MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION GUIDELINE

DBN

DATA BREACH NOTIFICATION

Version 1.0
Date of Issuance: 25 February 2025

Personal Data Protection Commissioner Malaysia

Address:

PERSONAL DATA PROTECTION COMMISSIONER OF MALAYSIA

Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana

Precinct 4, Federal Government Administration Centre

62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1 Background

1.1 Section 12B of the Personal Data Protection Act 2010 *[Act 709]* ("**Act 709**") introduces a mandatory requirement for data controller to notify the Personal Data Protection Commissioner ("**Commissioner**") and affected data subjects if the data controller has reasons to believe that a personal data breach has occurred.

1.2 This guideline sets out the procedure for data controller to notify the Commissioner and affected data subjects of a personal data breach, ensuring that such breaches are managed effectively and in compliance with the requirements of Act 709.

1.3 Please note that the examples provided in this Guideline are not intended to be exhaustive and are only included for context and for purposes of illustration.

1.4 This Guideline is to be read together with Act 709, Circular of Personal Data Protection Commissioner No. 2/2025 (Data Breach Notification) ("**Circular No. 2/2025**"), and any other relevant legislative instruments issued under the Act 709. This Guideline does not override any other specific data protection laws or data protection regulations in effect at any given time.

2 Legal Provisions

2.1 This Guideline is issued by the Commissioner pursuant to the functions of the Commissioner under subsection 48(g) of the Act 709.

2.2 In accordance with Section 12B(3) of the Act 709, any data controller who fails to comply with Section 12B(1) of the Act 709 shall, on conviction, be liable to a fine not exceeding two hundred and fifty thousand ringgit (RM250,000) or to imprisonment for a term not exceeding two (2) years or to both.

3 Interpretation

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings assigned to them under the Act 709, the Circular No. 2/2025 and any other relevant legislative instruments under the Act 709.

3.2 In this Guideline, unless the context otherwise requires:

"security incident"	means an event or occurrence that affects or tends to affect data protection or may compromise the availability, confidentiality or integrity of data;
"personal data breach"	means as defined in section 4 of the Act 709 and is not limited to modification, duplication, alteration or destruction.

PART B: REQUIREMENTS FOR PERSONAL DATA BREACH NOTIFICATION TO THE COMMISSIONER

4 What Constitutes a "Personal Data Breach"?

4.1 The notification obligation under Act 709 only applies in the event of a "personal data breach" as defined by the Act 709 and the Circular No. 2/2025. Therefore, it is essential for a data controller to be able to recognise and determine what constitutes a "personal data breach".

4.2 A "personal data breach" broadly refers to any event / incident that leads or is likely to lead to the breach, loss, misuse or unauthorised access of personal data. A personal data breach may be caused by accidental or deliberate actions, either internally or externally.

Examples:

(i) Access to personal data held by the data controller by unauthorised third party.

(ii) An employee accidentally sending an email containing personal data to the wrong recipient.

(iii) An employee accidentally losing / misplacing a company-issued laptop containing unencrypted personal data, leading to potential unauthorised access of personal data.

(iv) An employee with authorised access to sensitive personal data deliberately stealing personal data (e.g., customer information) and selling it to a third party.

(v) An external party gaining access by unlawful means to the data controller's network or user accounts and extracting personal data.

(vi) A system misconfiguration leading to the loss of personal data or inadvertent sharing of personal data with third party.

(vii) The alteration of personal data without permission.

(viii) A temporary or permanent loss of availability of personal data (such as situations where unauthorised third party holds personal data hostage by preventing the data controller from gaining access to it, or situations where the corresponding decryption key to encrypted data has been lost).

(ix) An employee misplacing or losing physical documents containing personal data such as medical records, financial statements, etc., during transit or storage.

(x) An employee leaving personal data such as forms with identification details unattended on desks or in open areas where unauthorised individuals can view them.

(xi) The sending of letters or forms containing personal data such as invoices or financial statements to the wrong recipient.

