ONE ASIA LAWYERS

Amendments to Personal Data Protection Act 2024

September 2024
One Asia Lawyers Group
Yuki Hashimoto Lawyer (Japan)
Sharil Ramli Lawyer (Malaysia)

1. Introduction

On 31 July 2024, the Malaysia's Dewan Negara (Senate) passed the Personal Data Protection (Amendment) Bill 2024 ("**Bill**"). The Bill was earlier passed in the Dewan Rakyat (House of Representatives) on 16 July 2024. The Bill introduces amendments to the Personal Data Protection Act 2010 (PDPA), including updated definitions, mandatory data breach notification and imposition of higher penalties for non-compliance.

It is anticipated that the Bill will receive the royal assent and take effect on a later date to be announced by the Minister of Digital, Gobind Singh Deo. The updates to the PDPA are Malaysia's response to the businesses' increased reliance on digital platforms, increase in data breaches and online fraud cases which have raised expectations for data protection.

2. Guidelines and Consultation Papers

The Minister of Digital also announced that the PDPA will be accompanied by several guidelines to supplement the amendments introduced by the Bill, covering data breach notification, data protection officers, data portability, cross-border data transfer and its mechanism, data protection impact assessment, privacy by design, and profiling and automated decision-making. The first three public consultation papers have been recently issued by the Commissioner in relation to the implementation of the Bill and its related Guidelines:

- Public Consultation Paper No. 01/2024 The Implementation of Data Breach Notification;
- Public Consultation Paper No. 02/2024 The Appointment of Data Protection Officer; and
- Public Consultation Paper No. 03/2024 The Right to Data Portability.

These public consultation papers provide some background on the incoming guidelines while seeking for the public feedback. It is very important for organisations/businesses to understand the amendments introduced by the Bill and start taking proactive steps to update internal policies and procedures to mitigate any potential legal liabilities.

3. Key highlights on amendments introduced by the Bill and practical recommendations to organisations/businesses

- **Substitution of "Data User" with "Data Controller"**

The Bill adopts the term "Data Controller" to replace the currently used "Data User" term, which is more aligned with the approaches in personal data protection framework adopted in other jurisdictions such as the EU. There is no material impact from this change, however we foresee

that organisations/businesses should be prepared to update their related documents including personal data protection policies, notices or forms when the Bill comes into force later.

- **Data Processor's obligation to comply with the Security Principle**

Presently, data processors do not have to comply with the Security Principle[1] in the PDPA, only the data users need to comply with it when processing of personal data is carried out by a data processor on behalf of the data user in accordance with Section 9(2) of the PDPA. The Bill now introduces a direct obligation for data processors including requiring them to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. Failures to do so will result in the data processors to be guilty of an offence and on conviction, a fine of up to RM1,000,000 (approximately ¥33,250,000) and/or imprisonment for up to 3 years. Organisations/businesses should be ready to update their practices with regards to how the data processors carry out their duties and obligations in compliance with the requirements introduced by the Bill.

- **Mandatory data breach notification**

Data controllers need to notify the Personal Data Protection Commissioner ("**Commissioner**") as soon as practicable if they have reason to believe that a personal data breach has occurred. This includes incidents such as breach, loss, misuses or unauthorised access of personal data. Non-compliance may subject one to a fine of RM250,000 (approximately ¥8,300,000) and/or two years imprisonment. We recommend organisations/businesses to be prepared to update their existing data breach notification guidelines or policies, or consider drafting new guidelines or policies on the subject matter if they haven't done so to comply with such requirement, the details of which are to be published through the Data Breach Notification Guidelines by the Ministry of Digital later.

- **Appointment of Data Protection Officers (DPO)**

The data controllers and data processors will be required to appoint one or more Data Protection Officers (DPOs). The DPOs will be responsible to ensure the organisation's compliance with the PDPA. However, we take note from the Bill that the appointment of the DPOs shall not discharge the data controller or data processor from all duties and functions stated in the PDPA.

Similarly, the Ministry of Digital has yet to provide the details for this requirement, such as relevant qualifications or recommended skillsets needed for the DPOs, which we believe will be provided later through the Data Protection Officer Guidelines. For the time being, organisations/businesses should consider identifying suitable candidates for the role of DPOs and to allocate the resources to provide support to the DPOs.

- **Increased penalties for breach of Personal Data Protection Principles**

The Bill proposes to increase the penalties for the breach of the Personal Data Protection Principles to a fine of up to RM1,000,000 (approximately ¥33,250,000) and/or a term of imprisonment of up to 3 years. This is a significant increase from the fine of up to RM300,000 (approximately ¥9,2975,000) and/or term of imprisonment of 2 years prescribed in the current PDPA.

Organisations/businesses need to offer thorough training to employees about the significance of data protection and the specific requirements of the Personal Data Protection Principles, which can be done through a workshop or seminar session by the respective Legal or Compliance unit. They must implement and uphold strict compliance measures which include conducting regular audits and assessments to detect, address any potential breaches of the PDPA and take actions against employees who have been found to breach the PDPA.

