The Standard Operating Procedure of Personal Data Protection

Introduction

Following the recent Personal Data Protection (Amendment) Act 2024 ("**the 2024 Amendment Act**"), IOI Properties Group Berhad ("**the Company**") has embarked on a journey to ensure the full compliance of the 2024 Amendment Act.

The first step of compliance is the appointment of the Data Protection Officer ("**DPO**") in the Company. In gist, the DPO shall act as the representative of the Company in undertaking the duties and obligations to ensure compliance of the Personal Data Protection Act 2010 and the 2024 Amendment Act together with all the relevant guidelines. The DPO shall be the main liaison between the Company and the PDP Commissioner and/or the Data Subjects relating to matters concerning Personal Data (and its breach).

The Privacy Policy provided in the Company's general website offers a general overview of the Company's commitment in protecting the Personal Data of each Data Subject that the Company comes across with. In order to achieve this protection, the practical duty of the Company via the DPO is outlined in this Internal Guidelines with the purpose to provide clarification and understanding of each department and their further cooperation in ensuring the Company's compliance and commitment with respect to Personal Data protection.

For the avoidance of doubt, the following definitions are provided herein for clarification of the respective roles played relating to the handling of Personal Data:

"Data Controller" – means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor.

"Data Processor" – in relation to personal data, means any person, other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes.

"Data Subject" – means an individual who is the subject of the personal data.

1. Duties & Obligations of our Data Protection Officer

1.1 The duties and obligations of the DPO are amongst others, as follows:

(a) To inform and advise on data protection issues.

(b) To support the compliance with PDPA and other related data protection laws.

(c) To monitor compliance with PDPA and related data protection laws.

(d) To support the carrying out of data protection impact assessment (DPIA) to review the relevant personal data protection law of the receiving country/ jurisdiction is equivalent to the PDPA.

(e) To ensure proper data breach and security incident management, by assisting to prepare, process and submit reports required by the Commissioner.

(f) To act as a facilitator and point of contact with data subjects.

(g) To act as the liaison officer and main point of reference for the Commissioner.

1.2 The DPO shall be provided with the requisite resources to perform his/her function with sufficient independence and autonomy, by avoiding the placing of the DPO in positions that could cause conflicts between the business interests and compliance.

2. Governance Requirements

2.1 The focus is to put in place adequate data breach management and response plans, which are aimed to promptly identify a Personal Data breach and to take appropriate measures to contain and mitigate the breach and ensure compliance with the data breach notification obligations.

2.2 The data breach management and response plan namely address:

(a) Personal Data breach identification and escalation procedures.

(b) Roles & responsibilities of relevant stakeholders (e.g. the data breach response plan, the data protection officer).

(c) Steps to contain and mitigate the impact of the breach.

(d) Steps to determine whether it is necessary to notify the Commissioner and/ or the affected data subjects.

(e) Communication Plan for notifying the Commissioner and/ or the affected data subjects.

(f) Post-incident review.

2.3 The Company via the DPO shall also conduct periodic training, as well as create awareness and simulation exercises, in order to ensure that the Company's employees are aware of their roles and responsibilities in assisting the Company and/or DPO in responding to the Personal Data breach.

3. Data Processors

3.1 The Company shall impose an obligation on the Data Processors liaising with the Company where the Data Processors are obliged to promptly notify the Company about a data breach that has occurred, and to provide all reasonable and necessary assistance to the Company to meet the Company's data breach notification obligation.

3.2 This obligation can be reflected through a contractual obligation where the Data Processor shall be bound to provide all means of assistance including the notification of the data breach to the Company.

Personal Data Breaches

4. Investigation in Determining the Occurrence of a Personal Data Breach

4.1 Once becoming aware of a Personal Data breach, the Company would consider the following immediate containment actions where applicable: -

(a) Isolate and disconnect the compromised database or system from the network.

(b) Suspend or disable compromised access rights.

(c) Stop the practices identified as having caused the data breach.

(d) 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.

4.2 During the initial investigation into a data breach, the Company would also be identifying the following information: -

(a) The type(s) of Personal Data involved.

(b) The number of affected Data Subjects.

(c) The systems, servers, databases, platforms and services affected.

(d) The chronology of events leading to the data breach.

(e) The severity of the data breach.

(f) The root cause of the data breach, and whether it is still ongoing.

(g) The harm and potential harm that may result from the data breach.

(h) The measures that should be taken to contain the data breach, and mitigate its possible adverse effects.

(i) The remedial actions that should be taken to reduce the harm to affected data subjects.

