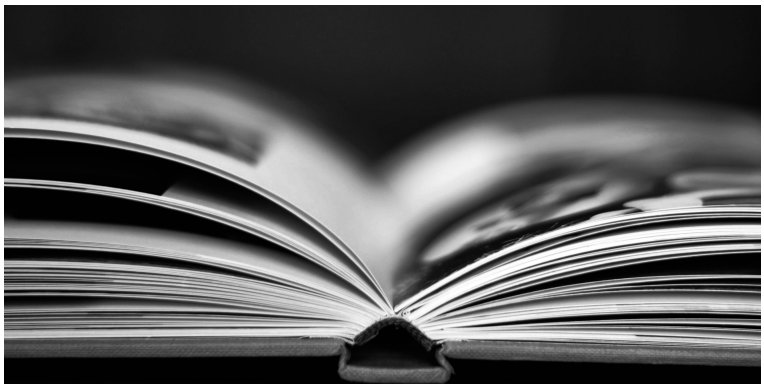

JEFF LEONG, POON & WONG

JLPW INSIGHTS CORPORATE LAW

FEBRUARY 2025

Legal Updates on Personal Data Protection

Summary of the Guideline on Data Breach Notification

Introduction

The long-anticipated amendments to the Personal Data Protection Act 2010 ("**PDPA 2010**") that were gazetted in October last year, introduced a requirement for data controllers to notify the Personal Data Protection Commissioner ("**Commissioner**") and affected data subjects if a data breach occurs (amongst other amendments). These amendments came into force on 1 January 2025.

Following the gazettement, the Department of Personal Data Protection ("**JPDP**") had in November 2024 announced that the Commissioner would release guidelines and a standard by early 2025 on compliance with the new requirements introduced by the amendments.

The Commissioner has now on 25 February 2025 issued a circular ("**Circular No. 2/2025**") as well as a guideline on data breach notifications ("**DBN Guideline**"), and we hope to provide a meaningful and concise summary below.

Defined Terms

Throughout this summary, we will be using certain defined terms from the PDPA 2010 which are explained below for your ease of reference.

"**data controller**"	:	means anyone other than a data processor, who processes personal data, or controls or authorises the processing of personal data.
"**data processor**"	:	means anyone who processes personal data only on behalf of a data controller and does not process the personal data for their own purposes. An employee of a data controller is not considered a data processor.
"**data subject**"	:	means the individual who is the subject of the personal data;
"**personal data**"	:	means any data from which a person can be identified;
"**sensitive personal data**"	:	means personal data containing information on a data subject's physical or mental health, political opinions, religious beliefs, commission of offences or alleged commission of offences and biometric data.

Definition of Personal Data Breach

Under section 2 of the PDPA 2010, a personal data breach is defined as any breach, loss, misuse or unauthorized access of personal data. The DBN Guideline expands this definition to include any event or incident that is likely to lead to such breach.

Requirement to Notify the Commissioner

In accordance with section 12B(1) of the PDPA 2010, if a data controller has reason to believe that a personal data breach has occurred, the data controller must notify the Commissioner as soon as practicable. The DBN Guideline clarifies that not all personal data breaches are required to be notified to the Commissioner, but only personal data breaches that cause or are likely to cause significant harm.

A personal data breach causes or is likely to cause significant harm if there is a risk of any of the following:

- the personal data breach may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
- the compromised personal data may be misused for illegal purposes;
- the compromised personal data consists of sensitive personal data;
- the compromised personal data consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or
- the personal data breach affects more than 1,000 data subjects, i.e. it is of significant scale.

Where a personal data breach involves more than 1 data controller, each data controller must submit a notification to the Commissioner.

It is important to note that the mandatory personal data breach notification obligations do not apply to data processors. Data controllers must contractually impose obligations on data processors engaged by them (if any) to notify them of data breaches that occur and to provide all reasonable and necessary assistance to meet data breach notification obligations.

Timing of the Notification to the Commissioner

Notification is required to be made as soon as practicable within 72 hours from the occurrence of the personal data breach.

