PUBLIC CONSULTATION PAPER NO. 01/2024:

THE IMPLEMENTATION OF DATA BREACH NOTIFICATION

PART 1: INTRODUCTION AND BACKGROUND

[A] Introduction

1.1 The Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**"), which introduces amendments to the Personal Data Protection Act 2010 ("**PDPA**"), was passed without amendments by the House of Representatives on 16 July 2024, and by the Senate on 31 July 2024. The Amendment Bill is currently pending assent by the Yang di-Pertuan Agong.

1.2 Clause 6 of the Amendment Bill seeks to introduce a new mandatory data breach notification obligation for data controllers (previously known as data users)[1] by inserting a new Section 12B under Part II of the PDPA.

1.3 For ease of reference, the full text of Section 12B of the PDPA which provides for the new mandatory data breach notification obligation states as follows:

> ***Data breach notification***
>
> ***12B.*** *(1) Where a data controller has reason to believe that a personal data breach has occurred, the data controller shall, as soon as practicable, notify the Commissioner in the manner and form as determined by the Commissioner.*
>
> *(2) Where the personal data breach under subsection (1) causes or likely to cause any significant harm to the data subject, the data controller shall notify the personal data breach to the data subject in the manner and form as determined by the Commissioner without unnecessary delay.*
>
> *(3) A data controller who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred and fifty thousand ringgit or imprisonment for a term not exceeding two years or both.*

1.4 Further to the above, the term "*personal data breach*" is defined under Clause 3 of the Amendment Bill as follows:

> *"personal data breach" means any breach of personal data, loss of personal data, misuse of personal data or unauthorized access to personal data.*

1.5 To supplement the data breach notification obligation that will be introduced by the new Section 12B of the PDPA, a proposed Personal Data Protection (Personal Data Breach Notification) Regulations ("**DBN Regulations**") and Data Breach Notification Guideline ("**DBN Guideline**") are being developed by the Personal Data Protection Commissioner ("**Commissioner**"). The DBN Regulations and DBN Guideline will provide additional provisions and guidance on implementation requirements for the data breach notification obligation and supplement Section 12B of the PDPA.

1.6 Pursuant to the above, this Public Consultation Paper ("**PCP**") seeks to gather public views and feedback regarding aspects that will be or should be addressed in the proposed DBN Regulations and DBN Guideline.

[1] Clause 2 of the Amendment Bill substitutes the term "data user(s)" with "data controller(s)" throughout the Amendment Bill.

PART 2: PROPOSED REQUIREMENTS FOR DATA BREACH NOTIFICATION OBLIGATION UNDER THE PDPA

2.1 As an overview, Part 2 of this PCP on proposed requirements that will be addressed in the DBN Regulations and DBN Guideline is categorised as follows:

(a) Notification thresholds for data breach notifications to the Commissioner;

(b) Notification thresholds for data breach notifications to affected data subjects;

(c) Manner and form of data breach notification to the Commissioner;

(d) Manner and form of data breach notification to affected data subjects;

(e) Timeframe for data breach notification to the Commissioner;

(f) Timeframe for data breach notification to affected data subjects;

(g) Exemptions from notifying data breach to the affected data subjects;

(h) Data processors' obligation to comply with the data breach notification obligation;

(i) Concurrent application of PDPA's data breach notification regime with other laws / sectoral breach notification regime; and

(j) Management of personal data breaches and record-keeping obligations.

[A] Notification Thresholds for Data Breach Notifications to the Commissioner

2.2 Background: To align with practices of data protection authorities in other jurisdictions (including the EU), it is proposed that the data breach notification obligation to the Commissioner under Section 12B(1) of the PDPA be restricted to only certain types of personal data breaches that meet the notification thresholds stipulated in the DBN Regulations and DBN Guideline.

2.3 Specifying a threshold for data breach notification to the Commissioner serves two (2) main purposes:

(a) to prevent the over-reporting of data breaches thereby averting unnecessary expenses for data controllers in responding to and reporting data breaches, and

(b) to prevent the Commissioner from being overwhelmed with notification reports for less severe personal data breaches.

2.4 Proposal: It is proposed that the mandatory data breach notification under Section 12B of the PDPA to the Commissioner be limited to only instances where:

(a) the personal data breach is likely to cause or have caused *"**significant harm**"*; **OR/AND**

(b) the personal data breach is likely to be or is of a "***significant scale***".

2.5 Please note that the thresholds or conditions outlined above in Paragraphs 2.4(a) and 2.4(b) are to be read disjunctively or conjunctively. In other words, data controllers will be required to notify the Commissioner and/or affected data subjects if the personal data breach meets **either or both** of the thresholds in Paragraphs 2.4(a) and 2.4(b).

