

POLICY

RAM

Personal Data  
Protection Policy

28 July 2025



# PERSONAL DATA PROTECTION POLICY

## Contents

1. INTRODUCTION.....	2
2. SCOPE.....	2
3. DEFINITIONS.....	2
4. ROLES AND RESPONSIBILITIES.....	4
5. GUIDING PRINCIPLES ON PERSONAL DATA PROTECTION .....	4
6. PROCESSING & DISCLOSURE OF PERSONAL DATA.....	5
7. SECURITY AND CONFIDENTIALITY .....	5
8. RIGHTS TO ACCESS AND RECTIFY PERSONAL DATA.....	6
9. ENGAGEMENT OF THIRD-PARTY SERVICES .....	6
10. RETENTION & DISPOSAL OF PERSONAL DATA.....	7
11. CROSS BORDER TRANSFER OF PERSONAL DATA .....	7
12. BREACH OF PERSONAL DATA.....	8
13. NOTIFICATION OF PERSONAL DATA BREACH.....	9
Notifying CEO and Board of Directors.....	9
Notifying the Personal Data Protection Commissioner (“PDPC”).....	9
Notifying Data Subjects.....	9
14. TRAINING AND AWARENESS .....	10
15. COMPLAINTS.....	10
16. MONITORING AND REVIEW .....	11

## Appendices

A - Consent for collection, use and disclosure of Personal Data	12-26
B - Summary of Exemption under Section 45 of the PDPA 2010	
C - Personal Data Access Request Form	
D - Personal Data Correction Request Form	
E - Personal Data Withdrawal of Consent Form	
F - Personal Data Breach Notification Flowchart	
G - Data Breach Notification Form	

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	11 August 2020	<b>Last reviewed date</b>	-

# PERSONAL DATA PROTECTION POLICY

## 1. INTRODUCTION

- 1.1 RAM Holdings Berhad and its subsidiaries (jointly referred as “RAM Group”) collect, record, hold, stores, use and disclose (“process”) personal data in accordance with Personal Data Protection Act 2010 (“PDPA 2010”) and other applicable personal data protection laws.
- 1.2 The purpose of this Personal Data Protection Policy (“Policy”) is to establish guidelines and practices for handling personal data in a way that complies with relevant laws and regulations. This Policy aims to protect the privacy of individuals' Personal Data, measures to keep these data safe, and establish the rights of individuals to whom the data relates.
- 1.3 The processing of Personal Data by RAM Group is subject to compliance with this Policy, and other RAM Group’s *Policies including Code of Conduct, Code of Ethics and Conduct, Treatment of Confidential Information Policy, Record Retention & Disposal Policy, Information Technology Policy, Cyber Security Policies and Procedures and Risk Management Policy (“RAM Policies”)*.

## 2. SCOPE

- 2.1 This Policy applies to all Personal Data processed by RAM Group for **commercial purposes** in Malaysia, including data collected from customers, Employees, contractors, and other stakeholders. It covers data processing activities conducted **both electronically and in hard copy format or processed with the use of Artificial Intelligence (AI)**.
- 2.2 The PDPA 2010 deals only with the Personal Data of individuals and does not extend to data of companies or corporations.

## 3. DEFINITIONS

- “Artificial Intelligence (AI)” shall mean the capability of machines and systems to perform tasks that typically require human intelligence. This includes learning from data, reasoning, problem-solving, perception, and language understanding (as defined in the National Guidelines on AI Governance and Ethics).
- “Data Owner” shall mean a designated group or department that owns the data and where the data originated from.
- “Data Subject” shall mean the individual who is the subject of the Personal Data.

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

“Employee” shall mean means any person employed under RAM Group, including temporary worker, contract worker, or any other person who works for RAM Group, regardless of their duration of employment or contract;

“Personal Data” shall mean data about an individual who can be identified:

- a) from such data alone; or
- b) from such data and other information that the organisation has or is likely to have access.