4.3 These identified information would assist in determining whether external assistance (e.g. data protection experts or technical forensic specialists) is/are required to assist in responding to and containing the Personal Data breach.

4.4 A post-breach evaluation shall be conducted to review the effectiveness of the data breach management and response plan, as well as the data protection practices and policies to prevent the recurrence of similar incidents.

5. Notification to the PDP Commissioner

5.1 Where the Company has reason to believe that a Personal Data breach has occurred, which is likely to cause ***any significant harm***, the Company will notify the PDP Commissioner of the Personal Data breach as soon as practicable and **not later than seventy-two (72) hours** from the occurrence of the Personal Data breach.

5.2 Breaches of Personal Data deemed as causing or likely to cause ***"significant harm"*** pose as a risk in the event that the compromised Personal Data:

(a) May result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;

(b) May be misused for illegal purposes;

(c) Consists of sensitive personal data;

(d) Consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or

(e) Is of significant scale [if the number of affected personnel (Data Subjects) exceeds one thousand (1,000)].

5.3 Examples of Personal Data breach scenarios, to notify the PDP 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 subject 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.

5.4 The notification to the PDP Commissioner shall be made through one of the following channels:

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

(b) Completing the **notification form** in **Annex B** and submitting it to the official e-mail address at dbnpdp@pdp.gov.my; or

(c) Completing the **notification form** in **Annex B** and submitting a hard copy to the Commissioner.

5.5 The Company shall ensure that all required/mandatory information fields in the notification form are completed, and that the notification to the PDP Commissioner, through the methods specified in **section 3.4** is submitted **within the prescribed seventy-two (72) hours**.

5.6 The PDP Commissioner will issue a confirmation notice to the Company upon receiving the Personal Data breach notification. The notification will not be considered submitted to the PDP Commissioner without this confirmation notice.

5.7 In addition to the required/mandatory fields in the notification form submitted under **section 3.4**, the Company shall also provide the PDP Commissioner with the following information:

(a) Details of the Personal Data breach, including: -

(i) The date and time the Personal Data breach was detected.

(ii) The type of Personal Data involved and the nature of the breach.

(iii) The method used to identify the breach and the suspected cause of the incident.

(iv) The number of affected Data Subjects.

(v) The estimated number of affected data records.

(vi) The Personal Data system affected, which resulted in the breach.

(b) The potential consequences arising from the Personal Data breach.

(c) The chronology of events leading to the loss of control over Personal Data.

(d) Measures taken or proposed to be taken by us to address the Personal Data breach, including steps implemented or planned to mitigate the possible adverse effects of the breach.

(e) Measures taken or proposed to be taken to address the affected Data Subjects.

(f) The contact details of the DPO from whom further information on the Personal Data breach may be obtained.

5.8 The above details may be provided in phases to the PDP Commissioner as soon as practicable and **no later than thirty (30) days** from the date of the notification submitted to the PDP Commissioner made under **section 3.4**.

5.9 Where the Personal Data breach involves more than one subsidiary in the Company as the Data Controller, each subsidiary as a Data Controller ought to submit his own separate data breach notification to the Commissioner.

6. Notification to Affected Data Subjects

6.1 Where the Company have reason to believe that a Personal Data breach has occurred, which is likely to cause any significant harm to the Data Subjects, the Company will notify the Data Subjects via email, SMS, direct messaging or postal communication, whichever form of communication that you have provided the Company with, without unnecessary delay and **not later than seven (7) days** after the initial data breach notification is made to the PDP Commissioner.

6.2 The meaning of "significant harm" is similar as that provided in **section 3.2**. However, the "significant scale" criterion under **section 3.2(e)** is inapplicable when determining whether notification to affected Data Subjects is required.

6.3 Examples of Personal Data breach scenarios, where the Company is required to notify the affected Data Subjects: -

Example	**Whether Notification to the Commissioner 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 suppler 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 PDP 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.

6.4 The details of the Personal Data breach which the Company will provide to the data subjects include the following: -

(a) The details of the Personal Data breach that has occurred.

(b) The details on the potential consequences resulting from the Personal Data breach.

(c) Measures taken or proposed to be taken by us to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(d) Measures that the Company may take to eliminate or mitigate any potential adverse effects resulting from the data breach.

(e) The contact details of the DPO where more information regarding the Personal Data breach can be obtained.

6.5 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 the affected Data Subjects of the Personal Data breach. The forms of public communication include notification on the official website, notice in printed media, social media posts through the Company's official pages or accounts and automated notifications (push notification).

6.6 Examples of "disproportionate effort" include the following: -

(a) 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

(b) 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.

6.7 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.