2.6 It is proposed that a personal data breach will be considered to be of "*significant harm*" if:

(a) the access, disclosure or loss of personal data from the personal data breach results or is likely to result in bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the data subjects' credit record, or damage to or loss of property;

(b) the access, disclosure or loss of personal data results or is likely to result in serious harm to affected data subjects to whom the information relates, or has been, is being or will likely be misused for illegal purposes; **OR**

(c) the personal data compromised by the personal data breach includes sensitive personal data or any other information that may be used to enable identity fraud such as usernames, passwords or identification numbers.

2.7 On the other hand, a personal data breach will be considered to be of "*significant scale*" if the number of affected data subjects exceeds or is likely to exceed 500 individuals.

Question 1

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposed framework to limit the mandatory data breach notification requirement to the Commissioner under Section 12B(1) of the PDPA to only personal data breaches that meet the thresholds stipulated in Paragraph 2.4 above?

(b) Do you consider the threshold of 500 data subjects to be appropriate to determine that a personal data breach is of "significant scale"? Should it be increased or lowered?

For reference, the threshold is 500 affected data subjects in Singapore, and 1,000 affected data subjects in Japan.

[B] Notification Thresholds for Data Breach Notifications to Affected Data Subjects

2.8 Background: Similar to the above, we note that in other jurisdictions, including the EU, UK, Singapore, and Indonesia, thresholds are determined for notifying affected data subjects about data breaches. While there are slight differences in these thresholds, the element of harm appears as a universal requirement across all jurisdictions.

2.9 A similar approach, focusing on the element of harm to data subjects, has been adopted under Section 12B(2) of the PDPA. Section 12B(2) of the PDPA provides that notification of personal data breaches to affected data subjects is mandatory where the personal data breach causes or is likely to cause ***"significant harm"*** to the affected data subject.

2.10 Proposal: The DBN Regulations and/or DBN Guideline will clarify that a personal data breach causes or is likely to cause ***"significant harm"*** to affected data subjects, if the breach falls within the circumstances outlined in Paragraph 2.6 and Paragraph 2.7 above. In this regard, it is also proposed for the circumstances outlined in Paragraph 2.6 to be read disjunctively or conjunctively, whereas the criterion outlined in Paragraph 2.7 shall be read conjunctively with the circumstances outlined in Paragraph 2.6.

Examples:

A data controller shall not be required to notify the affected data subjects even though the personal data breach fulfils all circumstances outlined under Paragraph 2.6 if the personal data breach does not fulfil the criterion stated in Paragraph 2.7.

A data controller shall be required to notify the affected data subjects even though the personal data breach fulfils only one of the circumstances outlined under Paragraph 2.6 if the personal data breach fulfils the criterion stated in Paragraph 2.7.

2.11 For ease of reference, the table below sets out the different notification thresholds applicable for notification to the Commissioner as well as notification to affected data subjects:

	Mandatory Notification to the Commissioner	**Mandatory Notification to Affected Data Subjects**
Where the personal data breach is likely to cause or have caused significant harm	✓	✓
Where the personal data breach is likely to be or is of a significant scale	✓	✓

Question 2

What are your views on the proposed scope of definition for "significant harm"? Would the definition be too broad, or should it be further restricted?

[C] Manner and Form of Data Breach Notification to the Commissioner

2.12 Background: Prior to the introduction of the mandatory data breach notification regime by way of the Amendment Bill, the Commissioner had deployed a template data breach reporting form ("**Template Reporting Form**") that data controllers have been using to voluntarily report personal data breach incidents affecting their organisations.

2.13 A copy of the Template Reporting Form can be found in **Annexure 1** below.

2.14 The Commissioner understands that data controllers may not have all the requested information during the initial reporting of the data breach to the Commissioner. Therefore, the Commissioner does not expect data controllers to complete all the information requested in the Template Reporting Form. Data controllers can subsequently furnish further details or information once they become available in relation to the said personal data breach.

2.15 Data controllers can either submit the completed Template Reporting Form in hard copy to the Commissioner's office at Putrajaya, or through the Commissioner's dedicated e-mail address for data breach notifications (i.e., dbnpdp@pdp.gov.my).

2.16 Proposal: The Commissioner proposes to retain the current Template Reporting Form for reporting of data breaches by data controllers under Section 12B(1) of the PDPA, with potential modifications made to the content and presentation style of the Template Reporting Form.