Personal Data may include *sensitive Personal Data* relating to race, religious beliefs and biometric or any definition as stipulated in the PDPA 2010. Non-exhaustive examples of an individual’s Personal Data includes:

- a) Personal contact information, including name, personal address, personal email address and telephone number, bank account and tax details;
- b) Details of NRIC, passport or other equivalent identification number; and
- c) Other information where the individual can be identified from such information.

The following are examples of information, which will not normally be personal data:

- a) mere reference to a person’s name, where the name is not associated with any other personal information;
- b) incidental reference in the minutes of a business meeting of an individual’s attendance at that meeting in an official capacity;
- c) where an individual’s name appears on a document or email indicating only that it has been sent or copied to that particular individual; or
- d) the content of that document or email does not amount to personal data about the individual unless there is other information about the individual in it.

“Personal Data breach” shall mean any breach of Personal Data, loss of Personal Data, misuse of Personal Data or unauthorised access of Personal Data.

“Senior Management” shall mean Employees of RAM Group at Grades 21 and above as stipulated in RAM Group’s Terms and Conditions of Service.

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

## 4. ROLES AND RESPONSIBILITIES

- 4.1 The **Board of Directors** is responsible to set the policy direction for ensuring compliance with PDPA 2010. The **Senior Management** shall be responsible for ensuring the implementation and compliance of this Policy. All **Employees** are responsible for adhering to this Policy and ensuring the security and confidentiality of Personal Data.
- 4.2 RAM Group may appoint a suitably qualified and experienced personnel to serve as **Data Protection Officer (“DPO”)**. The DPO shall be responsible for overseeing data protection compliance and acting as a point of contact for data protection authorities and Data Subjects. The DPO’s duties shall include monitoring the application of this Policy, providing advice, drafting and reviewing of policies, handling data breaches, conduct data protection impact assessment and compliance audit.
- 4.3 The Information Technology Department shall be responsible for the storing of data to meet the necessary data security standards under RAM Policies and evaluating third party services.

## 5. GUIDING PRINCIPLES ON PERSONAL DATA PROTECTION

- 5.1 RAM Group shall ensure compliance with the following seven (7) principles when collecting, using or disclosing Personal Data:

No	Principles	Brief Description
1	General	Personal Data collected shall be adequate, relevant and not excessive. The Personal Data shall be processed with consent and for a lawful purpose. The Consent Requirements Guide is at <b>Appendix A</b> .
2	Notice & Choice	Inform the purposes for which the Personal Data is being processed, collected or disclosed.
3	Disclosure	Disclosure without consent is not permissible <sup>1</sup> .
4	Security	Protection of data from loss, misuse, unauthorised access, etc <sup>2</sup> .
5	Retention	Personal Data shall not be kept longer than necessary
6	Data Integrity	Personal Data shall be accurate, up-to-date, verifiable
7	Access	The right to access Personal Data

<sup>1</sup> Please also refer to Code of Conduct, Treatment of Confidentiality Policy

<sup>2</sup> Please also refer to Risk Management Policy, IT Policy and Cyber Security Policy.

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

## 6. PROCESSING & DISCLOSURE OF PERSONAL DATA

- 6.1 The **processing** of Personal Data shall include but not limited to collecting, accessing, recording, holding, storing, organising, and disclosing of the Personal Data, including Personal Data processed with the use of AI. Before processing Personal Data, RAM group shall seek individual consent (where possible, express consent<sup>3</sup>; otherwise implied consent<sup>4</sup>) and set out the purpose for which the consent is sought. If sensitive Personal Data is processed, written consent shall be secured<sup>5</sup>.
- 6.2 No Personal Data shall be disclosed without the consent of the Data Subject. Notwithstanding the aforesaid, Personal Data may be disclosed to a third party under the following circumstances<sup>6</sup>:-
- a) the Data Subject has given his consent to the disclosure;
  - b) the disclosure —
    - i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or
    - ii) was required or authorized by or under any law or by the order of a court;
  - c) RAM Group acted in the reasonable belief that it had the right in law to disclose the Personal Data to the other person;
  - d) RAM Group acted in the reasonable belief that it would have had 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 (e.g. disclosure to the RAM’s Insurers the names and NRIC numbers of employees and family members for the purpose of insurance coverage);
  - e) the disclosure was justified as being in the public interest in circumstances as determined by relevant authority; or
  - f) fall within the exemptions under Section 45 of the PDPA 2010 (summarised at **Appendix B**) or any exemptions as determined by the relevant authority.

