

Overview of Amendments to the Malaysian Personal Data Protection Act 2010

Introduction

The Personal Data Protection Act 2010 (Act 709) ("**PDPA**") regulates the collection, use, and safeguarding of personal data in Malaysia, where such personal data is processed in the context of commercial activities.

On 16 July 2024, the highly anticipated Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**") was passed in the Malaysian House of Representatives (*Dewan Rakyat*).

According to Malaysia's Minister of Digital, Gobind Singh Deo ("**Minister of Digital**"), "*the proposed amendments to Act 709 (PDPA) aim to enhance policies, particularly in terms of security and enforcement, to address issues of personal data breaches and misuse in Malaysia.*"

The Amendment Bill reflects Malaysia's response to the rapid pace of technological change and society's increasing dependence on digital platforms for business, coupled with a growing demand for data protection. This article seeks to provide a broad overview of the key changes introduced by the Amendment Bill and preparatory steps which businesses in Malaysia may wish to consider implementing in anticipation of the Amendment Bill coming into force.

Nomenclature Update

The term "*data users*" will be substituted with "*data controllers*" to align with the terminology used in other data protection frameworks, such as the European Union's General Data Protection Regulation ("**GDPR**"). While this change is mainly terminological, existing data protection notices, policies, or agreements referencing "data user" may need to be updated to reflect the new terminology.

Deceased Individuals are not Data Subjects

The personal data of deceased individuals will be expressly excluded from the scope of the PDPA. Currently, the PDPA does not explicitly address the same.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my | T: +603 2201 5584

Shin Associates is a Malaysian-based law firm that is passionately driven to provide comprehensive legal advisory services of integrity and commercial edge, across national boundaries and on international platforms.

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal or other professional advice.

As a result, businesses may process the personal data of deceased individuals without being subject to the PDPA and the personal data protection principles (“**PDP Principles**”) thereunder. This could lead to an increase in data breaches and criminal activities, such as impersonation, scams, and fraud, by misusing the personal data of deceased individuals.

Increased Penalties

Currently, the maximum penalties for non-compliance with the PDP Principles are a fine not exceeding RM300,000.00 and/or imprisonment not exceeding 2 years. Under the Amendment Bill, the proposed penalties will be increased to a fine not exceeding RM1,000,000.00 and/or imprisonment not exceeding 3 years.

This amendment aligns with the global trend of strengthening enforcement of data protection laws in response to significant technological advancements that have led to an increase in data breach and online fraud cases. In 2023, a weekly average of 15 data breach cases were reported to the Department of Personal Data Protection (“**DPDP**”).

Application of Security Principle to Data Processors

Currently, the PDPA does not place specific obligations on data processors. However, under the Amendment Bill, data processors will be required to comply with the Security Principle under the PDPA. This principle mandates that data controllers and data processors must take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction.

Data processors, when processing on behalf of data controllers, will also need to provide sufficient guarantees regarding the technical and organizational security measures governing the processing and take reasonable steps to ensure compliance with those measures. Failure to comply with these additional obligations will attract increased penalties.

Notwithstanding the introduction of liability on data processors, data controllers will nevertheless remain primarily liable for any PDPA breaches.

In view of these developments, data controllers should ensure that their contracts with data processors are updated to codify the data processors’ guarantees stated above.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my | T: +603 2201 5584

Shin Associates is a Malaysian-based law firm that is passionately driven to provide comprehensive legal advisory services of integrity and commercial edge, across national boundaries and on international platforms.

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal or other professional advice.

Recognition of Biometric Data as Sensitive Personal Data

The definition of "*sensitive personal data*" in the PDPA will be expanded to include "*biometric data*". "*Biometric data*" is defined in the Amendment Bill as "*any personal data resulting from technical processing relating to the physical, physiological, or behavioural characteristics of a person*". This appears to include data obtained from fingerprint verification, voice recognition, or facial recognition.

As a result, businesses processing biometric data will need to comply with more stringent consent and security requirements applicable to "*sensitive personal data*" under the PDPA. In particular, such businesses will be required to obtain express consent from data subjects to process their biometric data, and expand the scope of their privacy notices to specifically address biometric data.

Appointment of Data Protection Officers

The Amendment Bill introduces a new mandatory requirement for data controllers and data processors to appoint one or more data protection officers ("**DPO**") to oversee compliance with the PDPA. The Commissioner of Personal Data Protection ("**Commissioner**") must be notified of the appointment of DPOs in such manner and form to be prescribed by the Commissioner at a later date.

The DPO requirement is not unique to Malaysia. Many other territories, such as the European Union and the Philippines, also mandate the appointment of a DPO, particularly in contexts involving extensive personal data processing.

In introducing the DPO requirement, it is apparent that Malaysia seeks to further align with international practices and standards vis-à-vis accountability for personal data protection matters.

While the Amendment Bill does not provide extensive information regarding the mechanics of appointing a DPO and their specific roles and duties, it is anticipated that these details (e.g. including notification process for DPO appointments, minimum qualifications, certifications, or expertise required of DPOs) may be addressed in future guidelines to be published by the Commissioner.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my | T: +603 2201 5584

Shin Associates is a Malaysian-based law firm that is passionately driven to provide comprehensive legal advisory services of integrity and commercial edge, across national boundaries and on international platforms.

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal or other professional advice.