5 Personal Data Breach that Must be Notified to the Commissioner

5.1 Not all personal data breaches are notifiable to the Commissioner. A data controller is only required to notify the Commissioner of a personal data breach if the personal data breach causes or is likely to cause "*significant harm*".

What is "significant harm"?

5.2 A personal data breach is considered to cause or is likely to cause "*significant harm*" if there is a risk that the compromised personal data:

5.2.1 may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;

5.2.2 may be misused for illegal purposes;

5.2.3 consists of sensitive personal data;

5.2.4 consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or

5.2.5 is of significant scale.

What is "significant scale"?

5.3 A personal data breach is considered to be of *"significant scale"* if the number of affected data subjects exceeds one thousand (1,000).

Examples of Personal Data Breach

5.4 Examples of personal data breach scenarios, where the data controller is required to notify the Commissioner:

Example	**Whether Notification to the Commissioner is Required**
An employee loses a laptop containing personal data of customers.	Yes, if the type of datasets compromised are those that may result in "*significant harm*, or if the breach involves more than 1,000 affected data subjects.
Unauthorised third-party gains access to the medical records of patients.	Yes, because a breach involving "sensitive personal data" (i.e., medical records) is considered to be of "*significant harm*", regardless of whether the number of affected data subjects exceeds 1,000 data subjects.
Theft of an encrypted laptop containing the email addresses of 200 employees of an organisation.	No, the disclosure of the e-mail addresses of employees is not likely to result in any "*significant harm*".
Medical records in a hospital are temporarily inaccessible due to a cyberattack.	Yes, because a breach involving "sensitive personal data" (i.e., medical records) is considered to have the potential to cause "*significant harm*", regardless of whether the number of affected data subjects exceeds 1,000.
An e-mail containing the account statement of a customer was sent to the wrong recipient.	Yes, because the compromised personal data involves the financial information of a data subject.

5.5 The data controller shall assess whether a 'personal data breach' meets any of the notification criteria stipulated in paragraph 5.2. If any of the criteria is met, the data controller shall notify the Commissioner of the breach.

6 Timeframes for Notification to the Commissioner

6.1 The notification shall be made as soon as practicable and no later than seventy-two (72) hours from the occurrence of the personal data breach.

Computation of the 72-hour Timeframe for Notification

6.2 Once the data controller is informed by an individual, a media organisation, or any other source, or detects a security incident, he shall conduct a preliminary investigation to determine whether a personal data breach has actually occurred.

Examples:

The following are examples of the computation of the 72-hour timeframe for submission of data breach notification to the Commissioner:

(i) When a USB key containing unencrypted personal data is reported as lost, the 72-hour notification period to the Commissioner begins as soon as the data controller is informed of the loss.

(ii) The 72-hour notification period to the Commissioner begins as soon as the data controller unintentionally sends personal data without authorisation and realises the mistake."

(iii) In cases where a data controller's network is potentially compromised or infiltrated, the 72-hour notification period to the Commissioner begins as soon as the data controller confirms, during the inspection of their system, that the system has indeed been compromised.

(iv) A ransomware attack is a type of cyberattack in which criminals encrypt the victim's data and prevent them from accessing their system. The criminals then demand a ransom payment to restore the victim's access. In such cases, the 72-hour notification period to the Commissioner begins when the data controller realises he has lost access to the data or, after being informed by the cybercriminal of the breach, conduct own assessment and confirm that a personal data breach has occurred.

(v) Where a data processor processes data on behalf of a data controller, the 72-hour notification period to the Commissioner begins once the data processor notifies the data controller of the personal data breach or when the data controller itself obtains clear evidence that a personal data breach has occurred, whichever is earlier."

7 Notification Process to the Commissioner

Format and Channels of Notification

7.1 Notification to the Commissioner shall be made through one of the following channels:

7.1.1 completing the notification form available on the official website of the Department of Personal Data Protection (JPDP) at www.pdp.gov.my;

7.1.2 completing the notification form in **Annex B** and submitting it to the official e-mail address dbnpdp@pdp.gov.my; or

7.1.3 completing the notification form in **Annex B** and submitting a hard copy to the Commissioner.

