Shearn Delamore &co.

Personal Data Protection Guidelines: Appointment of Data Protection Officer & Data Breach Notification

As anticipated in our December 2024 Legal Update, the phased implementation of the provisions of the Personal Data Protection (Amendment) Act 2024 ("**PDP Amendment Act**") is already underway. Among others, the newly introduced requirements for the appointment of data protection officer ("**DPO**") and data breach notification ("**DBN**") are set to come into force on 1 June 2025. This Legal Update summarises the recent regulatory developments relating to the appointment of DPO and DBN.

The Personal Data Protection Guideline on Appointment of Data Protection Officer ("**DPO Guidelines**") and Personal Data Protection Guideline on Data Breach Notification ("**DBN Guidelines**") have been issued pursuant to the Personal Data Protection Commissioner's ("**Commissioner**") functions under Section 48(g) of the Personal Data Protection Act 2010 ("**PDPA**"). They are to be read in conjunction with the Commissioner's Circular No. 1/2025 (Appointment of Data Protection Officer) and Circular No. 2/2025 (Data Breach Notification), respectively, which will come into force on 1 June 2025.

Appointment of Data Protection Officer

We discussed the requirement for DPO to be appointed in our July 2024 and December 2024 Legal Updates. Pursuant to the newly introduced Section 12A of the PDPA, data controllers and data processors are required to appoint one or more DPOs, who shall be accountable to the data controller or data processor (as the case may be). Notwithstanding the foregoing, such appointment shall not discharge the data controller or data processor from all duties and functions under the PDPA.

Pursuant to Circular No. 1/2025, the requirement for DPO appointment is subject to the conditions determined by the Commissioner. The DPO Guidelines now clarify that a data controller or data processor is required to appoint one or more DPOs if the processing of personal data involves:

Personal Data Protection & Privacy Laws Update

FEBRUARY 2025

Shearn Delamore & Co
7th Floor
Wisma Hamzah Kwong-Hing,
No 1, Leboh Ampang
50100, Kuala Lumpur, Malaysia
T: 603 2027 2727
F: 603 2078 5625
info@shearndelamore.com
www.shearndelamore.com
www.linkedin.com/company/shearn-delamore-&-co

- personal data of more than 20,000 data subjects;

- sensitive personal data including financial information data of more than 10,000 data subjects; or

- activities that require regular and systematic monitoring of personal data.

The DPO Guidelines provide several examples of activities that require regular and systematic monitoring of personal data; for instance, any form of activity where data subjects are tracked and profiled online or offline for purposes of behavioural advertising will be considered as an activity which requires regular and systematic monitoring of personal data, which in turn requires the relevant data controller or data processor to appoint one or more DPOs.

The DPO Guidelines also address, among others:

- the roles and responsibilities of DPOs, including advising the data controller or data processor on data processing matters, assisting the data controller or data processor with PDPA compliance, assisting with data protection impact assessments, ensuring proper data breach and security incident management, and acting as liaison officer with data subjects and the Commissioner;

- the DPO's engagement terms and criteria, including the minimum term of appointment and other related issues such as:

    - whether a part-time DPO is permissible;
    - whether a DPO may also assume other non-data protection responsibilities (e.g. risk management); and
    - whether the functions of the DPO may be outsourced;

- the accessibility of the DPO, including requirements on residency and language proficiency;

- the expertise and qualifications of DPOs. In this regard, while there are no minimum professional qualifications required prior to being appointed as a DPO (unless otherwise determined by the Commissioner), it is suggested that a DPO may need to possess a higher level of skill and expertise under certain circumstances, depending on factors such as the scale of sensitive personal data being processed, and the involvement of complex processing of personal data (e.g. cross-border transfer of personal data);

- the DPO's level of knowledge. The DPO must demonstrate a sound level of knowledge of, among others, the PDPA and other applicable data protection laws, and information technology and data security;

- the training of DPOs, including the requirement for DPOs to attend courses and training programmes as determined by the Commissioner;

- the independence of DPOs, including the requirement for DPOs to be provided with direct reporting access to the senior management (or its equivalent) of the data controller or data processor; and

- the obligations of the data controller and data processor to ensure the effective implementation of the DPO's role, including the requirement to notify the Commissioner about the appointment of a DPO within the prescribed timeframe, the requirement to involve the DPO in all personal data protection matters within the organisation, and the requirement to provide the DPO with adequate resources to carry out the DPO's duties effectively.

Data Breach Notification

Data breach notification, as required by the newly introduced Section 12B of the PDPA, has been discussed in our July 2024 and December 2024 Legal Updates. In summary, data controllers must notify the Commissioner of any personal data breaches as soon as practicable. Failure to do so could result in a fine of up to RM250,000 and/or imprisonment for up to 2 years. The relevant data subject must also be notified where the personal data breach causes or is likely to cause any significant harm to the data subject.