[1] Section 9 of the PDPA, also known as the Security Principle states that a data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

- **Data Portability Rights**

Data subjects have the right to request a data controller to transfer their personal data directly to another data controller of their choice, as long as the transfer is technically feasible and compatible with the data formats. This request must be made in writing by the data subjects through electronic means to the data controller and the data controller shall complete the transmission of personal data within the period as may be prescribed.

Organisations/businesses should get ready to implement data portability rights operationally. This can be done by developing policies or protocol to manage such data portability request, training employees on the new data portability rights and the processes for handling such requests.
From the Public Consultation Paper No. 03/2024 The Right to Data Portability, it was clarified that this amendment only affects data that fulfils these requirements:

(a) directly provided by the data subject;
(b) processed based on consent or contract with the data subject;
(c) processed by automated means; and
(d) such data is not inferred/ derived data.

We understand that this would include data such as data subject's names, email address, identity card number or your music listening history. For example, your listening history or music preference on Spotify which creates a personal data can be ported out to another music streaming platform like Apple Music if it is generated in the same code or format. Once you change your music streaming platform from Spotify to Apple Music, Apple Music will know your music preference with the Data Portability Rights. Once the data is transferred out, it will be deleted if it is no longer necessary.

- **Updates to Cross-border Data Transfers Requirements**

The white-list regime (where a data user shall not transfer any personal data to a place outside Malaysia unless it is to a place specified by the Minister) in Section 129 of the PDPA will be removed as the Bill now allows for cross-border data transfers outside Malaysia under two circumstances; if that place has laws substantially similar to the PDPA or provides an adequate level of protection in relation to the processing of personal data at least equivalent to the level of protection afforded by the PDPA. We foresee organisations/businesses are required to assess and determine the level of data protection afforded by the country which receives such cross-border personal data.

However, the Bill retains the original Section 129(3)(a) of the PDPA which was previously relied on by businesses to transfer personal data abroad where a transfer of personal data to a place outside Malaysia is possible if the data subject has given his consent.

In other words, under the current PDPA, the process of obtaining consent from the data subject under Section 129(3)(a) to the transfer of personal data out of the country is still a lawful requirement even after the Bill takes effect. Given the difficulty in determining which countries provide the same level of protection as the Malaysian PDPA, we believe businesses would continue to rely on obtaining consent under Section 129(3)(a) of the PDPA.

- **Biometric Data is Recognised as Sensitive Personal Data**

The Bill defines "biometric data" as any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person and recognises it as sensitive personal data. Organisations/businesses need to ascertain whether they process biometric

data such as facial or fingerprint verification data and update their policies to comply with the stricter consent and security PDPA requirements that apply to the sensitive personal data.

- **Exclusion of Deceased Individuals from Data Subjects**

The Bill excludes deceased individuals from the definition of data subjects. As such, we believe PDPA and its principles will no longer apply to the processing of data related to deceased individuals. Where appropriate, organisations/businesses should update their internal policies to reflect such changes.

4. Conclusion

The amendments introduced by the Bill will certainly enhance data protection in Malaysia as the updates take into consideration the global trend of personal data and privacy framework across the world, once they take effect. This is a welcome move which offers organisations/businesses a chance to improve their data protection policies to be more consistent with international practices, consequentially making Malaysia a more desirous place for international trades.

Our team in Malaysia is well-versed in advising on various regulatory compliance personal data protection and privacy issues and we actively assist clients with their day-to-day operational and commercial concerns. If you would like to know more about our services, please feel free to contact us.

＜Authors＞

Yuki Hashimoto
One Asia Lawyers Malaysia
Lawyer (Japan)

He established his own firm in Japan and worked as a representative partner of a law firm with three offices in Japan. He has provided legal service as advisor to a wide range of organization in Japan, including companies in construction, real estate management, system development as well as local government and politic parties. He has been a member of One Asia Lawyers since September 2020, providing advice on general cross-border Asian legal matters (M&A, regulatory investigations, etc.) with a focus on Malaysia. yuki.hashimoto@oneasia.legal

Sharil Ramli
One Asia Lawyers Malaysia
Lawyer (Malaysia)

Sharil is a Senior Associate at One Asia Lawyers and is an attorney qualified in Malaysia. He is an experienced lawyer in cross border M&A transactions, private equity, regulatory compliance, corporate governance, data protection, employment, dispute resolution and general commercial transactions. He has provided legal advice to various clients including ministries, regulatory bodies, government agencies and corporations in financial services, capital market, telecommunication, construction, energy, oil and gas industries.

He is also a Certified Integrity Officer (CeIO) with the Malaysia Anti-Corruption Academy and previously sat in the panel of the Malaysian Mediation Centre as an Accredited Mediator. In 2016, he obtained a Master of Laws (LLM) from the University of Edinburgh with a Yayasan Khazanah scholarship.

sharil.ramli@oneasia.legal