6.8 The Flowchart overview of the data breach notification requirement under the PDPA is provided in **Annex A**.

7. Notification to Other Units

7.1 The Company will further notify the following bodies with regard to the occurrence of the Personal Data breach: -

(a) Royal Malaysia Police (PDRM), when the data breach involves criminal activity.

(b) 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.

(c) The Chief Executive of the National Cyber Security Agency (NACSA) and National Critical Information Infrastructure (NCII) Sector Leads (NCII Sector Leads) if we are a designated NCII Entity under the Cyber Security Act 2024.

7.2 The above are for reference purposes only and independent assessments shall be conducted to determine the notification requirements under other applicable Malaysian laws and regulations.

8. Retention of Records of Personal Data Breaches

8.1 The Company 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 PDP Commissioner, including those that did not meet the notification criteria for informing the PDP Commissioner and/or affected Data Subjects.

8.2 The register should at a minimum document the following information:

(a) Description of the Personal Data breach, including the date and time we 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.

(b) Description of the likely consequences of the Personal Data breach.

(c) Description of a chronology of events leading to Personal Data breach.

(d) Containment and recover measures taken to address the Personal Data breach.

(e) Details of notifications made to the Commissioner and/or affected Data Subjects and justification for not making notifications, where applicable.

8.3 The Company 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 PDP Commissioner to verify that the Company has complied with this documentation requirement.

9. Annexes

9.1 The annexes attached to this Internal Guidelines for ease of reference are as follows: -

(a) Annex A - Flowchart Overview of the Data Breach Notification Requirement under the Act 709

(b) Annex B – Data Breach Notification Form

(c) Annex C – Fact Finding Questionnaire of Subsidiary/ Department as to the Handling of Personal Data

(d) Annex D – General Principle Prior to Collecting any Personal Data

(e) Annex E – "Is Consent Required" Checklist

(f) Annex F – "Can I Disclose" Checklist

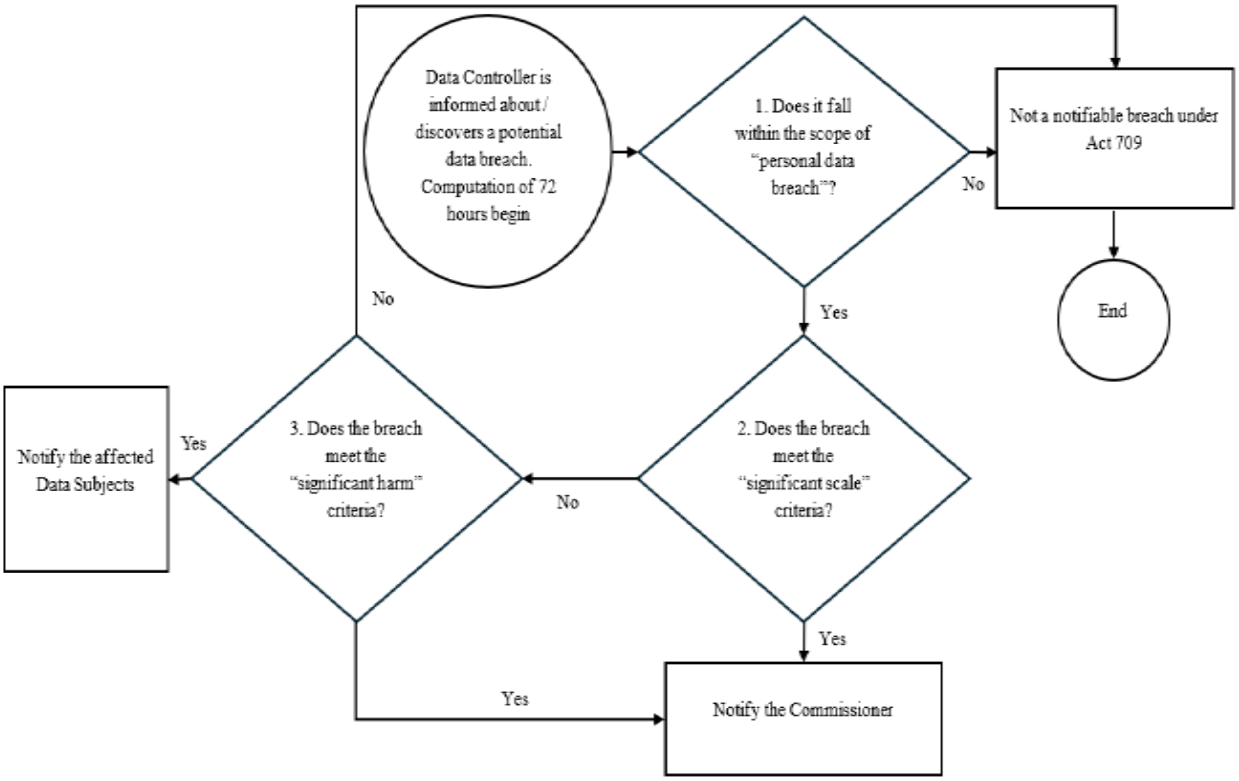
(g) Annex G – PDPA Notice Review Checklist

