Steven Thiru
ADVOCATES & SOLICITORS

Malaysia's Guidelines on Data Protection Officers and Data Breach Notifications

Two key requirements introduced under the Personal Data Protection Act 2010 ("**PDPA**") are, firstly, the appointment of a Data Protection Officer ("**DPO**") and secondly, the issuance of a Data Breach Notification ("**DBN**") in the event of a personal data breach. These requirements will take effect on 1 June 2025.

The Personal Data Protection Commissioner ("**Commissioner**") recently published a comprehensive Guideline on Appointment of Data Protection Officer ("**DPO Guidelines**") and Guideline on Data Breach Notification ("**DBN Guidelines**"). This article seeks to summarise the key points from these Guidelines.

Data Protection Officers

1. When does a DPO need to be appointed?

Data controllers and data processors must appoint one or more DPOs if their processing of data involves:

(1) Personal data exceeding 20,000 data subjects;
(2) Sensitive personal data (including financial information data) exceeding 10,000 data subjects; or
(3) Activities that require regular and systematic monitoring of personal data (e.g. where data subjects are tracked and profiled online or offline for behavioural advertising, operating a telecommunications network, monitoring wellness, fitness and health data, and/or activities involving CCTVs or connected devices).

2. What are the criteria for a DPO?

While no minimum professional qualifications are mandated, a DPO must:

(1) Be resident in Malaysia (i.e. be physically present in Malaysia for at least 180 days in one calendar year) OR be easily contactable via any means;
(2) Be proficient in Bahasa Malaysia and English; and
(3) Demonstrate a sound level of the following:
  (a) Knowledge on the PDPA and data protection practices in the country;
  (b) Understanding of the data controller / data processor's business operations and the personal data processing operations that are carried out;
  (c) Understanding of information technology and data security;
  (d) Personal qualities such as integrity, understanding of corporate governance, and high professional ethics; and
  (e) Ability to promote data protection culture within the organisation.

3. How is a DPO appointed?

A DPO may be appointed internally from among existing employees or through outsourcing services. If appointed on a contract basis, the appointment should be

for at least two (2) years to ensure stability.

A DPO may also be appointed to serve multiple organisations, provided that they are easily accessible.

Data controllers must:

(1) Register the appointed DPO and submit their business contact information within 21 days from the date of appointment;
(2) Notify the Commissioner of the appointment through the Personal Data Protection System; and
(3) Update any change in the appointed DPO or DPO's business contact information within 14 days.

4. What are a DPO's functions and responsibilities?

Amongst others, the DPO is required to:

(1) Inform and advise the data controller/data processor on the processing of personal data;
(2) Support compliance with the PDPA and other related data protection laws;
(3) Support the carrying out of Data Protection Impact Assessments;
(4) Monitor personal data compliance; and
(5) Ensure proper data breach and security incident management.

It is important that the DPO performs their functions with sufficient independence and autonomy. The data controller/data processor must avoid placing the DPO in positions that could cause conflict between business interests and PDPA compliance. The DPO should have direct reporting access to senior management (or equivalent).

Further, a DPO cannot be dismissed for performing their duties in good faith, unless the DPO has breached applicable laws and/or is found to have committed negligence or misconduct.

5. What are a data controller/data processor's responsibilities in respect of a DPO?

Critically, the appointment of a DPO does not discharge a data controller/data processor from its obligations under the PDPA, and they remain liable for any non-compliance under the PDPA.

Amongst others, data controllers/data processors must:

(1) Ensure that the DPO is involved in personal data protection matters in a timely manner;
(2) Engage the DPO in all data protection matters;
(3) Ensure that the DPO is provided with adequate resources to carry out tasks effectively;
(4) Create a dedicated official email account for the DPO, which must be actively monitored and maintained, and distinct from the DPO's personal and business email addresses;
(5) Publish the DPO's business contact information through its official website or other official media, personal data protection notices, and/or security policies and guidelines; and
(6) Accurately maintain and retain records of the appointed DPO.