## 7. SECURITY AND CONFIDENTIALITY

- 7.1 RAM Group shall ensure reasonable precautions are taken to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. These precautions should include **administrative, technical and cybersecurity measures, such as measures to prevent unauthorized access**, that commensurate with the sensitivity of the information and the level of risk associated with the processing of the Personal Data.

<sup>3</sup> *Express Consent*: Wet ink Signature, e-signature, ticking a box or verbal consent followed by confirmation.

<sup>4</sup> *Implied Consent*: No objection after timeframe of being notified, Data Subject proceeds to use the services and volunteers to provide data after being notified.

<sup>5</sup> Section 40 of the PDPA 2010. *Explicit Consent*: Ensure the type of data being processed is clearly defined and explained and the purpose of use of such data is clear and there is Express Consent.

<sup>6</sup> Section 39 of the PDPA 2010.

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

Relevant data security measures are documented in *Treatment of Confidential Information Policy, Code of Conduct, Code of Ethics and Conduct, Information Technology Policy, Cyber Security Policies and Procedures and Risk Management Policy.*

## 8. RIGHTS TO ACCESS AND RECTIFY PERSONAL DATA

- 8.1 Every Data Subject shall have the right to obtain at any time, on written request, confirmation as to whether Personal Data relating to the individual is being processed. Refer to **Appendix C** for the Data Access Request (DAR) Form, and **Appendix D** for the Data Correction Request Form. Completed Forms are to be emailed to DPO at [ram\\_pdpa@ram.com.my](mailto:ram_pdpa@ram.com.my).
- 8.2 RAM Group shall observe the Data Subject’s right to access the Personal Data and the right to correct the Personal Data, except if the refusal is in accordance with PDPA 2010. RAM Group may charge fees in accordance with the provisions of PDPA 2010<sup>7</sup>.
- 8.3 Individuals may withdraw their consent by notice in writing and the *sample* template is at **Appendix E**.
- 8.4 Upon receipt of any request from individuals, the DPO shall **acknowledge receipt, verify the identity of the requestor**, and observe the rights of the Data Subject in accordance with this Policy and the PDPA 2010.

## 9. ENGAGEMENT OF THIRD-PARTY SERVICES

- 9.1 In the event that RAM Group retains third-party service providers (e.g. cloud and other hosting services, payroll solutions, disaster recovery, software developers and other IT support services) that have access to Personal Data, the contractual arrangement shall be as follows:

Obligations of RAM Group	Obligations of Third-Party Service Provider
a) where possible, maintain control over processing of such Personal Data at all times; b) where possible, to include the contractual terms on data security; c) where necessary, to carry out assessments or audits on the third party; and/or d) put in place any other necessary measures to ensure compliance with this Policy.	a) the third-party to comply with the applicable laws and regulations, as required for processing of Personal Data in accordance with the services that will be provided; and b) the third-party has sufficient measures in place to safeguard the Personal Data from any unauthorised or unlawful processing, accidental loss, destruction or damage.

<sup>7</sup> Personal Data Protection (Fees) Regulations 2013 [P.U. (A) 338/2013]

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

9.2 When Personal Data of an individual is obtained from third parties, there is a risk that such third parties had failed to collect the Personal Data in compliance with the PDPA (e.g. the third-party may have failed to obtain the necessary consent from the individual at the time the third-party had collected the individual’s Personal Data). In this, RAM Group shall ensure that there was sufficient notice given to Data Subjects to ensure consent is obtained and to collect such Personal Data only for legitimate purposes.

9.3 For the purpose of verifying third-party source, RAM Group shall ensure that contractual warranties and/or obligations are imposed on the third-party to obtain the individual’s consent prior to disclosing Personal Data to RAM Group.

