TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION

The Personal Data Protection (Amendment) Bill 2024: An Analysis and Upcoming Developments

Introduction

On 31 July 2024, the Malaysian Parliament passed the long-awaited Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**"), tabled by Digital Minister Gobind Singh ("**Minister**").

The Amendment Bill has been in the works since the Malaysian Government initiated a review exercise in 2018 to update the Personal Data Protection Act 2010 ("**PDPA**"), in order to align the PDPA with international data protection standards and also to address issues arising from new and emerging ways of using and processing personal data.

The amendments proposed to be included in the Amendment Bill have evolved several times due to a variety of reasons, including changes of Ministers, Ministries, as well as the Personal Data Protection Commissioner ("**Commissioner**").

In our previous Legal Update, we provided a brief overview of the key changes introduced by the Amendment Bill. This Update therefore aims to provide further details regarding the Amendment Bill, including status of the Amendment Bill, upcoming developments that can be expected following the Amendment Bill, and brief compliance steps for organisations to take in view of these new changes.

Status of the Amendment Bill and Upcoming Developments

The Amendment Bill is currently awaiting royal assent and publication in the Federal Gazette before it becomes law. It is expected that this process will be completed by **October 2024**, at which point the Amendment Bill will officially come into effect.

In the interim, the Commissioner has issued three public consultation papers to seek feedback on the following upcoming guidelines which will supplement the Amendment Bill. These are:

1. the Public Consultation Paper No. 01/2024: The Implementation of Data Breach Notification Guideline ("**DBN PCP**");

2. the Public Consultation Paper No. 02/2024: The Appointment of Data Protection Officer Guideline ("**DPO PCP**"); and

3. the Public Consultation Paper No. 03/2024: the Right to Data Portability Guideline ("**Data Portability PCP**").

The consultation period for these public consultation papers has since concluded, but they offer valuable insights into how the upcoming guidelines will shape the implementation of the new changes introduced by the Amendment Bill. For further information regarding the proposed implementation details outlined in the public consultation papers, please refer to our Legal Update.

Given that the Amendment Bill is expected to come into effect soon, organisations should begin reviewing their personal data protection-related documentation and processes to ensure they are prepared to comply with the new changes introduced by the Amendment Bill when it takes effect.

The Key Changes Introduced by the Amendment Bill and How They Impact Organisations

The Amendment Bill contains eight key amendments, which are examined in turn below. Briefly, these amendments are:

1. replacement of the term "data users" with "data controllers";
2. recognition of biometric data as a type of sensitive personal data;
3. increased penalties for breach of the Personal Data Protection Principles ("**PDP Principles**");
4. extension of the Security Principle to data processors;
5. new data protection officer ("**DPO**") appointment obligation for both data users/data controllers and data processors;
6. new mandatory personal data breach notification regime for data users/data controllers, to both the Commissioner and affected data subjects;
7. new right to data portability for data subjects; and
8. removal of the whitelisting regime for cross border data transfers.

(1) Replacement of the Term "Data Users" with "Data Controllers"

At the outset, the Amendment Bill introduces global amendments to replace all references to "data users" in the PDPA with "data controllers", aligning with the terminology used in other data protection regimes such as the European Union General Data Protection Regulation ("**EU GDPR**").

Apart from streamlining the terminology for alignment with international data protection standards, this amendment does not materially impact the obligations of data users/data controllers under the PDPA.

Key Compliance Measures: While this change is largely cosmetic, moving forward businesses will need to use the term "data controllers" instead of "data users" (e.g. during the review of privacy notices to address other changes under the Amendment Bill).

(2) Recognition of Biometric Data as a Type of Sensitive Personal Data

Under the PDPA, "sensitive personal data" is a distinct sub-category of personal data that is subject to more stringent consent and security requirements compared to personal data in general, due to the sensitive nature of the information involved.

The PDPA currently recognises four types of personal datasets as sensitive personal data. This includes any information relating to an individual's:

- physical or mental health or condition;
- political opinions;
- religious beliefs or other beliefs of a similar nature; and
- commission or alleged commission of any offence.

The Amendment Bill recognises "biometric data" as a type of sensitive personal data. "Biometric data" is defined as any personal data resulting from technical processing relating to a person's physiological or behavioural characteristics.[1]

Examples of the potential types of personal datasets that will be considered as biometric data pursuant to the Amendment Bill include personal data processed for facial recognition, fingerprint verification, voice recognition, retinal analysis, keystroke analysis, gaze analysis (eye tracking), and handwritten signature analysis.

