NEWSLETTER

A Sea Change in Malaysia's Data Protection Framework (Part 3)

– New Guidelines on Appointment of Data Protection Officers and Data Breach Notifications Unveiled by the Commissioner –

Asia & Data Protection Newsletter April 8, 2025

Author:
Wan May Leong
w.m.leong@nishimura.com
Tomonobu Murata
to.murata@nishimura.com
Wai Kin Leo
waikin.leo@wmlaw.com.my
Ryan Heng
ryan.heng@wmlaw.com.my

Since our previous newsletter on this topic (which can be accessed here), there have been several developments relating to the entry into force of the amendments to the Malaysian Personal Data Protection Act 2010 ("**PDPA**").

New Guidelines issued by the Commissioner

The salient amendments to the PDPA under the Personal Data Protection (Amendment) Act 2024 ("**Amended Act**") include: (a) a requirement that each data controller and data processor appoint a data protection officer, and (b) the requirement that a data controller notify the Commissioner if it has reason to believe a personal data breach has occurred. Our article discussing the amendments to the PDPA, and the resulting Amended Act, can be accessed here.

On 25 February 2025, the Personal Data Protection Commissioner ("**Commissioner**") introduced the following personal data protection guidelines, which clarify these new requirements in the PDPA:

(a) Personal Data Protection Guideline on Appointment of Data Protection Officer ("**DPO Guidelines**"); and
(b) Personal Data Protection Guideline on Data Breach Notification ("**DBN Guidelines**").

These guidelines will come into force on 1 June 2025.

Overview of the DPO Guidelines

Section 12A of the PDPA introduces a new obligation for data controllers and data processors to appoint a data protection officer ("**DPO**") for purposes of overseeing compliance with the PDPA.

The DPO Guidelines contain additional guidance on the requirement for appointment of a DPO. The key requirements of the DPO Guidelines are summarized below.

No.	Aspect of the DPO Guidelines	Requirement In the DPO Guidelines
1.	Conditions for appointment of	Data controllers and data processors are required to appoint one or more DPOs if their processing of personal data involves:

	DPO	(a) personal data of more than 20,000 data subjects; (b) sensitive personal data, including financial information data, of more than 10,000 data subjects; or (c) activities that require regular and systematic monitoring of personal data (examples include any form of activity in which data subjects are tracked and profiled online or offline for purposes of behavioral advertising).
2.	Expertise and qualifications of DPO	Data controllers and data processors must ensure that the appointed DPO demonstrates a sound level of the following skills, qualities, and expertise: (a) knowledge of the PDPA and requirements for data protection practices in Malaysia; (b) understanding of the data controller/processor's business and personal data processing operations; (c) understanding of information technology and data security; (d) personal qualities such as integrity, understanding of corporate governance, and a high level of professional ethics; and (e) the ability to promote data protection culture within the organization. The data controller and processor must determine the necessary qualifications, experience, skills, and expertise of their DPO based on the data processing activities in which the data controller or processor engages.
3.	Method of appointing DPO	A DPO may be appointed from existing employees or through outsourcing services, based on a service contract with an individual or organization. If the DPO is appointed via a contract, it is recommended that the data controller or data processor ensure the appointment lasts for at least 2 years, to maintain stability.
4.	Notification of the appointment of DPO	Data controllers must notify the Commissioner of the appointed DPO and the DPO's business contact information within 21 days of the appointment, via the Personal Data Protection System (SPDP) (https://daftar.pdp.gov.my). The details of any changes must be provided via SPDP within 14 days of the relevant change.
5.	Responsibilities of DPO	The DPO shall have at least the following core responsibilities with respect to the data processing activities of the data controller or data processor: (a) provide information and advice to the data controller/processor on the processing of personal data; (b) support for compliance with the PDPA and related laws, including staying informed of data processing risks affecting the relevant data controller/processor; (c) support for carrying out Data Protection Impact Assessments in accordance with requirements determined by the Commissioner from time to time; (d) monitor the personal data compliance of the data controller/processor; (e) ensure proper data breach and security incident management by assisting with preparation, processing, and submission of reports and other documents