On this point, it is worth noting that based on the examples provided in the DBN Guideline, the computation of the 72 hours is from the time that the data controller is made aware of a personal data breach, or from the time that the data controller confirms that a personal data breach has occurred, as applicable.

Format of the Notification to the Commissioner

Notification to the Commissioner may be made through completing the notification form available on the official website of JPDP or by completing the notification form in Annex B of the DBN Guideline and submitting it through e-mail or by hand.

Along with the notification form, the data controller is also required to provide the below listed information to the Commissioner. If this is not possible at the time of the initial notification, the information may be provided in phases, as soon as practicable within 30 days from the date of the initial notification.

The requested information is as follows:

- details of the personal data breach, including:
  - the date and time the personal data breach was detected by the data controller;
  - the type of personal data involved and the nature of the breach;
  - the method used to identify the breach and the suspected cause of the incident;
  - the number of affected data subjects;
  - the estimated number of affected data records; and
  - the personal data system affected, which resulted in the breach;
- the potential consequences arising from the personal data breach;
- the chronology of events leading to the loss of control over personal data;
- measures taken or proposed to be taken by the data controller to address the personal data breach, including steps implemented or planned to mitigate the possible adverse effects of the breach;
- measures taken or proposed to be taken to address the affected data subjects; and
- the contact details of the data protection officer or any other relevant contact person from whom further information on the personal data breach may be obtained.

If the data controller fails to notify the Commissioner within the 72-hour timeframe, written notice must be submitted to the Commissioner, detailing the reasons for delay and providing supporting evidence, including documentation of the incident timeline, internal communications and any technical issues or external factors that contributed to the delay.

Requirement to Notify Data Subjects

In accordance with section 12B(2) of the PDPA 2010, data controllers are additionally required under section 12B(2) of the PDPA 2010 to notify affected data subjects without unnecessary delay if the personal data breach causes or is likely to cause any significant harm.

The DBN Guideline clarifies that the criteria for assessing significant harm for notification to the Commissioner also applies for the notification to affected data subjects, save for the significant scale criterion.

Timing of the Notification to Data Subjects

Notification is required to be made without unnecessary delay within 7 days from the date of the initial notification to the Commissioner.

Format of the Notification to Data Subjects

The notification to affected data subjects shall be provided directly and individually in a practical manner, using clear and appropriate language, to allow data subjects to take necessary precautions to protect themselves. Such notification should be separate from other communication, such as regular updates or newsletters, so that the communication is clear and transparent.

If direct notification is not practical, the data controller may use alternative means of notification, such as public announcement or other similar methods.

The notification must include the following information:

- the details of the personal data breach that has occurred;
- details on the potential consequences resulting from the personal data breach;
- measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
- measures that the affected data subjects may take to eliminate or mitigate any potential adverse effects resulting from the data breach; and
- the contact details of the data protection officer or other contact point from whom more information regarding the personal data breach can be obtained.

Assessment Requirements

Data controllers should act promptly upon becoming aware of any personal data breach to assess, contain and reduce its potential impact.

Data controllers may consider the following immediate containment actions, as applicable:

- isolate and disconnect the compromised database or system from the network;
- suspend or disable compromised access rights;
- stop the practices identified as having caused the data breach; and
- determine whether the lost data can be recovered or whether any immediate remedial action can be taken to minimise further harm caused by the breach.

During the investigation, data controllers should also identify the following:

- the type(s) of personal data involved;
- the number of affected data subjects;
- the systems, servers, databases, platforms and services affected;
- the chronology of events leading to the data breach;
- the severity of the data breach;
- the root cause of the data breach, and whether it is still ongoing;
- the harm and potential harm that may result from the data breach;
- the measures that should be taken to contain the data breach, and mitigate its possible adverse effects; and
- the remedial actions that should be taken to reduce the harm to affected data subjects.

The data controller should conduct a post-breach evaluation to review the effectiveness of their data breach management and response plan, as well as their data protection practices and policies to prevent the recurrence of similar incidents.

