information Security and the Law on Telecommunications. Vietnam has since taken a major stride by consolidating personal data protection regulations into a single piece of legislation. The comprehensive Draft Decree on Personal Data Protection (**Draft Decree**) was circulated for public consultation in February 2021 following the circulation of an outline of the laws in December 2019.

The Draft Decree sets out an extensive framework for the processing of personal data including cross-border data transfer, rights of data subjects, processing of sensitive personal data and other relevant provisions. The principles governing the Draft Decree bear strong similarities to the GDPR principles, which include, among others, the principles of lawfulness, data minimisation, purpose and use limitations. Additionally, the Draft Decree has put forward the proposed establishment of the Personal Data Protection Committee to regulate matters pertaining to personal data. It is pertinent to note that the Draft Decree is set to have extraterritorial effect on any organisation or individual, whether established in Vietnam or abroad, that processes personal data of Vietnamese residents. Sanctions contemplated under the Draft Decree include monetary penalties of up to VND100 million (approximately RM18,000) and up to 5% of the total revenue for repeated violations, as well as additional sanctions such as the suspension of processing personal data for up to three months and the revocation of the written consent in respect of sensitive personal data and cross-border transfer of personal data.

The Draft Decree is envisaged to take effect on 1 December 2021.

Indonesia

Similar to Vietnam, Indonesia does not currently have an all-encompassing Act to govern the protection of personal data but rather, data protection regulations can be found in various laws including the law on Electronic Information and Transactions² and the Minister of Communications and Informatics Regulation No 20 of 2016 regarding the Protection of Personal Data.

In January 2020, the Personal Data Protection Bill (**PDP Bill**) was signed by the President of Indonesia and is now pending the review of the Indonesian House of Representatives. The scope of the PDP

²

Law No 11 of 2008 regarding Electronic Information and Transactions, as amended by Law No 19 of 2016

Bill is expected to largely reflect the GDPR and will comprehensively govern the processing of personal data. The PDP Bill sets out administrative and criminal penalties of up to IDR70 billion (approximately RM20.3 million) for any contravention of the PDP Bill.

Once passed, organisations will be granted a two-year grace period prior to the full enforcement of the PDP Bill in order to allow businesses to adapt and modify their processes in compliance with the requirements therein.

Singapore

Singapore's Personal Data Protection Act³ (**Singapore PDPA**) has been significantly amended in February 2021⁴ as part of a continuous effort to align it with international standards. Some of the major changes include enhancing the data breach notification regime from a voluntary basis to a mandatory requirement. Pursuant to the amendments, organisations are now obliged to notify the Personal Data Protection Commission of any data breach if such breach is likely to result in significant harm, or is of a significant scale, no later than three days of the assessment by such organisation that the breach amounts to a notifiable data breach. New exceptions to the consent requirement were also introduced to facilitate business processes, such as provisions on deemed consent by contractual necessity and by notification, as well as allowing the processing of personal data without consent for the purposes of carrying out business improvement and research and development.

Other amendments to the Singapore PDPA that are expected to be enforced in upcoming months include the increase of financial penalties for organisations from a capped amount of SGD1 million (approximately RM3.1 million) to up to 10% of the organisations' turnover or SGD1 million, whichever is higher. The amendments will also introduce the data subject's right to data portability, as well as criminal liability for individuals in the event of egregious or reckless mishandling of personal data.

Malaysia — Where do we stand?

The Personal Data Protection Commissioner issued a Public Consultation Paper on the Review of the Personal Data Protection Act 2010 (**PDPA**) in February 2020 for public consultation, with the

³ The Singapore Personal Data Protection Act 2021, available at <https://sso.agc.gov.sg/Act/PDPA2021>

⁴ The Singapore Personal Data Protection (Amendment) Act 2020, available at <https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210?DocDate=20201210>

objective of proposing amendments to enhance the existing provisions under the PDPA to be parallel with international standards. Our previous alert on this can be read [here](#).

Following the end of the consultation period in March 2020, the Commissioner has yet to publish any potential steps or measures to be taken in effecting the proposed amendments to the PDPA. In this regard, the Malaysian Digital Economy Blueprint⁵ recently launched by the Prime Minister's Department specified the strengthening of the existing data protection regulatory framework as one of the strategies to be adopted in order to facilitate a holistic digital economy. However, the stipulated targeted timeline for the review of the PDPA is by 2025, and other relevant laws by 2030.⁶ Given the aggressive and proactive steps forward taken by our neighbouring countries to ensure that local personal data protection laws are at par with the GDPR, it is high time that the PDPA be given a comprehensive makeover as soon as possible so as to afford the highest standards of protection to personal data.

Eleena Abd Wahab



Eleena Abd Wahab
Senior Associate
**Technology, Media &
Telecommunications**
T: +603 6208 5815
E: eaw@lh-ag.com

⁵ The Malaysia Digital Economy Blueprint published by the Economic Planning Unit of the Prime Minister's Department on 19 February 2021, available at <https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf>

⁶ *Ibid*, at p 74