PERSONAL
DATA PROTECTION
COMMISSIONER MALAYSIA
Ministry of Communication and Multimedia Malaysia

DATA BREACH NOTIFICATION

This notification template is to be used when data users wish to report a personal data breach that has occurred or may have occurred in the organisation, in circumstances where the breach presents a risk to the affected data subjects. When completing this form, do not include any of the personal data involved in the breach. Please note that the notification template is by no means exhaustive. The Commissioner may require further details of the incident to facilitate investigation.

PARTICULARS OF DATA USER AND THE PERSON GIVING THIS NOTIFICATION

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

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

Contact person

Name :

Job Title :

Telephone Number : **Fax :**

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
6th Floor, Lot 4G9, Kompleks KKMM
Persiaran Perdana, Presint 4,
62100 Putrajaya
or via email: dbnpdp@pdp.gov.my

DATA BREACH NOTIFICATION

The notification template is by no means exhaustive. The Commissioner may require further details of the incident to facilitate investigation.

DETAILS OF THE DATA BREACH	
1.	**Summary of the incident:** **a) Nature of the breach (e.g. loss, leakage, unauthorised access, cyber-attack, technological flaw, criminal intent, loss of equipment etc.)** **b) When, where and how did the breach happen?** **c) When was the breach discovered?** **d) Who discovered it and how was it discovered?** **e) What was the duration of the data breach?** **f) What was the cause of the breach?**
2.	**Compromised data:** **a) The amount and type of data that has been compromised (financial, employment, health data etc.);** **b) The estimated number of the affected data subjects.**
3.	**What are the potential harms caused by the incident? It may include:** **a) Threat to personal safety** **b) Identity theft** **c) Financial loss** **d) Reputational damage, humiliation and embarrassment** **e) Loss of business and employment opportunities**
4.	**Current security measures/controls at organisation (prior to this incident)**
CONTAINMENT AND RECOVERY	
5.	**a) Action taken to contain the breach** **(e.g.: Procedures / instructions in place to minimise risks to security of data)** **b) Action taken to recover any lost data and minimise the damage of the breach** **(e.g.: Restoration of data via back-up servers/tapes)**
NOTIFICATIONS	
6.	**Have you notified these parties?** **a) Regulators and law enforcement agencies** **b) The affected parties** **c) Data processors** **d) Other (overseas) data protection authorities (if necessary)**