## 10. RETENTION & DISPOSAL OF PERSONAL DATA

10.1 Personal Data can be retained by RAM Group for as long as it is necessary. Notwithstanding the aforesaid, Personal Data may be retained for extended duration if it is required for legitimate business purposes (e.g. to fulfil legal requirements or comply with regulatory reporting and other similar purposes).

10.2 RAM Group shall cease to retain documents containing Personal Data if:

- a) the purpose for which the Personal Data was collected is no longer being served by the retention of such Personal Data; and
- b) retention is no longer necessary for legal or business purposes.

In such event, the retention and disposal shall be subject to the provisions of Record Retention and Disposal Policy and such disposal shall be properly documented.

## 11. CROSS BORDER TRANSFER OF PERSONAL DATA

11.1 RAM Group shall not transfer any Personal Data to a recipient outside Malaysia except if the receiving country has equivalent or substantially similar data protection laws. In this, the DPO may conduct **Transfer Impact Assessment** (“TIA”) to determine:

- a) the receiving party’s Security Principles,
- b) the legal enforceable obligations,
- c) the applicable laws, jurisdictions and governing authority.

11.2 Notwithstanding the aforesaid, RAM Group may transfer<sup>8</sup> Personal Data if :

- a) consent has been obtained from Data Subject;

---

<sup>8</sup> Section 129 of the PDPA 2010

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

- b) it is necessary for the performance of a contract between RAM Group and Data Subject (e.g. travel insurance)
- c) it is necessary for the performance of a contract between RAM Group and third-party (e.g. overseas work travel);
- d) it is for legal proceedings or obtaining legal advice;
- e) all reasonable precautions and due diligence have been exercised for the cross-border transfer (e.g. implementing relevant contractual clauses to ensure there is adequate level of protection); or
- f) any other circumstances as set out under the provisions of the PDPA 2010<sup>9</sup>.

11.3 The relevant department shall inform the DPO in the event there is a potential cross border transfer of Personal Data and the DPO may conduct Transfer Impact Assessment (TIA) in accordance with relevant guidelines<sup>10</sup> to ensure compliance thereto. The validity of a TIA shall not exceed three (3) years.

## 12. BREACH OF PERSONAL DATA

- 12.1 All Employees shall ensure compliance of this Policy. Any Employee found violating any provision of this Policy, shall be subject to investigation and if found to be in breach or the non-compliance of the PDPA 2010 or this Policy, RAM Group will take necessary measures, including disciplinary and/or legal action against the Employee as provided under Code of Ethics and Conduct Policy.
- 12.2 All Employees shall notify the DPO immediately upon becoming aware of any occurrence of data breach. If the notification or complaint is via the Whistleblowing Policy's [complaint@ram.com.my](mailto:complaint@ram.com.my), the DPO shall be duly informed if it involves a breach of Personal Data.

## 13. NOTIFICATION OF PERSONAL DATA BREACH

### Notifying CEO and Board of Directors

- 13.1 The DPO upon receipt of any complaint or breach notification **shall immediately notify the Group CEO** and the **CEO of the affected entity** or in their absence, any member of Senior Management so authorised. The Group CEO or in his/her absence, the CEO of the affected entity shall inform the Board of Directors.

<sup>9</sup> Section 129 of the PDPA 2010.

<sup>10</sup> Cross Border Personal Data Transfer Guidelines ("CBPDT Guidelines") and any amendments thereto.

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

13.2 The DPO together with the relevant members of Senior Management as assigned by the Group CEO (in his/her absence, the CEO of the affected entity), shall first assess whether the breach involves Personal Data breach or otherwise. Depending on the outcome, either of the following shall apply:

- a) If it is determined that it is a Personal Data breach, Para. 13.3 to 13.7 of this Policy shall apply; and
- b) If it is determined that it is not a Personal Data breach, Para. 13.8 of this Policy shall apply.