Notification in Phases

7.2 The data controller shall ensure that all required / mandatory information fields in the notification form in paragraph 7.1 are completed, and that the notification to the Commissioner, through the methods specified in paragraph 7.1, is submitted within the prescribed seventy-two (72) hours.

7.3 The Commissioner will issue a confirmation notice to the data controller upon receiving the personal data breach notification. The notification will not be considered submitted to the Commissioner without this confirmation notice.

7.4 In addition to the required / mandatory fields in the notification form submitted under paragraph 7.1, the data controller shall also provide the Commissioner with the following information:

7.4.1 Details of the personal data breach, including:

7.4.1.1 the date and time the personal data breach was detected by the data controller;

7.4.1.2 the type of personal data involved and the nature of the breach;

7.4.1.3 the method used to identify the breach and the suspected cause of the incident;

7.4.1.4 the number of affected data subjects;

7.4.1.5 the estimated number of affected data records; and

7.4.1.6 the personal data system affected, which resulted in the breach;

7.4.2 the potential consequences arising from the personal data breach;

7.4.3 the chronology of events leading to the loss of control over personal data;

7.4.4 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;

7.4.5 measures taken or proposed to be taken to address the affected data subjects; and

7.4.6 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.

7.5 Where and to the extent that it is not possible for the data controller to provide all the information requested in paragraph 7.4 at the time of submitting the initial notification to the Commissioner, the information may be provided in phases, as soon as practicable and no later than thirty (30) days from the date of the notification made under paragraph 7.1.

Personal Data Breach Involving Multiple Data Controllers

7.6 Where a personal data breach involves more than one (1) data controller, each data controller shall submit his own separate data breach notification to the Commissioner.

Delayed Data Breach Notification

7.7 Where the data controller fails to notify the Commissioner within seventy-two (72) hours, a written notice shall be submitted to the Commissioner, detailing the reasons for the delay and providing supporting evidence. The supporting evidence shall include documentation of the incident timeline, internal communications and any technical issues or external factors that contributed to the delay. All relevant documents shall be submitted together with the notification.

Contact Point and Assistance with the Commissioner's Investigations

7.8 Where the data controller is subject to the mandatory requirement to appoint data protection officer under Section 12A of the Act 709, the data protection officer shall act as the main point of contact for any inquiries or requests from the Commissioner regarding the personal data breach. Where the data controller is not subject to the mandatory requirement to appoint data protection officer, the data controller shall name or designate a representative with sufficient seniority and expertise to act as the point of contact.

7.9 In accordance with Section 105 of Act 709, the Commissioner may conduct an investigation into the data controller to determine whether any act, practice or request violates the provisions of Act 709.

7.10 The Commissioner may direct the data controller to submit records related to data breach notifications or any report documents upon request, in accordance with Section 121 of Act 709.

PART C: REQUIREMENTS FOR PERSONAL DATA BREACH NOTIFICATION / COMMUNICATION TO DATA SUBJECTS

8 Personal Data Breach that Must be Notified to Affected Data Subjects

8.1 The data controller shall 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.

8.2 Paragraph 5.2 which defines "significant harm" in the context of notifying the Commissioner, also applies when assessing whether a breach constitutes "significant harm" for the purpose of notifying data subjects. However, the "significant scale" criterion under paragraph 5.3 does not apply when determining whether notification to affected data subjects is required.

Examples of Personal Data Breach That Require Notification to the Affected Data Subjects

8.3 Examples of personal data breach scenarios where a data controller is required to notify the affected data subjects:

Example	**Whether Notification to the affected data subjects is Required**
A financial institution suffers a cyberattack which results in the theft of customers' personal and financial information including names, account numbers and passwords.	Yes, the risk of significant harm is high as a financial loss is likely to occur and the data includes information that may be used to enable identity fraud. As such, the data subjects would need to be informed about the breach.
A cybercriminal hacked the server which contains customers' personal and financial data and gained control of the pharmaceutical supplier's server. However, the cybercriminal is not able to access the said personal and financial data as the pharmaceutical supplier had implemented two layers of security measures.	No, in this situation, the data subjects do not need to be informed as the data is protected by security measures that render the information unintelligible or meaningless to the cybercriminal. However, the data controller needs to inform the Commissioner in the prescribed manner.
A cybercriminal circumvents the server security system of a direct seller and gains overall control of the data on the server. The cybercriminal threatens to delete the data on the server if the company does not pay a ransom. The direct seller does not have any backups of the said data.	Yes, in this situation, the data subjects need to be informed as there is a risk of loss of the personal and financial data of the data subjects.