2.17 Proposed modifications include simplifying the Template Reporting Form by incorporating predefined dropdown options to streamline and standardise the responses required as well as avoiding compound questions.

2.18 For instance, Question 2(d) of the Template Reporting Form reproduced below for ease of reference is currently set out in a compounded form:

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?

2.19 This question will be modified to separate the different types of information being requested into individual questions.

2.20 Additionally, the Commissioner is also considering providing self-assessment tools to assist data controllers to determine whether a personal data breach is notifiable, and establishing a designated helpline channel to offer guidance to data controllers.

Question 3

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Are there any information fields in the current Template Reporting Form that should be added, or removed (e.g., where the question may be too technical / difficult for some data controllers, or the information can be requested later by the Commissioner during its investigation process)?

For illustration purposes, information requested under Question 4 (regarding existing security measures / controls implemented by the data controller) may be too technical for certain categories of data controllers, and can be requested subsequently by the Commissioner on a case-by-case basis.

(b) Do you think replacing certain questions with pre-defined dropdown options for answers would help streamline and make it easier for data controllers to complete the Template Reporting Form?

(c) As a data controller, have you encountered or do you foresee any potential challenges or difficulties in completing the Template Reporting Form and submitting the data breach notification to the Commissioner through the notification channels mentioned in Paragraph 2.15 above?

(d) Do you think JPDP should continue to allow submission of data breach notifications in physical or hard copies, bearing in mind that small businesses may not have the technological proficiency to submit data breach notifications through electronic or online channels?

(e) Do you think that self-assessment tools or a helpline channel would be beneficial in assisting data controllers in determining whether a personal data breach is notifiable?

(f) In your opinion, what other improvements can be made to the Template Reporting Form or the notification process to the Commissioner in general?

[D] Manner and Form of Data Breach Notification to Affected Data Subjects

2.21 Background: Other jurisdictions generally adopt a more flexible approach on the manner and form of data breach notification required to affected data subjects, compared to notifications to data protection authorities.

2.22 However, these jurisdictions still prescribe the minimum information that must be provided when data controllers notify data subjects. The types of minimum information prescribed are typically not as extensive as the information required for notifications to data protection authorities.

2.23 This is because the primary purpose of notification to affected data subjects is to alert them to the potential risks that may result from a personal data breach affecting the data controller and to provide information about preventive steps that data subjects can take to mitigate such risks.

2.24 Proposal: It is proposed that data controllers be required to provide, at a minimum, the following information when notifying affected data subjects about a personal data breach:

(a) A description of the personal data breach that has occurred;

(b) Details regarding personal data that has been compromised or affected by the personal data breach;

(c) The potential consequences or harm that may arise as a result of the personal data breach;

(d) A description of the measures that has been taken or will be taken by the data controller to address / contain the personal data breach;

(e) Recommendations about the steps / measures that can be taken by affected data subjects in response to the personal data breach; and

(f) Provide contact details of the contact point from whom more information about the data breach can be obtained (for example, details of the data controller's data protection officer).

2.25 Additionally, it is also proposed that data controllers be required to notify / communicate the personal data breach to the affected data subjects directly (e.g., through direct e-mail notification to the data subject), unless doing so would involve a disproportionate effort. In which case, a public communication / statement or similar measures would be sufficient.

2.26 The DBN Guideline will provide further examples on the communication channels that can be adopted / used by data controllers to notify data subjects about any personal data breaches affecting their personal data.

Question 4

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposed list of minimum information that must be provided by data controllers to affected data subjects? Are there any additional types of information that you believe should be included in the notification to affected data subjects? If so, please specify.

(b) Do you foresee any challenges or obstacles for data controllers in providing the proposed minimum information to affected data subjects? If yes, please describe them.

(c) How can the process of notifying affected data subjects be made more efficient and less burdensome for data controllers, particularly for small and medium-sized enterprises (SMEs)?

(d) What are your views on the proposal to use public communication / statement as an alternative notification method when direct communication would involve disproportionate effort? Are there any other alternative methods that should be considered?

[E] Timeframe for Data Breach Notification to the Commissioner

2.27 Background: In terms of the timeframe for notification of personal data breaches to data protection authorities, other jurisdictions generally require notification within seventy-two (72) hours (or three (3) calendar days, such as in Singapore) from the time the data controller "becomes aware" of the data breach.

2.28 Proposal: With regards to the notification timeframe to the Commissioner, it is proposed that data controllers must notify the Commissioner no later than seventy-two (72) hours after the data controller becomes aware of a data breach. This would align with the data breach notification timeframe adopted by other jurisdictions, including the EU.

