



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, MALAYSIA

8th Floor, Galeria PjH, Jalan P4W,

Persiaran Perdana, Presint 4,

62100 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)

<i>Date :</i>	<i>Time :</i>

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. 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 / 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, press release, etc.).

SECTION F: OTHERS

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

--