9 Timeframes for Notification to Data Subjects

9.1 The notification to the affected data subjects, as referenced in paragraph 8.1, must be made without unnecessary delay, not later than seven (7) days after the initial data breach notification is made to the Commissioner under paragraph 7.1.

10 Manner of Notification to Affected Data Subjects

10.1 The notification to the affected data subjects shall be provided directly and individually to the data subjects in a practicable manner using intelligible language 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.

Information to be Provided in Notification

10.2 The notification of a personal data breach by the data controller to the affected data subjects shall include the following information:

10.2.1 the details of the personal data breach that has occurred;

10.2.2 details on the potential consequences resulting from the personal data breach;

10.2.3 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;

10.2.4 measures that the affected data subjects may take to eliminate or mitigate any potential adverse effects resulting from the data breach; and

10.2.5 the contact details of the data protection officer or other contact point from whom more information regarding the personal data breach can be obtained.

Manner of Notification

10.3 If direct notification 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.

10.4 Examples of "*disproportionate effort*" include the following:

10.4.1 the data controller is required to contact a large number of data subjects across multiple states or countries, where doing so would result in an excessive logistical, administrative or financial burden; or

10.4.2 the data controller must notify data subjects who have provided outdated or incorrect contact information, where doing so would require extensive resources to obtain the correct contact details for each data subject.

Examples of methods for notifying affected data subjects individually:

- email;
- SMS;
- direct messaging; and
- postal communication.

Examples of public communication:

- notification on the official website;
- notice in printed media;
- social media posts through the data controller's official pages or accounts; and
- automated notifications (push notification).

10.5 The form of notification used to inform the affected data subjects of the personal data breach should be sent separately from other information, such as regular updates, newsletters or standard messages, so that the communication of the breach is clear and transparent.

11 Governance Requirements

11.1 Data controller shall put in place adequate data breach management and response plans.

11.2 The focus of any breach management and response plan should be on ensuring that the data controller is able to promptly identify a personal data breach, take appropriate measures to contain and mitigate the breach and ensure compliance with his data breach notification obligations.

11.3 The data breach management and response plan shall, at a minimum, outline policies and procedures to address the following:

11.3.1 personal data breach identification and escalation procedures;

11.3.2 roles and responsibilities of relevant stakeholders (e.g., the data breach response plan, the data protection officer);

11.3.3 steps to contain and mitigate the impact of the breach;

11.3.4 steps to determine whether it is necessary to notify the Commissioner and / or the affected data subjects;

11.3.5 communication plan for notifying the Commissioner and / or the affected data subjects; and

11.3.6 post-incident review.

11.4 Data controller should also conduct periodic training, as well as awareness and simulation exercises, in order to ensure that his employees are aware of their roles and responsibilities in assisting the data controller in responding to the personal data breach.

12 Personal Data Breach involving Data Processor

12.1 The mandatory personal data breach notification under Section 12B of the Act 709 does not directly apply to data processor.

12.2 The data controller is required to contractually impose an obligation on his data processor to promptly notify him about a data breach that has occurred, and to provide all reasonable and necessary assistance to the data controller to meet the data controller's data breach notification obligation under the Act 709.

13 Duty of Data Controller to Conduct Assessment of Data Breach

13.1 The data controller should act promptly as soon as he becomes aware of any personal data breach to assess, contain and reduce the potential impact of the data breach.

13.2 Investigating a data breach can be time-consuming and the data controller may not be able to obtain a complete understanding of the breach during the initial stages of the investigation, particularly if the breach is complex.