Steven Thiru
ADVOCATES & SOLICITORS

Data Breach Notifications

1. **When is a DBN required to be issued to the Commissioner?**
   A DBN must be issued to the Commissioner in the event of a personal data breach, if the personal data breach causes or is likely to cause significant harm.

   In this regard, a personal data breach refers to any event / incident that leads or is likely to lead to the breach, loss, misuse or unauthorised access of personal data, whether it is caused accidentally or deliberately, internally or externally. For example, unauthorised third-party access to personal data held by the data controller, personal data sent to incorrect recipients, and alteration of personal data without permission.

   In respect of "significant harm", a personal data breach is considered to cause or be likely to cause "significant harm" if there is a risk that the compromised personal data:

   (1) May result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
   (2) May be misused for illegal purposes;
   (3) Consists of sensitive personal data;
   (4) Consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or
   (5) Is of significant scale (i.e. if the number of affected data subjects exceeds 1,000).

   The notification shall be made as soon as practicable and no later than 72 hours from the occurrence of the personal data breach.

2. **How is a DBN made to the Commissioner?**
   A DBN is made by completing the notification form available on the Department of Personal Data Protection's website or completing the notification form in the DBN Guidelines and submitting it to the Commissioner via email or hard copy.

3. **When is a DBN required to be issued to the affected data subjects?**
   Data controllers must notify data subjects of a personal data breach, if the breach results in or is likely to result in "significant harm" to the data subjects.

   "Significant harm", as defined above, also applies for the purpose of notifying data subjects, except for the "significant scale" criterion.

   The DBN must be issued without unnecessary delay, not more than seven (7) days after the initial DBN is made to the Commissioner.

4. **How should a DBN be communicated to the affected data subjects?**
   Data controllers must issue the DBN to the affected data subjects:

   (1) Directly;
   (2) Individually; and
   (3) In a practicable manner using intelligible language appropriate to the circumstances, to allow the data subjects to take necessary precautions or measures to protect themselves against possible adverse effects of the breach.

However, if direct notification is not practicable or requires a disproportionate effort, the data controller may use alternative means of notification. This includes public communication or any similar method that effectively informs affected data subjects of the personal data breach.

5. What must the DBN to affected data subjects include?

The DBN to affected data subjects must include:

(1) Details of the personal data breach that has occurred;
(2) Details on the potential consequences resulting from the breach;
(3) Measures taken or proposed to be taken by the data controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects;
(4) Measures that the affected data subjects may take to eliminate or mitigate any potential adverse effects resulting from the data breach; and
(5) Contact details of the DPO or other contact point from whom more information regarding the breach can be obtained.

6. What other obligations do data controllers have?

In addition to issuing DBNs, data controllers are also required to:

(1) Put in place adequate data breach management and response plans;
(2) Where data controllers work with data processors, contractually impose an obligation on the data processor to promptly notify them about a data breach that has occurred;
(3) Act promptly as soon as they become aware of any personal data breach to assess, contain and reduce the potential impact of the data breach. The data controller should consider the immediate containment actions required, where applicable, and identify relevant key information during the initial investigation;
(4) Keep records and main a register detailing all personal data breaches for a period of at least two (2) years from the date of the notification to the Commissioner, including those that did not meet the notification criteria for informing the Commissioner and/or affected data subjects; and
(5) Comply with other applicable notification obligations under Malaysian laws. This may include notification to the Royal Malaysia Police, Bank Negara Malaysia, Securities Commission Malaysia, and Malaysian Communications and Multimedia Commission if the breaches involve criminal activity or regulated industries.

Conclusion

Please refer to the Personal Data Protection Guideline on Appointment of Data Protection Officers and Personal Data Protection Guideline on Data Breach Notification for the full guidelines.

These Guidelines offer clear and detailed insights into the responsibilities of data controllers and data processors concerning DPOs and DBNs, as well as the role and function of DPOs. To mitigate the risk of

regulatory penalties, data controllers and data processors should adopt proactive measures to ensure full compliance with the PDPA.

Written by:
Priscilla Faith Lim
Associate

For any related enquiries, please contact our Partner, David Dinesh Mathew (ddm@steventhiru.my) or Associate, Priscilla Faith Lim (pfl@steventhiru.my)