#### Notifying the Personal Data Protection Commissioner (“PDPC”)

13.3 The DPO shall within **seventy-two (72) hours upon being aware of breach, notify the incident to the Personal Data Protection Commissioner (“PDPC”)** if the breach is deemed as likely to cause **“significant harm/significant scale”**. In this, aspects for consideration by the DPO, together with the relevant Senior Management shall include:

- a) whether the breach may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
- b) whether the Personal Data may be misused for illegal purposes;
- c) whether the breach consists of sensitive Personal Data;
- d) whether the breach consists of Personal Data and other personal information which, when combined, could potentially enable identity fraud; or
- e) whether the breach is of significant scale in that it would affect more than one thousand (1,000) Data Subjects.

Notification under this Paragraph shall be made in accordance with the manner as stipulated in **Appendix G** with a copy of the Notice extended to the Group CEO and CEO of affected entity prior to submission to PDPC.

#### Notifying Data Subjects

13.4 The DPO shall, within **seven (7) days after notifying the PDPC** under Para. 13.3, **notify the affected Data Subjects of the Personal Data breach** if the breach is deemed as likely to result in **“significant harm”**. In this, the aspects for consideration by the DPO, together with the relevant members of Senior Management shall include:

- a) whether the breach may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property of impacted Data Subjects;
- b) whether the Personal Data may be misused for illegal purposes;
- c) whether the breach consists of sensitive Personal Data; or

<b>Title</b>	Personal Data Protection Policy	<b>Revision no.</b>	0
<b>Initial approved date</b>	28 July 2025	<b>Last reviewed date</b>	-

- d) whether the breach consists of Personal Data and other personal information which, when combined, could potentially enable identity fraud towards the affected Data Subjects.

In notifying the Data Subject, notification to the Group CEO and CEO of the affected entity before transmission to the affected Data Subjects shall be extended.

- 13.5 If however, it is impractical or requires a disproportionate effort<sup>11</sup> to provide direct notification to each of the affected Data Subjects under Para 13.4 (e.g. where it would result in excessive financial burden on the data controller due to the sheer number of Data Subjects, or where it would be difficult for the data controller to ascertain the contact details of the Data Subjects), RAM Group may **opt for public communication (through notification on the data controller’s website, publication of notice in printed media or social media) of data breach notification**. In this, subject to the timeline of seven (7) days, the DPO shall liaise with the Group CEO, the CEO of affected entity and Corporate Communications Team in the preparation and dissemination of the press release.
- 13.6 The Personal Data Protection Guidelines on Data Breach Notification<sup>12</sup> and any amendments thereto shall provide the necessary guidance in complying with the preceding subparagraphs.
- 13.7 In the event that the Personal Data breach is caused by a cyber security issue, the **Information Technology Department** shall be immediately notified to take necessary action pursuant to the Information Technology Policy, Cyber Security Policies and Procedures and other relevant laws and regulations governing cyber security breach.
- 13.8 Where it is determined that the incident is not a breach related to Personal Data, the Group CEO (in his/her absence, the CEO of the affected entity) shall take necessary action as he deems fit (e.g. reporting to the Police, Securities Commission Malaysia, and/or National Cyber Security Agency).

The Personal Data Breach Notification Flowchart is at **Appendix F**.

## 14. TRAINING AND AWARENESS

RAM Group shall ensure regular training and awareness programs are provided to Employees on compliance, data protection practices, and handling of personal data.

## 15. COMPLAINTS

Any complaint may be channelled to the appointed DPO at [ram\\_pdpa@ram.com.my](mailto:ram_pdpa@ram.com.my).

<sup>11</sup> Para. 10.3-10.5 of the Personal Data Protection Guidelines on Data Breach Notification.

<sup>12</sup> Issued by the Personal Data Protection Commissioner on 25 February 2025.

## 16. MONITORING AND REVIEW

This Policy will be subject to annual review and where necessary, to be updated to ensure ongoing compliance with data protection requirements and any changes in data protection laws or regulations.