13.3 Once the data controller becomes aware of a personal data breach, he should consider the following immediate containment actions where applicable:

13.3.1 isolate and disconnect the compromised database or system from the network;

13.3.2 suspend or disable compromised access rights;

13.3.3 stop the practices identified as having caused the data breach; and

13.3.4 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.

13.4 During the initial investigation into a data breach, the data controller should identify the following information:

13.4.1 the type(s) of personal data involved;

13.4.2 the number of affected data subjects;

13.4.3 the systems, servers, databases, platforms and services affected;

13.4.4 the chronology of events leading to the data breach;

13.4.5 the severity of the data breach;

13.4.6 the root cause of the data breach, and whether it is still ongoing;

13.4.7 the harm and potential harm that may result from the data breach;

13.4.8 the measures that should be taken to contain the data breach, and mitigate its possible adverse effects; and

13.4.9 the remedial actions that should be taken to reduce the harm to affected data subjects.

13.5 The information above may also assist the data controller in determining whether external assistance (e.g., data protection experts or technical forensic specialists) is required to help him respond to and contain the personal data breach.

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

14 Obligation to Maintain Records of Personal Data Breaches

14.1 The data controller shall keep records and maintain a register detailing personal data breach 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. The register should, at a minimum, document the following information:

14.1.1 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;

14.1.2 description of the likely consequences of the personal data breach;

14.1.3 description of a chronology of the events leading to personal data breach;

14.1.4 containment and recovery measures taken to address the personal data breach; and

14.1.5 details of notifications made to the Commissioner and/or affected data subjects and justification for not making notifications, where applicable.

14.2 The data controller is free to determine what method and format to use when documenting the breach, provided that the documentation is in such a way that is clear, concise and enables the Commissioner to verify that the data controller has complied with this documentation requirement.

14.3 Documentation of the personal data breach under Paragraph 14.1 above shall be made available when requested by the Commissioner.

PART D: NOTIFICATION OBLIGATION UNDER OTHER LAWS

15 Duty to Comply with Other Applicable Notification Obligation under Malaysian Laws

15.1 The mandatory personal data breach notification obligation under Act 709 applies independently and concurrently with any other similar notification obligations that may be applicable to the data controller under existing laws and regulations in Malaysia.

15.2 The Data controller should identify the relevant notification requirements that may apply to him, as well as establish internal processes and procedures to facilitate compliance with the multiple notification requirements that may be applicable to him.

16 Notification Requirement under Other Malaysian Laws

16.1 Below is a non-exhaustive listing of notification requirements imposed under other Malaysian laws and regulations that may be applicable to the data controller:

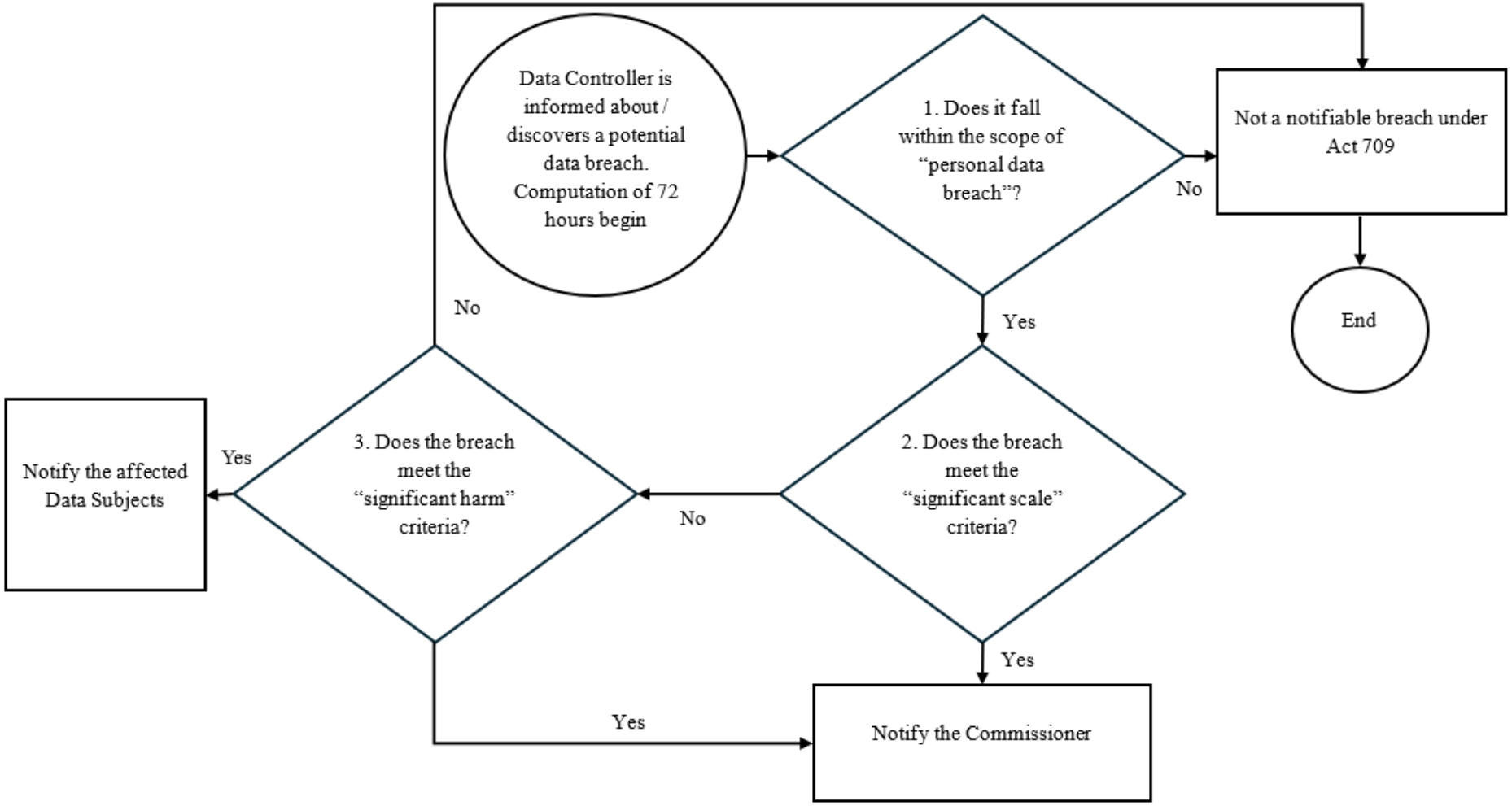
16.1.1 notification to the Royal Malaysia Police ("**PDRM**"), when the data breach involves criminal activity;

16.1.2 notification to sectoral regulators, such as Bank Negara Malaysia ("BNM"), Securities Commission Malaysia ("SC") and Malaysian Communications and Multimedia Commission ("MCMC"), pursuant to sectoral cyber incident or data breach notification requirements; and

16.1.3 notification to the Chief Executive of the National Cyber Security Agency ("NACSA") and National Critical Information Infrastructure ("NCII") Sector Leads ("NCII Sector Leads"), where the data controller is a designated NCII Entity under the Cyber Security Act 2024.

16.2 Please note that the list above is for reference purposes only. The data controller should conduct an independent assessment to determine the notification requirements under other applicable Malaysian laws and regulations.

ANNEX A: FLOWCHART OVERVIEW OF THE DATA BREACH NOTIFICATION REQUIREMENT UNDER THE ACT 709



ANNEX B: DATA BREACH NOTIFICATION FORM

DATA BREACH NOTIFICATION

This notification form is to be used when a data controller wishes to report a data breach to the Personal Data Protection Commissioner ("**Commissioner**").

Please note that the information requested in this notification form is non-exhaustive. The Commissioner may require further details of the incident to facilitate investigation.

Where and to the extent that it is not possible to provide all of the information requested in the notification form, is sufficient to complete the form only to the extent of the information available. Additional information to the Commissioner in phases as soon as practicable not later than thirty (30) days from the date of the initial notification.