Mandatory Data Breach Notification

The Amendment Bill imposes an obligation on data controllers to inform the Commissioner when there is reason to believe that a personal data breach has occurred. This applies when personal data has been compromised, hacked, or shared without authorization.

If the personal data breach *“causes or is likely to cause significant harm”* to the data subject, the data controller must notify the affected individuals without delay. Any data controller in contravention of this requirement shall be liable to a fine not exceeding RM250,000.00 and/or imprisonment not exceeding 2 years.

As the term *“causes or is likely to cause significant harm”* is not defined nor elaborated on in the Amendment Bill or the PDPA, data controllers may wish to adopt a conservative approach by notifying data subjects of any data breach, regardless of whether it is likely to cause significant harm or otherwise, in order to avoid penalties.

This amendment aligns with global trends in data protection legislation, such as the GDPR, which requires timely data breach notifications. Currently, there is no requirement to notify personal data breaches. The aim of this requirement is to ensure timely and appropriate measures are taken to mitigate the impact of the breach and to prevent further unauthorized access or disclosure of personal data. Additionally, it aims to ensure that incidents of data breaches involving personal data are under the surveillance and enforcement of the Commissioner.

The Amendment Bill is silent on specific requirements of this obligation, such as the time frame, steps, and mode of notification, and the threshold to inform data subjects or notify the Commissioner.

Right to Data Portability

The Amendment Bill introduces a new right to data portability. Data portability empowers users by allowing them to request the transfer of their personal data from one data controller to another.

Upon receiving a request for data portability, the data controller must complete the transmission of personal data within a prescribed period. It remains unclear whether this time period will be set by law, by the data subject, or by the data controller.

However, this right is qualified by technical feasibility and compatibility of data formats. If the data formats are incompatible, or if the transfer is technically impossible or prohibitively expensive, implementing data portability may not

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my | T: +603 2201 5584

Shin Associates is a Malaysian-based law firm that is passionately driven to provide comprehensive legal advisory services of integrity and commercial edge, across national boundaries and on international platforms.

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal or other professional advice.

be practical. This qualification ensures that the right to data portability does not impose undue burdens on service providers while still aiming to enhance data movement.

Data portability is a legal obligation in some jurisdictions, such as the GDPR, which requires companies to provide users with personal data in a structured, commonly used, and machine-readable format. In Malaysia, implementing data portability will be challenging as it necessitates the standardization of data formats across platforms. Data controllers may also need to invest in new technologies, software, or internal processes to ensure secure and efficient data transfer. For example, companies may need to redesign data collection, data processing, and data management systems to facilitate the transfer and extraction of data to ensure data security.

The Amendment Bill is similarly silent regarding the scope and application of this right. The DPDP is expected to issue guidelines on the implementation of data portability. In the meantime, data controllers can take the initiative by evaluating the personal data they possess and working on making it portable to be prepared for any portability requests that may arise.

Removal of Whitelisting Mechanism

The Amendment Bill removes the whitelisting mechanism under Section 129 of the PDPA and the power of the Commissioner to decide whether the cross-border transfer of personal data is necessary for public interests. Currently, the PDPA stipulates that a data user shall not transfer any personal data of a data subject to a place outside Malaysia unless specified by the Minister of Digital. The list of approved countries is known as the 'whitelist.' Since the enactment of the PDPA, no whitelist has been issued or gazetted.

The Amendment Bill allows the transfer of personal data outside of Malaysia if the destination country has similar personal data protection laws or ensures an adequate level of protection equivalent to the PDPA. It is important to note that the requirements under Section 129(3) of the PDPA, including obtaining consent and demonstrating necessity, must still be adhered to.

The Amendment Bill is silent on the specific criteria to be followed when determining whether the conditions for cross-border transfer have been met. This lack of clarity may require further guidance from the Commissioner to ensure compliance and proper implementation. Businesses may need to assess the adequacy of the receiving country's data protection standards for compliance with the Amendment Bill.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my | T: +603 2201 5584

Shin Associates is a Malaysian-based law firm that is passionately driven to provide comprehensive legal advisory services of integrity and commercial edge, across national boundaries and on international platforms.

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal or other professional advice.

Conclusion

The Amendment Bill represents a long-anticipated and greatly appreciated development in Malaysia's data protection regulatory framework. At the time of writing, there is no indication as to when the Amendment Bill will come into force. However, it is expected to receive royal assent and thereafter come into force on a date to be appointed by the Minister of Digital by notification in the Federal Government Gazette.

Specific details not covered in the Amendment Bill are expected to be further clarified in guidelines to be issued by the Commissioner and the DPDP. The Minister of Digital also announced that several guidelines are being developed to support the Amendment Bill's changes, including those on Data Breach Notification, Data Protection Officers, Data Portability, Cross-border Data Transfers, Data Protection Impact Assessments, Privacy by Design, and Profiling and Automated Decision-making.

The introduction of new obligations under the Amendment Bill further aligns the PDPA with internationally recognized standards. In view of these developments, businesses should closely monitor updates in the Malaysian personal data protection space and may need to reassess their data protection policies as well as allocate resources to ensure compliance. Given the lack of detailed implementation guidelines at the time of writing, there will likely be a transition period before the changes are fully enforced.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my | T: +603 2201 5584

Shin Associates is a Malaysian-based law firm that is passionately driven to provide comprehensive legal advisory services of integrity and commercial edge, across national boundaries and on international platforms.

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal or other professional advice.