Governance Requirements

In addition to notification procedures, the DBN Guideline requires a data breach management and response plan to be put in place by data controllers, with a focus on prompt identification of personal data breaches and appropriate measures to contain and mitigate any breaches as well as ensure compliance with data breach notification obligations.

A data breach management and response plan should outline the following:

- personal data breach identification and escalation procedures;
- roles and responsibilities of relevant stakeholders (e.g., the data breach
- response plan, the data protection officer);
- steps to contain and mitigate the impact of the breach;
- steps to determine whether it is necessary to notify the Commissioner and/or the affected data subjects;
- communication plan for notifying the Commissioner and/or the affected data subjects; and
- post-incident review.

Data controllers should also conduct periodic training as well as awareness and simulation exercises, to ensure that employees are aware of their roles and responsibilities in responding to a personal data breach.

Record Keeping Requirements

Data controllers must keep records and maintain a register detailing personal data breaches for at least 2 years from the date of the notification to the Commissioner. Such records and register should also detail any personal data breaches that were not required to be notified to the Commissioner, but the timeframe for retention is not mentioned. The documentation must be made available on request by the Commissioner.

The register should document the following information:

- description of the personal data breach, including the date and time the data controller became aware of the personal data breach, an analysis and identification of the root cause, the type of personal data involved, the estimated number of affected data subjects, the estimated number of affected data records and the compromised personal data system
- which allowed the breach to occur;
- description of the likely consequences of the personal data breach;
- description of a chronology of the events leading to personal data breach;
- containment and recovery measures taken to address the personal databreach; and
- details of notifications made to the Commissioner and/or affected data subjects and justification for not making notifications, where applicable.

Concerns

During our perusal of the DBN Guideline, we noticed that there is a discrepancy with the PDPA 2010 on what constitutes a personal data breach. Under section 2 of the PDPA 2010, a personal data breach is defined as any breach, loss, misuse or unauthorized access of personal data. However, under the DBN Guideline, a personal data breach also includes any event or incident that is likely to lead to such breach, loss, misuse or unauthorised access.

There is also a discrepancy on when notifications are required to be made to the Commissioner. In accordance with section 12B(1) of the PDPA 2010, if a data controller has reason to believe that a personal data breach has occurred, the data controller must notify the Commissioner as soon as practicable. Data controllers are additionally required under section 12B(2) of the PDPA 2010 to notify affected data subjects without unnecessary delay if the personal data breach causes or is likely to cause any significant harm.

The difference between sections 12B(1) and (2) of the PDPA 2010 (that is where subsection 12B(1) requires notification to the Commissioner of personal data breaches but subsection 12B(2) requires notification to the data subject only where the personal data breach causes or is likely to cause significant harm) implies that there is a difference between the breaches where notification is required to the Commissioner than those where notification is required to the data subject.

However, the DBN Guideline provides that notification to the Commissioner is only required for personal data breaches that cause or are likely to cause significant harm. The DBN Guideline further states that the criteria to assess significant harm are the same for both notification to the Commissioner and notifications to data subjects (except for the significant scale criterion).

These discrepancies between the PDPA 2010 and the DBN Guideline (as well as Circular No. 2/2025) may lead to confusion and a lack of clarity.

To illustrate, an example given by the DBN Guideline of a personal data breach is the accidental sending of letters containing personal data to the wrong recipient. As the definition of a personal data breach under the DBN Guideline is very wide (including events or incidents likely to lead to a breach), and the requirement for notification to the Commissioner under the PDPA 2010 is also very wide (being of all personal data breaches whether of significant harm or otherwise). Data controllers may then be required to notify the Commissioner every time it logs similar email addresses.

We urge the JPDP to clarify these discrepancies.

The full Circular 2/2025 and the DBN Guideline are available on the official website of JPDP here.

Prepared by **Alicia Teoh** (Partner)

Jeff Leong, Poon & Wong
Advocates & Solicitors
B-11-8, Block B, Megan Avenue II
Jalan Yap Kwan Seng
50450 Kuala Lumpur

Telephone : +60 3 2203 3388
Facsimile : +60 3 2203 3399
E-mail : alicia.teoh@jlpw.com.my