(h) Annex H – Template Clauses

The Standard Operating Procedure of Personal Data Protection

Annex A:

Flowchart Overview of the Data Breach Notification Requirement under the Act 709



The Standard Operating Procedure of Personal Data Protection

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 ("PDP Commissioner").

Please note that the information requested in this notification form is non-exhaustive. The PDP 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 PDP Commissioner in phases as soon as practicable not later than thirty (30) days from the date of the initial notification.

PARTICULARS OF THE DATA CONTROLLER

Organisation: _____

Address: _____

CONTACT PERSON

Name: _____

Designation: _____

Tel. No.: _____

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 PDP Commissioner.

Submission of notification:
PERSONAL DATA PROTECTION COMMISSIONER
8th Floor, Galeria PjH, Jalan P4W, Persiaran Perdana
Presint 4, 62100 W.P. Putrajaya
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 72 hours after becoming aware of the Personal Data breach?

   ☐ New notification.

   ☐ 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 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?

- ☐ No.
- ☐ Yes (please list out these parties).

_____

15. What harm or risks may result from the Personal Data breach affecting Data Subjects?

- ☐ Physical harm to threat or safety.
- ☐ Financial loss.
- ☐ Identity theft or fraud.
- ☐ Misuse of data for unlawful purpose.
- ☐ Data contains sensitive data.
- ☐ Data contains financial information.
- ☐ No potential harm to Data Subjects.
- ☐ Others.

_____

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?

_____

The Standard Operating Procedure of Personal Data Protection

Annex C:

Fact Finding Questionnaire of Subsidiary/ Department as to the Handling of Personal Data

Department/ Division **(e.g. Group People & Culture and etc.)**	

No.	Questions	Response
1.	List down the types of data collected. Example: • Name • Address • Phone Number Email Address • I/C Number	
2.	Who does this personal data relate to? Example: • Customer • Vendor • Supplier • Employees • Members • Others (please specify)	
3.	Do you collect any of these data? (sensitive personal data) • Health related data (physical & mental health) • Political opinions • Religious beliefs • Criminal data • Biometric data	
4.	Is the collection of such personal data:- • Mandatory • Voluntary	
5.	Do you receive personal data from other sources other than personal data which you collect directly from the individual? Example, data is received from: - • Other third parties • Referrals • Other group entities	

6.	Do you collect any personal data via the website or social media platforms? If so, please provide details.	
7.	Please identify the purpose of collection of the personal data identified in section 1. above. Example: • To deliver the services/ goods to customers • To perform the employment contract • For administrative purposes	
8.	Besides the purposes above, do you also use the data for marketing purposes? If so please provide details.	
9.	Will the personal data be shared/ disclosed with other third parties? Examples: • IT providers/ cloud providers • Marketing/ advertising agencies • Distributors/ agents etc. Please identify these parties.	
10.	Do you transfer or send personal data outside of Malaysia? If so, where and why?	
11.	Is any personal data stored in servers located outside of Malaysia? If so, where and what data is involved?	
12.	Do you currently issue Data Protection Notice/ Privacy Policy and obtain consents where required?	
13.	Who/ which team is currently responsible for handling the personal data?	

The Standard Operating Procedure of Personal Data Protection

Annex D:

General Principle Prior to Collecting any Personal Data

Before collecting any personal data,

ASK:

- Is this data related to our business?
- Is this data directly related to the purpose we are collecting it for?
- Can we justify collecting this data?
- Is it absolutely necessary for us to collect this data?
- Is the collection of the data proportionate to the purpose we need it for?

If the answer to any of the above is "NO" or "I DON'T KNOW" then reconsider the collection of such personal data.

The Standard Operating Procedure of Personal Data Protection

Annex E:

"Is Consent Required" Checklist

In determining whether consent is required for processing of the personal data, **ASK**:

- What personal data are we collecting?
- Is there sensitive personal data involved?

  Sensitive personal data
  - ☐ Medical information
  - ☐ Criminal data
  - ☐ Religious beliefs
  - ☐ Political opinions
  - ☐ Biometric data
- What are we using this data for?
- Do any exceptions apply to the purposes we are intending to use?