PARTICULARS OF DATA CONTROLLER

Organisation : ----------

Address : ----------

Contact person

Name : ----------

Designation : ----------

Telephone Number : ----------

Email : ----------

Date : ----------

Signature : ----------

Based on the information you have provided, we will contact you to inform about our next steps. All personal data submitted will only be used for purposes which are directly related to this notification and the exercise of the regulatory powers and functions of the Commissioner.

Submission of notification:

PERSONAL DATA PROTECTION COMMISSIONER
8th Floor, Galeria PjH, Jalan P4W
Persiaran Perdana, Presint 4
62100 W.P Putrajaya
or via email: dbnpdp@pdp.gov.my

SECTION A: BASIC INFORMATION

1. Is this a new notification or an update to a previous notification that has been submitted to the Commissioner?

☐ New notification

☐ Update. Please indicate the reference number of the original notification:

2. If this is a new notification, are you submitting it within the 72 hours after becoming aware of the personal data breach?

☐ Yes

☐ No. Please provide the reason(s) for the delay with supporting evidence:

SECTION B: DETAILS OF THE PERSONAL DATA BREACH

3. When did your organisation become aware of the personal data breach?
(Please include the date and time of when your organisation became aware of the breach)

Date :	*Time :*

4. How did your organisation become aware of the personal data breach?
(Please provide a brief explanation of how your organization detected the personal data breach)

5. How was personal data affected or compromised?

(Select all that apply)

☐ Data was disclosed to unintended parties

☐ Data was lost

☐ Data was temporarily unavailable

☐ Data was exfiltrated / stolen

☐ Unauthorised access of personal data

☐ Others:

6. What is the actual or suspected cause of the incident?

(Select only one)

☐ Cyber incident

☐ Human error

☐ System error

☐ Theft / misuse of information by malicious actors

☐ Others:

7. How was the actual cause of the above incident identified? (Please specify)

8. Which system or application was affected in this personal data breach incident? (Please specify)

9. Where is the storage location of the personal data affected by this personal data breach?

☐ Malaysia

☐ Other jurisdictions (Please specify)

10. What is the status of the personal data breach incident?

☐ In Progress

☐ Rectified / Contained

11. Are there any other parties affected by the personal data breach (e.g., other data controllers or data processors)?

☐ No.

☐ Yes. Please list out these parties:

SECTION C: DETAILS OF COMPROMISED DATA

12. What types of personal data were compromised?

13. Number of data subjects affected or potentially affected?

14. Does this personal data breach only affect data subjects who are Malaysian citizens?

☐ Yes.

☐ No. The breach also affects data subjects in the following jurisdictions:

15. What harm or risks may result from the personal data breach affecting data subjects?

☐ Physical harm to threat to safety

☐ Financial loss

☐ Identity theft or fraud

☐ Misuse of data for unlawful purposes

☐ Data contains sensitive data

☐ Data contains financial information

☐ No potential harm to data subjects

☐ Others (Please specify)

SECTION D: CONTAINMENT AND RECOVERY ACTIONS

16. What actions have been or will be taken to contain and mitigate the harm or risks arising from the breach?

17. **What actions have been or will be taken to address the affected data subjects?**

SECTION E: COMMUNICATION AND NOTIFICATION

18. **Have you communicated or directly interacted with the suspected or actual threat actor?**

☐ Yes

☐ No

☐ Not applicable. There are no threat actor is involved.

19. **Have you notified or will you notify any local or foreign regulatory bodies regarding this personal data breach?**

☐ Yes. These regulatory bodies include:

☐ No

20. **Have you notified the affected data subjects about the personal data breach?**

☐ Yes. (Please attach a copy or sample of the notification provided)

☐ No, but we intend to notify the affected data subjects.

☐ No. We do not intend to notify the affected data subjects. (Please provide justifications)

21. If you answered "Yes" to Question 20, how was the notification to the affected data subjects made?

☐ Direct and individual notification (e.g., via email to affected data subjects).

☐ Public announcement (e.g., social media and press release).

SECTION F: OTHERS

22. Is there any additional information related to this personal data breach?