2.29 A data controller is considered to have "become aware" of a data breach when there is reasonable degree of certainty that a data breach has occurred and which has led to personal data being compromised. A data controller can be said to have reasonable degree of certainty if there is sufficient evidence showing that a personal data breach has occurred.

2.30 For instance, a data controller is considered to have become aware of a personal data breach when a third party notifies them that they have wrongly received personal data of one of the data controller's customers and provides evidence of unauthorised disclosure. Additionally, a data controller will be considered to have become aware if it receives notification from its data processor that there is evidence of a personal data breach.

2.31 Further guidance and clarification will be provided in the DBN Guidelines to assist data controllers determining when they will be considered to have "become aware" of a data breach, which will start the 72-hour timeframe within which data controllers must assess whether the data breach must be notified to the Commissioner.

Question 5

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you think the calculation of time for the 72-hour timeframe from when the data controller "becomes aware" is clear, or could it potentially cause confusion to data controllers?

(b) What are your views on the proposed timeline for data breach notification to the Commissioner?

(c) Do you think the proposed timeline for notification of data breaches to the Commissioner adequately balances the need for prompt notification with the practicalities of managing a data breach? If not, can you please provide clear examples how the timeline may be difficult to comply with for data controllers in your sector?

[F] Timeframe for Data Breach Notification to Affected Data Subjects

2.32 Background: In other jurisdictions, the timeframe for notifying affected data subjects tends to be more flexible compared to the notification timeframe to data protection authorities regarding a personal data breach. It is generally stipulated that notification should be made without undue delay, at the same time as the notification to the data protection authority, or as soon as practicable thereafter.

2.33 Proposal: Section 12B(2) of the PDPA requires the data controller to notify affected data subjects "without unnecessary delay". In this regard, it is proposed that the DBN Guideline clarifies "without unnecessary delay" to mean that data controllers must notify data subjects at the same time as the notification to the Commissioner, or as soon as practicable thereafter.

Question 6

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposed timeline for data breach notification to affected data subjects?

(b) Do you think the proposed timeline for notification of data breaches to affected data subjects adequately balances the need for prompt notification with the practicalities of managing a data breach? If not, can you please provide clear examples how the timeline may be difficult to comply with for data controllers in your sector?

[G] Exemptions from Notifying data breach to the affected Data Subjects

2.34 Background: The data breach notification regime in other jurisdictions, including the EU, UK, Japan, Singapore and New Zealand, exempt or allow data controllers to postpone notifications to affected data subjects in certain circumstances, e.g. where steps have been taken by the data controller to ensure that the risk or harm to the affected data subject will no longer materialise.

2.35 Proposal: It is proposed that data controllers be exempted or allowed to postpone data breach notifications to affected data subjects in the following circumstances:

(a) the data controller has implemented appropriate technological and organisational protection measures that renders it unlikely that the breach will result in significant harm to the affected data subjects;

(b) the personal data compromised or affected by the breach is protected by one or more security measures that make the information unintelligible or meaningless to any individual who is not authorised to obtain the information; or

(c) where the Commissioner directs otherwise.

2.36 It is proposed that data controllers will not be required to obtain prior approval from the Commissioner for the exemption or postponement of notification to affected data subjects.

2.37 However, data controllers will be required to state in the Template Reporting Form, when notifying the Commissioner, whether they plan to inform affected data subjects about the data breach and provide their justification(s) for not informing or postponing the notification to affected data subjects.

2.38 The Commissioner, may upon its own investigation and assessment, subsequently direct the data controller to notify affected data subjects about the data breach if the Commissioner does not agree with the justification(s) provided by the data controller.

Question 7

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposed exemptions / grounds of delaying the notification to affected Data Subjects? Do you believe there are any additional circumstances where exemptions or postponements should be considered? If so, please specify and justify.

(b) In your experience, what factors could delay the notification to affected data subjects, and how might these be addressed in the DBN Guideline?

[H] Data Processors' Obligation to Comply with the Data Breach Notification Obligation

2.39 Background: The data breach notification regimes in other jurisdictions, for instance, in the EU and Singapore, impose an obligation on data processors (and their equivalent) to notify their data controllers where there is reason to believe that a personal data breach has occurred. This enables the data controller to assess and comply with the data breach notification requirements under their respective data protection legislation.

2.40 Proposal: It is proposed that the DBN Regulations and/or the DBN Guideline includes a requirement for data controllers to contractually impose an obligation on their data processors to promptly notify them about personal data breaches that have occurred, and to provide all reasonable and necessary assistance to the data controller to meet the data controller's data breach notification obligations under the PDPA and the DBN Guideline.