		required by the Commissioner with respect to personal data breaches; and (f) such additional responsibilities as the Commissioner or the data controller/processor may include from time to time (e.g., as a result of technological developments). Note that the data controller/processor must ensure that the DPO is provided with the necessary resources to enable the DPO to perform the relevant functions with sufficient independence and autonomy. The DPO also should have direct reporting access to the senior management of the data controller/processor.
6.	Matters relating to appointment of DPO	The DPO may carry out other official duties and responsibilities or perform additional tasks as part of his or her job. However, the data controller/processor shall ensure that the performance of other tasks and functions does not create a conflict of interest for the DPO. The DPO's position may be part-time or full-time, taking into account the organization's function, structure, and size.
7.	Accessibility of DPO	A DPO may serve multiple data controllers or data processors, provided that the DPO is easily accessible by the different entities that receive the DPO's services. The DPO also is required to be: (a) a resident in Malaysia (physically present in Malaysia for at least 180 days during one calendar year) or easily contactable via any means; and (b) proficient in the Bahasa Melayu and English languages.

Overview of DBN Guidelines

Section 12B of the PDPA imposes a new mandatory obligation on data controllers to notify both the Commissioner and affected data subjects of personal data breaches. Any failure in compliance may result in penalties of a fine of up to RM 250,000, imprisonment for a term of up to 2 years, or both.

The DBN Guidelines provide guidance to data controllers for compliance with this notice obligation, as summarized below:

No.	Aspect of the DBN Guidelines	Notification to the Commissioner	Notification to Affected Data Subjects
1.	Materiality threshold for notification of data breaches	A data controller is required to notify the Commissioner of a personal data breach if the breach causes, or is likely to cause, "significant harm," which means there is a risk that the compromised personal data: (a) may result in physical harm, financial loss, a negative effect on credit records, or damage to or loss of property;	A data controller is required to notify the affected data subjects if the personal data breach results, or is likely to result, in "*significant harm*." The factors to be considered in connection with notifications to the Commissioner apply, except for the "*significant scale*" criterion.

		(b) may be misused for illegal purposes; (c) consists of sensitive personal data; (d) consists of personal data and other personal information which, when combined, potentially could enable identity fraud to occur; or (e) is of significant scale (if the number of affected data subjects exceeds 1,000).	
2.	Timeframe for notification	The notification shall be made as soon as practicable, and no later than 72 hours after the occurrence of the personal data breach. If the data controller fails to give notice within 72 hours, it must provide a written explanation with supporting evidence, including an incident timeline, internal communications, and information about relevant factors that contributed to the delay.	The affected data subjects must be notified without unnecessary delay, not later than 7 days after the initial data breach notification is made to the Commissioner.
3.	Notification process and form	Notifications must be provided to the Commissioner through one of the following channels: (a) completing the notification form available on the official website of the Department of Personal Data Protection at http://www.pdp.gov.my/; or (b) completing the notification form in Annex B of the DBN Guidelines and submitting it via email to dbnpdp@pdp.gov.my or submitting a hard copy to the Commissioner.	Notice shall be given to the affected data subjects directly and individually, in a practicable manner, using intelligible language that is appropriate to the circumstances, in order to allow the data subjects to take necessary precautions or other measures to protect themselves against the possible adverse effects of the breach. If direct notice is not practicable or requires a disproportionate effort, the data controller may use alternative means of notification, such as public communication or any similar method that effectively informs affected data subjects of the personal data breach.
4.	Governance requirements	The data controller is required to put adequate data breach management and response plans in place. At a minimum, these plans must outline policies and procedures including (a) personal data breach identification and escalation procedures, (b) roles and responsibilities of relevant stakeholders (e.g., data breach response plan, DPO), and (c) steps to contain and mitigate the impact of the breach.	
5.	Personal data breach	The data controller is required to impose contractual obligations on its data processor to notify the data controller promptly about any data breaches that occur, and to	

	involving a data processor	provide all reasonable and necessary assistance to the data controller in connection with the data controller's compliance with its data breach notification obligations under the PDPA.
6.	Obligation to maintain records of personal data breaches	The data controller shall keep records and maintain a register detailing personal data breaches for a period of at least 2 years from the date of the notification to the Commissioner, including information about and records of breaches that did not meet the criteria for providing notifications to the Commissioner and/or affected data subjects.

In particular, it is recommended that data controllers review their contracts, and ensure they have sufficient contractual obligations in place to ensure that data processors provide prompt notice of data breaches and provide assistance with the data controller's data breach notification obligations.

Conclusion

The DPO Guidelines and DBN Guidelines provide valuable insights into relevant requirements in the amended PDPA. All organizations should consider the specific requirements in these guidelines carefully, and tailor implementation measures to ensure compliance before the amendments come into effect on 1 June 2025.

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com