---

## CONSENT FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

---

- 1) Employee must OBTAIN THE CONSENT of an individual BEFORE the:
  - (i) collection;
  - (ii) use; and/or
  - (iii) disclosure of an individual's Personal Data.
- 2) Where possible, consent must be obtained IN WRITING. This is to mitigate against disputes.
- 3) When seeking such consent, Employee must:
  - (i) notify the individual IN WRITING of the PURPOSE(S) for which RAM Group intends to collect, use or disclose his/her Personal Data. The purpose should be clearly set out.
  - (ii) obtain the individual's WRITTEN confirmation that the Personal Data provided is accurate and complete.
- 4) If consent is obtained, the Personal Data must only be collected, used or disclosed by RAM Group for the purposes for which the consent was obtained, and not for any other purpose.
- 5) The individual is entitled to WITHDRAW CONSENT upon giving reasonable notice to the Employee. In such event:
  - (i) Employee should direct the individual to submit their notice of withdrawal in writing to the DPO (see **Appendix C**);
  - (ii) On receipt of withdrawal notice, the DPO shall inform the individual of the likely consequences of withdrawing the consent; and
  - (iii) Upon withdrawal, RAM Group MUST CEASE to collect, use or disclose the Personal Data of such individual (as the case may be).

(the rest of the page is intentionally left blank)

## Summary of Exemption under Section 45 of the PDPA 2010

Sections	Type of Processing	Exemptions
45(1)	Domestic Purposes	<ul style="list-style-type: none"> <li>▪ PDPA</li> </ul>
45(2) (a)	Process for; <ul style="list-style-type: none"> <li>(i) the prevention or detection of crime or for the purpose of investigations;</li> <li>(ii) the apprehension or prosecution of offenders; or</li> <li>(iii) the assessment or collection of any tax or duty or any other imposition of a similar nature</li> </ul>	<ul style="list-style-type: none"> <li>▪ General Principle</li> <li>▪ Notice and Choice Principle</li> <li>▪ Disclosure Principle</li> <li>▪ Access Principle</li> <li>▪ Other related provisions</li> </ul>
45(2) (b)	Physical or mental health data where the application of the provisions to the Data Subject would be likely to cause serious harm to the physical or mental health of the Data Subject or any other individual	<ul style="list-style-type: none"> <li>▪ Access Principle</li> </ul>
45(2) (c)	Statistics or carrying out research PROVIDED not processed for any other purposes and resulting statistics or the results of the research are not in an identifiable form.	<ul style="list-style-type: none"> <li>▪ General Principle</li> <li>▪ Notice and Choice Principle</li> <li>▪ Disclosure Principle</li> <li>▪ Access Principle</li> </ul>
45(2) (d)	In connection with any order or judgement of a court	<ul style="list-style-type: none"> <li>▪ General Principle</li> <li>▪ Notice and Choice Principle</li> <li>▪ Disclosure Principle</li> <li>▪ Access Principle</li> <li>▪ Other related provisions</li> </ul>
45(2) (e)	Discharging regulatory functions if the application would be likely to prejudice the proper discharge of those functions	<ul style="list-style-type: none"> <li>▪ General Principle</li> <li>▪ Notice and Choice Principle</li> <li>▪ Disclosure Principle</li> <li>▪ Access Principle</li> <li>▪ Other related provisions</li> </ul>
45(2) (f)	Journalistic, literary or artistic purposes provided that— <ul style="list-style-type: none"> <li>(i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;</li> <li>(ii) the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and</li> <li>(iii) the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.</li> </ul>	<ul style="list-style-type: none"> <li>▪ General Principle</li> <li>▪ Notice and Choice Principle</li> <li>▪ Disclosure Principle</li> <li>▪ Retention Principle</li> <li>▪ Data Integrity Principle</li> <li>▪ Access Principle</li> <li>▪ Other related provisions</li> </ul>

## PERSONAL DATA ACCESS REQUEST FORM

The following information is required to help us provide you a timely and accurate response to your Personal Data Access Request pursuant to Act 709.