  Example exceptions: -
  - ☐ Performance of the contract with the data subject.
  - ☐ Taking steps with a view of entering into contract.
  - ☐ The purposes of use is to comply with law/ legal obligation.
  - ☐ The data is for purposes of prevention or detection of crime.
  - ☐ The data is to protect vital interests of the data subject.
  - ☐ The data is for purposes of investigations.
  - ☐ Sensitive personal data exceptions under Section 40 apply.

If no exceptions apply ⟶ Consent is Required

Consent methods

- Express/ Implied Consent for general personal data
- Explicit Consent for Sensitive Personal Data

The Standard Operating Procedure of Personal Data Protection

Annex F: "Can I Disclose" Checklist

In determining whether consent is required for processing of the personal data,

ASK:

- Does this disclosure come within the purposes identified in our Personal Data Protection Notice?
- Is this disclosure to a third party identified in our Personal Data Protection Notice?

YES to the above would likely mean disclosure is possible.

If **NO**, ask the following questions: -

- Does the disclosure fall within the exemptions, such as: -

  - ☐ Consent has been obtained from data subject for this disclosure.
  - ☐ The disclosure is for preventing or detecting a crime, or for the purpose of investigations.
  - ☐ The disclosure is required or authorised by or under any law or by the order of a court.
  - ☐ We are acting in reasonable belief that we have the legal right to disclose the personal data to this party.
  - ☐ We are acting in reasonable belief that we would have the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure.
  - ☐ The disclosure is for public interest as declared by the Minister.
  - ☐ Section 45 Exemptions apply.

If no exceptions apply → **Consent is Required**

The Standard Operating Procedure of Personal Data Protection

Annex G: PDPA Notice Review Checklist

- Clear indication who is the data controller (Company name, group etc)
- Description of the personal data processed (i.e. name, contact details etc)
- Source of that personal data must be provided (i.e. website, third parties etc)
- Purposes of use of the personal data must be described
- Explain whether it is obligatory or voluntary for the data subject to supply the personal data. Where it is obligatory, the consequences for the data subject if he fails to supply the personal data (e.g. will not be able to perform the services)
- Detail the categories of third parties to whom the personal data will be disclosed (e.g. IT vendors, outsourced service providers)
- If there will be transfer of personal data out of Malaysia, to notify and explain the purposes of the transfer
- Explain security measures that will be undertaken
- Explain data retention period
- How the data subject may request for access or correction of data or to limit the processing of his/ her personal data
- Contact details for data subjects to contact in the event of inquiries or complaints (name of DPO, designation, business telephone number, business address, dedicated and official business e-mail address or business fax number of the DPO)
- If there are minors (under 18 years of age) consent must be given by parent or guardian
- Ensure that the Notice is also provided in Bahasa Malaysia

The Standard Operating Procedure of Personal Data Protection

Annex H: Template Clauses

I. General Reciprocal Clause for Compliance with PDPA

Personal Data Protection

1. Both Parties shall comply with the PDPA in the processing of any Personal Data disclosed and/ or received in connection with this agreement.

2. The Parties agree to only use any Personal Data received from the other Party for the purposes related to the performance of their obligations under this agreement and not for any other purposes unless otherwise agreed between the Parties.

3. Each Party warrants and represents that it has complied with all requirements under the PDPA to enable the other Party to use and disclose the Personal Data as envisaged under this agreement including compliance with all notification and consent requirements.

Definitions: -
"**Personal Data**" means "any information from which an individual is identified or identifiable".

"**PDPA**" means "the Personal Data Protection Act 2010 of Malaysia, as may be amended from time to time".

II. Basic Clause when Contracting with Data Processors

Pursuant to your engagement by the Company to provide products or services under this agreement, Personal Data may be disclosed by the Company to you in order for you to carry out your obligations under the agreement. In such case, you will be deemed as the Company's "data processor".

As the Company's data processor, you warrant and undertake the following: -

(a) To have in place appropriate technical and organisation security measures so that the Personal Data is protected against unauthorised or unlawful processing and against accidental access, disclosure, alteration, loss, destruction or damage and shall take steps to ensure compliance with these security measures.

(b) Upon the request of the Company, you will provide all assistance to the Company to enable the Company to verify your compliance with your obligations under (a).

(c) Where a security breach involving Personal Data occurs, you will immediately notify the Company with all information relating to the breach and provide all reasonable and necessary assistance to the Company in order for the Company to meet its notification obligations under applicable law.

Definitions: -

"**Personal Data**" means "any information from which an individual is identified or identifiable".