Key Compliance Measures: As sensitive personal data is subject to stricter consent and security requirements under the PDPA, businesses processing biometric data will need to review their documentation and processes to reflect these enhanced requirements. This may include reviewing the business' privacy notices and consent clauses, as well as ensuring that robust security measures are in place to protect biometric data.

(3) Increased Penalties for Breach of the PDP Principles

The seven Personal Data Protection Principles ("**PDP Principles**") outlined in the PDPA form the foundational requirements that data users/data controllers must comply with when handling/processing personal data.[2]

Currently, a breach of any of the PDP Principles carries a maximum penalty of a fine of up to RM300,000, or imprisonment for a term of up to two years, or both. In practice, the highest compound issued under the PDPA to date is RM108,000, which was imposed on a security services firm for breaching the General Principle, Disclosure Principle, and Retention Principle.

The Amendment Bill will increase the penalty for breach of the PDP Principles to a maximum penalty of a fine of up to RM1,000,000, or imprisonment for a term of up to three years, or both.[3]

Key Compliance Measures: While the increased penalties do not directly result in any specific compliance actions, they may indicate a shift toward stricter enforcement and more severe penalties

[1] Section 3(b) of the Amendment Bill.
[2] The seven PDP Principles consists of the (i) General Principle, (ii) Notice and Choice Principle, (iii) Disclosure Principle, (iv) Security Principle, (v) Retention Principle, (vi) Data Integrity Principle and (vii) Access Principle.
[3] Section 4(b) of the Amendment Bill.

moving forward. Businesses should take this opportunity to review their practices and consider conducting an audit to ensure they have adequate and comprehensive measures and documentation in place to demonstrate compliance with the PDPA in a holistic manner.

(4) Extension of the Security Principle to Data Processors

Similar to the data protection regimes in other jurisdictions (such as the EU GDPR), the PDPA distinguishes and regulates two main actors – data users/data controllers and data processors.

However, prior to the Amendment Bill, the PDPA only directly regulates data users. Data processors' obligations to comply with the PDPA have thus far been solely contractual in nature, typically imposed through their agreements with data users.

The Amendment Bill amends the PDPA to impose a direct obligation on data processors to comply with the requirements prescribed by the Security Principle under section 9 of the PDPA.[4] Failure to comply with these requirements will result in data processors being directly held liable for penalties under the PDPA.

In other words, data processors who breach the Security Principle risk facing a maximum penalty of a fine of up to RM1,000,000 and/or imprisonment for up to three years, under the increased penalties introduced by the Amendment Bill.

Key Compliance Measures: Now that data processors are subject to a direct obligation to comply with the PDPA, they would need to implement the necessary measures required by the Security Principle. This includes, among other things, ensuring they have a security policy that meets the minimum security standards prescribed by the Commissioner through the Personal Data Protection Standard 2015 ("**PDP Standard**"), as required by the Personal Data Protection Regulations 2013.

(5) New DPO Appointment Obligation for Both Data Users/Data Controllers and Data Processors

The Amendment Bill introduces a new obligation for both data users/data controllers and data processors to appoint a DPO for their organisation.[5] Appointed DPOs are required to be registered with the Commissioner and will be responsible for monitoring the data user/data processor's compliance with the PDPA as well as acting as the data user/data processor's contact point with the Commissioner.

The DPO PCP issued by the PCP provides further insights into the implementation of this new obligation, which will be detailed in the upcoming Appointment of Data Protection Officer Guidelines ("**DPO Guidelines**"). Notably, this requirement will not apply universally but will be limited to certain classes of organisations that engage in large-scale processing of personal data. Appointed DPOs will also be required to be ordinarily resident in Malaysia; however, they can be appointed internally or contracted externally.

The Amendment Bill, however, does not prescribe any penalties for non-compliance with the DPO appointment obligation. It remains to be seen if this will be separately addressed in the forthcoming guidelines or other subsidiary regulations.

[4] Sections 4(a) and 5 of the Amendment Bill.
[5] Section 6 of the Amendment Bill.

Key Compliance Measures: Businesses need to take note of the newly introduced requirement to appoint DPO for their organisations, and to ensure compliance with the requirements under the DPO Guidelines (once they are finalised).

Additionally, internal data protection policies and procedures will also need to be reviewed to ensure that the DPO's role and authority are formalised, well-defined and embedded within the organisation's data processing activities. This will help ensure that DPOs can carry out their responsibilities in the manner envisaged by the DPO PCP.

(6) New Mandatory Personal Data Breach Notification Regime

Under the current PDPA, notification of personal data breaches by data users/data controllers to both the Commissioner and affected data subjects is voluntary in nature.