Pursuant to Circular No. 2/2025, DBN shall be made in the manner and form as determined by the Commissioner in the DBN Guidelines. The DBN Guidelines clarify that *not all* personal data breaches are notifiable to the Commissioner; as stated in the DBN Guidelines, a data controller is only required to notify the Commissioner if the personal data breach causes or is likely to cause "significant harm" – this seems to align the threshold for making DBN to the Commissioner with that for notifying the data subjects, even though based on a strict reading of Section 12B(1) of the PDPA, DBN is required to be made to the Commissioner regardless of the level of harm caused by the personal data breach.

In this regard, the DBN Guidelines set out, among others:

- the criteria for assessing if the personal data breach causes or is likely to cause significant harm;

- several examples of personal data breaches (which clarify that, among others, the mere alteration of personal data without permission, or the accidental delivery of email containing personal data to the wrong recipient, are considered as personal data breaches);

- several examples of situations where DBN has to be made to the Commissioner and/or the affected data subjects;

- the timelines for making DBN to the Commissioner (i.e. 72 hours) and affected data subjects, and the method for computing the timelines;

- the additional requirements in case of delayed DBN notification to the Commissioner beyond the 72-hour timeframe;

- the procedure and required information for making DBN to the Commissioner, including the possibility of disclosing information in phases where it is not possible for the data controller to provide all required information at the time of submitting the initial notification to the Commissioner;

- the DBN procedure in the event of personal data breach involving data processors or multiple data controllers;

- the manner of making DBN to the affected data subjects, including acceptable modes of public communication (e.g. website notification) where direct communication with the affected data subjects requires "disproportionate effort";

- the requirement for data controllers to have in place adequate data breach management and response plans;

- the requirement for data controllers to conduct periodic training, as well as awareness and simulation exercises, in order to ensure that employees are aware of their roles and responsibilities in assisting the data controller with responding to personal data breaches;

- the requirement for imposing DBN-related contractual obligations on data processors;

- the duty of data controllers to conduct assessment of data breach upon awareness of the breach, and to contain and reduce the potential impact resulting from the breach; and

- the duty to maintain records of personal data breaches.

These requirements, along with the necessary actions and responses, must be carefully considered and where appropriate, incorporated into a data controller's data breach response plan and playbook, as well as the relevant data breach response training, exercises and drills.

Where a personal data breach results in or otherwise involves a cyber security incident as defined by the Cyber Security Act 2024 ("**CSA**"), and where the data controller has also been designated as a national critical information infrastructure entity (commonly known as "NCII

entity") under the CSA, the data controller shall evaluate how the DBN requirements under the PDPA interact with the cyber security incident notification requirements under the CSA. The CSA and its requirements on the notification of cyber security incident have been discussed in our April 2024, August 2024 and December 2024 Legal Updates.

Data controllers within certain regulated sectors (e.g. the banking sector) shall also evaluate how the general DBN requirements under the PDPA may relate to their sectoral requirements that may already mandate similar notifications to be made to the relevant sectoral regulators (e.g. notification of customer information breach to Bank Negara Malaysia). This includes assessing how the general and sectoral requirements may align or conflict, and ensuring that any overlaps or discrepancies are effectively managed.

Concluding Remarks

The introduction of the DPO Guidelines and DBN Guidelines marks a significant milestone in the implementation of the PDP Amendment Act. Since its introduction, many organisations and businesses have already conducted audits and gap analyses of their existing data protection policies and procedures in anticipation of adopting new or updated data protection practices. In this regard, the DPO Guidelines and DBN Guidelines provide much-needed clarity, enabling organisations and businesses to assess the changes required to remain compliant with the requirements of the PDPA. Based on the necessary changes that have been identified, we recommend organisations and businesses to review and, where necessary, revise their data protection operations, policies, procedures, playbooks, and contracts, as well as human resource practices (to the extent the appointment of DPO is concerned), which should ideally streamline the otherwise complex compliance obligations.

For further enquiries, please contact:

Janet Toh Yoong San
Head, Personal Data Protection & Privacy
Co-Head, Technology, Media & Telco
E: janet.toh@shearndelamore.com
P: +603 2027 2978

Boo Cheng Xuan
Associate, Personal Data Protection & Privacy
Associate, Technology, Media & Telco
E: boo.chengxuan@shearndelamore.com
P: +603 2027 2662

Yee Yong Xuan
Associate, Personal Data Protection & Privacy
Associate, Technology, Media & Telco
E: yongxuan.yee@shearndelamore.com
P: +603 2027 2615