2.41 It is proposed that the DBN Guideline allow flexibility for data controllers to determine the specific timeframe of notification / escalation of personal data breaches to the data controller's attention, provided that the timeframe is able to support the data controller in meeting its data breach notification obligations to both the Commissioner and affected data subjects.

2.42 If a data processor provides services to multiple data controllers that are all affected by the same personal data breach incident, the data processor must separately report details of the incident to each data controller.

Question 8

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposal to require data controllers to contractually bind their data processors to notify them about a personal data breach that has occurred?

(b) Should there be a specific timeframe within which data processors must notify data controllers of a potential data breach? If so, what would be an appropriate timeframe (e.g., within 24 hours)?

(c) Based on your experience, what challenges or issues might arise from the proposed requirement for data processors to notify data controllers, and how might these be addressed in the DBN Guideline?

[I] Concurrent Application of PDPA's Data Breach Notification Regime with Other Laws / Sectoral Breach Notification Regime

2.43 Background: Apart from the data breach notification obligation under the PDPA, data controllers may be required to notify other relevant regulatory authorities of personal data breaches, where applicable.

2.44 This may include notification requirements as set out in the Cyber Security Act, Bank Negara Malaysia's Policy Document on Management of Customer Information and Permitted Disclosure, and Securities Commission Malaysia's Guidelines on Technology Risk Management (which will supersede the Management of Cyber Risk Guidelines on 1 August 2024).

2.45 We note that personal data breach notification regimes in other jurisdictions (for example, the EU and Singapore) operate separately and concurrently with other applicable data breach notification requirements imposed under their laws. Data controllers are required to conduct separate assessments to determine whether they need to comply with different notification obligations imposed by different regulators, and submit separate data breach notifications to different regulators where applicable.

2.46 This approach for separate notification is necessary because notification thresholds and requirements vary across different regulations. Additionally, each regulator has different regulatory mandates and focuses on different aspects when investigating data breaches.

2.47 Proposal: It is proposed that the DBN Regulations and/or the DBN Guideline clarifies that the data breach notification obligation under the PDPA does not override any applicable notification obligation to other regulators or under any other laws / regulations in Malaysia.

2.48 This means that data controllers are required to make separate assessments as to whether a data breach incident falls within the notification thresholds stipulated under different regulations that may be applicable to them, including the PDPA and other sectoral regulations, and submit separate notifications to the relevant regulators based on their assessment.

Question 9

Are there any other regulations applicable to your business / sector which imposes a similar data breach notification requirement for data controllers or organisations in general within your sector? Please provide a brief explanation of the applicable requirements.

[J] Management of Personal Data Breaches and Record-Keeping Obligations

2.49 Background: In addition to outlining the obligations of data controllers and data processors in notifying data protection authorities and affected data subjects about personal data breaches, other jurisdictions also provide guidance on steps that must be taken by data controllers to respond, contain and manage such breaches.

2.50 Besides that, there are also record-keeping obligations outlined for data controllers to document personal data breaches that have affected their organisation as well as the steps that were taken to respond and contain the personal data breach.

2.51 Proposal: It is proposed that the DBN Guideline clarifies and provides guidance on best practices for data controllers on how to effectively respond to data breaches, investigate and contain them, and implement measures to prevent the recurrence of similar breaches in the future.

2.52 Additionally, it is also proposed that the DBN Guideline introduces a requirement for data controllers to develop and implement a data breach management plan to ensure that they are able to promptly respond to any personal data breaches. The DBN Guideline will outline a minimum list of matters or components that must be addressed in the data breach management plan.

2.53 In terms of the record-keeping obligations of data controllers, it is proposed that data controllers be required to document and maintain proper records of all personal data breaches, regardless of whether the data breach is notifiable to the Commissioner and/or affected data subjects.

Question 10

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the types of best practices that should be recommended for data controllers when assessing, containing, mitigating, and preventing similar personal data breaches from occurring in the future? Are there specific practices you believe are essential for effective management of personal data breaches?

(b) Do you agree with the proposal to require data controllers to develop and implement a data breach management plan? What key components do you believe should be included in this plan to ensure effective management of data breaches?

(c) In terms of the proposed record-keeping obligation, what key elements or types of information do you think must be included in a data controller's records to ensure comprehensive documentation of personal data breaches?

(d) Based on your experience, what are the common challenges faced by data controllers in complying with data breach notification requirements, as well as in taking steps to contain and mitigate a personal data breach?

Annexure 1 –Reporting Form Template

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, cyberattack, 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)**