The Amendment Bill imposes a new mandatory obligation on data users/data controllers to notify both the Commissioner and affected data subjects of personal data breaches. "Personal data breach" is broadly defined under the Amendment Bill to refer to any breach, loss, misuse or unauthorised access of personal data.

Failure to comply with this notification obligation may result in penalties of a fine of up to RM250,000, imprisonment for a term of up to two years, or both.

The DBN PCP provides further clarification on details regarding the notification obligation, including the threshold for when the notification obligation applies, the specific notification timeframe (e.g. 72 hours from the time the data user becomes aware of the personal data breach), the manner and form of notification required to the Commissioner and affected data subjects, and the obligations of data processors in relation to the new notification requirement.

Key Compliance Measures: Based on the information provided in the DBN PCP, data users / data controllers should start developing or reviewing their internal data breach management and reporting procedures, in anticipation of the implementation / enforcement of the new mandatory data breach obligation once the upcoming Implementation of Data Breach Notification Guidelines ("**DBN Guidelines**") is finalised and published.

Additionally, data users/data controllers will also need to review their template data processing contractual clauses and agreements entered into with their data processors in order to ensure the inclusion of provisions relating to (i) a data processors' obligations to notify data controllers of personal data breaches, and (ii) their responsibility to facilitate their respective data controllers' compliance with data breach notification obligations, amongst others.

(7) New Right to Data Portability for Data Subjects

The Amendment Bill introduces a new right of data portability, enabling data subjects to request a data user/data controller to directly transmit their personal data to another data user/data controller of their choice. For example, with the right of data portability, data subjects can request the transmission of their personal data directly from one healthcare service provider to another.

However, the right of a data subject to data portability is not absolute and will be subject to technical feasibility and data format compatibility. Notably, the Amendment Bill does not specify penalties for data users/data controllers who fail to comply with this right.

The Data Portability PCP provides further insights into key components for the implementation of the right to data portability, such as the types of personal datasets covered by the right and the fees that may be charged for responding/fulfilling data portability requests.

Key Compliance Measures: In anticipation of the finalisation and issuance of the Right to Data Portability Guidelines ("**Data Portability Guidelines**"), data users/data controllers will need to begin developing internal processes and guidelines to handle and respond to data portability requests.

(8) Removal of the Whitelisting Regime for Cross Border Data Transfers

Under section 129 of the PDPA, outbound transfers of personal data from Malaysia to foreign jurisdictions are primarily governed by two main mechanisms:

- **Whitelisting mechanism**: This mechanism allows data transfers to jurisdictions that have been whitelisted in the Federal Gazette by the Minister, pursuant to sections 129(1) and 129(2) of the PDPA. Whitelisting occurs when the Minister determines that the jurisdiction's laws are substantially similar to, or offer an adequate level of protection equivalent to the PDPA; or

- **Alternative conditions mechanism**: This allows for outbound transfers if the data user can comply with at least one of the conditions stipulated under section 129(3) of the PDPA, such as obtaining the data subject's consent for the transfer of their personal data.

However, no jurisdictions have been whitelisted to date. As a result, the Amendment Bill removes the whitelisting mechanism for cross-border data transfers. That said, the Amendment Bill does not entirely eliminate the concept of whitelisting from the PDPA.

In addition to the existing alternative conditions mechanism in section 129(3), data users or controllers may now transfer personal data abroad if they can demonstrate that the recipient jurisdiction's laws are substantially similar to, or offer an adequate level of protection equivalent to, the PDPA. This departs from practices in other jurisdictions, where adequacy-like mechanisms are typically determined by the supervisory authority rather than the data controllers themselves.

We believe that this amendment may pose practical challenges for organisations. By shifting the responsibility to data controllers to determine whether a third country's data protection laws are substantially similar to the PDPA or offer an adequate level of protection, organisations may need to engage external legal experts or consultants to make this determination. This could increase costs and require significant resources, particularly for smaller organisations.

The absence of a centralised adequacy mechanism could also lead to inconsistent assessments by different data controllers, creating further uncertainty and complexity in cross-border data flows. Furthermore, this amendment may inadvertently be counterintuitive to the Malaysian Government's efforts to promote more efficient and seamless cross-border data transfers for the digital economy.

Notwithstanding the above, the Commissioner is developing the Cross-Border Data Transfers Guidelines ("**Data Transfer Guidelines**"), which is intended to clarify the steps data users and data controllers must take to conduct outbound transfers of personal data under the amended section 129 of the PDPA. Additionally, based on past consultation sessions conducted by the Commissioner's office, we note that the Commissioner is considering the adoption of commonly used transfer mechanisms recognised by other jurisdictions, such as binding corporate rules and standard

contractual clauses. The Data Transfer Guidelines may provide further guidance on how these mechanisms will integrate with section 129 of the PDPA.

