PERSONAL
DATA PROTECTION
COMMISSIONER MALAYSIA

Ministry of Communications
and Digital

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 : ----------

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

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 Kementerian Komunikasi & Digital
Persiaran Perdana, Presint 4,
62100 Putrajaya
or via email: dbnpdp@pdp.gov.my

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? Compromise on database only or inclusive of API breach?** **c) When was the breach discovered?** **d) Who and how was the breach discovered?** **e) What was the duration of the data breach?** **f) What was the cause of the breach?** **g) What is the compromised system?** **h) Who developed the compromised system? In-house or outsourced? If it is outsourced, who is the developer?** **i) What categories of organisation data does the outsourced entity has? Does the outsourced entity has direct access to the organisation's network?** **j) Which part of system was compromised? File folder system (NAS / SAN / Cloud Storage) or also involves application and system database?** **k) Does your organisation implement on-premise infrastructure or cloud infrastructure?** **l) Who was the previous cloud service provider prior to data breach incident? What security measures were lacking at the cloud service provider's end?**
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.** **c) What data does the organisation collect, process, and store? Where is the data being stored, and what security measures are in place to protect the data?** **d) Who has access to the data, and how is access granted and monitored? Are there any third parties involved in processing of the data, and how is their access and use of the data being monitored?** **e) How long is the data being retained, and how is it being disposed of?**

	f) Does the organisation obtain consent from individuals for processing their personal data? **g) Does the breach involve only Malaysian citizens? If not, please specify the country(ies) affected and number of affected data subjects.** **h) Has the organisation conducted a data protection impact assessment for high-risk processing activities?**
3.	**What are the potential harms caused by the incident? It may include:** **a) Threat to personal safety (Yes/No);** **b) Identity theft (Yes/No);** **c) Financial loss (Yes/No);** **d) Reputational damage, humiliation and embarrassment (Yes/No);** **e) Loss of business and employment opportunities (Yes/No);** **f) Others (please specify):**
4.	**Current security measures/controls at organisation (prior to this incident):** **a) Please specify current security measures/controls at your organisation (prior to this incident).** **b) Is your organisation certified to comply with :** **- ISO/IEC27002:2022 Information Security, Cybersecurity and Privacy Protection (Information Security Controls)** **- ISO/IEC27001:2022 Information Security, Cybersecurity and Privacy Protection (Information Security Management Systems)** **- ISO/IEC27701:2019 Security Techniques (Privacy Information Management System)** **If your organisation is yet to be certified in compliance to the Standards above, do illustrate and explain in detail measures & timeline to be certified.** **c) Any other data & system security compliance that your organisation has been certified and in compliance to? (Example: PCI DSS)** **d) Does your organisation systems implement Network Time Protocol synchronisation between all servers & network equipments inclusive of time synchronisation of system & security appliances?** **e) Does the organisation have an incident response plan in place for cybersecurity incidents?** **f) Has the organization conducted a vulnerability assessment of its systems and infrastructure?**

	g) Does the organization have appropriate measures in place to protect against malware, phishing attacks, and other common cybersecurity threats? **h) Are employees regularly trained on cybersecurity best practices?** **i) Are third-parties subject to appropriate cybersecurity controls and contractual terms?**
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/optical disk)**
COMMUNICATION & NOTIFICATIONS	
6.	**a) Have you attempted to directly communicate / negotiate with the Threat Actor? (Yes/No);** **b) Have you attempted to communicate / negotiate with the Threat Actor via its agent(s) / proxy(ies)? (Yes/No);** **c) Have you appointed any agent(s) / proxy(ies) in attempt to directly communicate / negotiate with the Threat Actor? (Yes/No);** **d) Have you appointed any agent(s) / proxy(ies) in attempt to communicate / negotiate with the Threat Actor via its agent(s) / proxy(ies)? (Yes/No).** **Kindly provide all related evidence including transcribed voice communication with the Threat Actor or its agent(s) / proxy(ies).**
7.	**Have you notified these parties? What are the methods used to notify?** **a) Regulators and law enforcement agencies** **b) Data subjects** **c) Other affected parties** **d) Data processors** **e) Other (overseas) data protection authorities (if necessary)**