Key Compliance Measures: Once the Data Transfers Guidelines are issued by the Commissioner, data users/data controllers will need to ensure that they comply with the further requirements/guidance as outlined in the guidelines to conduct outbound transfers of personal data under the conditions prescribed by section 129(3) of the PDPA.

Upcoming Developments to Note

As highlighted above, public consultation papers for the upcoming guidelines are currently being developed by the Commissioner. These public consultation papers are in anticipation of a suite of supplementary guidelines which have been announced by the Digital Minister earlier this year and which are expected to be issued in stages, as per the following:

1. DBN Guidelines;
2. DPO Guidelines;
3. Data Portability Guidelines;
4. Data Transfer Guidelines;
5. Privacy by Design Guidelines; and
6. Profiling and Automated Decision-Making Guideline.

Now that the Commissioner has issued public consultation papers for the first three guidelines, namely the DBN Guidelines, DPO Guidelines and Data Portability Guidelines, we anticipate that public consultation papers for the remaining guidelines will similarly be issued in stages in due course.

In addition, the Commissioner has indicated that new subsidiary regulations may be introduced, along with amendments to existing subsidiary regulations, such as the PDP Standards (which relates to three PDP Principles, i.e. Security, Retention and Data Integrity). These guidelines and regulations are likely to be issued over the course of the upcoming year.

Over and above that, the Digital Minister has indicated that ongoing efforts are being made to review the PDPA, with further amendments expected to strengthen the PDPA in the near future.

Concluding Remarks

The introduction of the long-awaited Amendment Bill is a much-welcomed development in Malaysia's data protection regulatory landscape, following the protracted review exercise of the PDPA undertaken by the Malaysian Government since 2018.

As noted, with the many upcoming developments scheduled to take place, the Amendment Bill will be just the beginning of a series of improvements to Malaysia's data protection framework. We anticipate that further enhancements to the PDPA will be introduced by the Digital Minister and Commissioner in the coming months and years.

We recommend that businesses stay informed about developments regarding the guidelines being formulated and begin reviewing their internal data protection policies and practices to prepare for compliance with the new changes introduced by the Amendment Bill. While some of the new requirements and obligations are subject to further details to be provided in the upcoming guidelines, the public consultation papers issued thus far provide valuable insights for businesses to start reviewing and updating their personal data protection practices and documentation.

We trust the above provides a useful update on the latest developments regarding the PDPA and the Amendment Bill. Should you require any assistance or clarification in relation to the above, or any matter relating to personal data protection, please feel free to contact us at your convenience.

Contacts

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION PRACTICE GROUP

Deepak Pillai

HEAD

D +60 3 2275 2675
F +60 3 2273 8310
deepak.pillai@christopherleeong.com

Intan Haryati Binti Mohd Zulkifli

PARTNER

D +60 3 2675 2674
F +60 3 2273 8310
intan.haryati@christopherleeong.com

Anissa Maria Anis

PARTNER

D +60 3 2267 2750
F +60 3 2273 8310
anissa.anis@christopherleeong.com

Yong Shih Han

PARTNER

D +60 3 2273 1919
F +60 3 2273 8310
shih.han.yong@christopherleeong.com

Contribution Note

This Legal Update is contributed by the Contact Partners listed above, with the assistance of **Yeap Yee Lin** (Associate, Christopher & Lee Ong) and **Matthew Chang** (Associate, Christopher & Lee Ong).

Please feel free to also contact Knowledge Management at RTApublications@rajahtann.com.

Regional Contacts

Cambodia
Rajah & Tann Sok & Heng Law Office

T +855 23 963 112 / 113
kh.rajahtannasia.com

China
Rajah & Tann Singapore LLP
Shanghai & Shenzhen Representative Offices

T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

Indonesia
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

Lao PDR
Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

Malaysia
Christopher & Lee Ong

T +603 2273 1919
F +603 2273 8310
www.christopherleeong.com

Myanmar
Rajah & Tann Myanmar Company Limited

T +951 9253750
mm.rajahtannasia.com

Philippines
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)

T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

Singapore
Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand
Rajah & Tann (Thailand) Limited

T +66 2656 1991
F +66 2656 0833
th.rajahtannasia.com

Vietnam
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
vn.rajahtannasia.com

Our Regional Presence

Christopher & Lee Ong is a full service Malaysian law firm with offices in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of Christopher & Lee Ong, who are Malaysian-qualified, have accumulated considerable experience over the years in the Malaysian market. They have a profound understanding of the local business culture and the legal system and are able to provide clients with an insightful and dynamic brand of legal advice.

Christopher & Lee Ong is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.