Full Name of Data Subject or Relevant Person	
Relevant Person's Relationship with the Data Subject	
Address	
Mobile Number	
Email address	
Please provide the following details:	
a) Purpose of access:	
b) The type of data that you would like to access:	
c) Relevant information about you, for us to verify your identity (e.g.	

**Declaration:** I am the Data Subject/Relevant Person named above and hereby request, under the provisions of Sections 12 and 30 of the Personal Data Protection Act 2010 [Act 709], that RAM Group provide me with a copy of the personal data held about me as specified above. I understand that there may be a charge for this service and that RAM Group will contact me to request payment. I also note that RAM Group will respond within the time stipulated under Act 709 after receipt of payment from me and will notify me of a date and time to collect a copy of the documents personally.

Signature .....

Date .....

<sup>13</sup> As adopted from Appendix 2 of the General Code of Practice of Personal Data Protection.

## PERSONAL DATA CORRECTION REQUEST FORM

- Please note that we reserve the right to restrict and/ or refuse your access to certain particulars of your personal data as may be permitted under the Personal Data Protection Act 2010 [Act 709].
- Your request may not be processed if the information/document provided is incomplete.
- Any request for Personal Data Correction Request must be supported with proof or evidence.
- Please use CAPITAL LETTERS to fill in the form.

Please tick (v) on one of the following:

- I would like to access my personal data  
(Please fill in Section 1 and Section 3 below)
- I am a Third-Party Requestor  
(Please fill in Section 2 and Section 3 below)

### SECTION 1 : TO BE FILLED IN BY DATA SUBJECT

Full Name (per NRIC/Passport)	
New NRIC/Passport No.	
Mobile Phone No.	

### SECTION 2 : TO BE FILLED IN BY DATA SUBJECT (AUTHORIZED PERSON)

This request is based on (please tick (v) one of the following):

- I am acting under the Data Subject's authorisation/mandate/Power of Attorney
- I am the legal/personal representative of the Data Subject
- I have Warrant or Court Order allowing the correction to the Data Subject's Personal Data
- I am executor/administrator of the Data Subject's estate
- Others (please specify) \_\_\_\_\_

Please enclose proof of your authority to correct the personal data of the Data Subject.

<sup>14</sup> As adopted from Appendix 3 of the General Code of Practice of Personal Data Protection.

<b>A : Particulars of Data Subject</b>	
Full Name (per NRIC/Passport)	
New NRIC/Passport No.	
Mobile Phone	
<b>B: Particulars of Third Party</b>	
<b>Requestor</b>	
Full Name (per NRIC/Passport)	
New NRIC/Passport No.	
Mobile Phone	
Email Address	
Correspondence Address	
<b>SECTION 3 : CORRECTION OF PERSONAL DATA</b>	
(Please tick (v) and fill in at relevant Section only)	
<input type="checkbox"/> Full Name (per NRIC/Passport)	
<input type="checkbox"/> New NRIC/Passport No.	
<input type="checkbox"/> Address of premise	
<input type="checkbox"/> Mobile Phone	
<input type="checkbox"/> Postal Address	
<input type="checkbox"/> *House Phone No.	
<input type="checkbox"/> *Office Phone No.	
<i>*Non-mandatory information</i>	



## PERSONAL DATA WITHDRAWAL OF CONSENT FORM

---

**NOTICE UNDER SUBSECTION 43(1) OF  
THE PERSONAL DATA PROTECTION ACT 2010 [ACT 709]**

Date:

Data User's Address:

.....  
.....  
.....

Sir / Madam,

**NOTICE UNDER SUBSECTION 43(1) OF THE PERSONAL DATA PROTECTION ACT 2010 [ACT 709] TO PREVENT PROCESSING OF PERSONAL DATA FOR PURPOSES OF DIRECT MARKETING**

I, ..... (full name) ..... (New NRIC/Passport No.) need you to cease or not to begin processing my personal data for purposes of direct marketing in the duration of \_\_\_\_\_ \* from the date of receipt of this notice.

Thank you.

Signature: .....

Name: .....

Address: .....

.....  
.....  
.....

Phone No.: .....

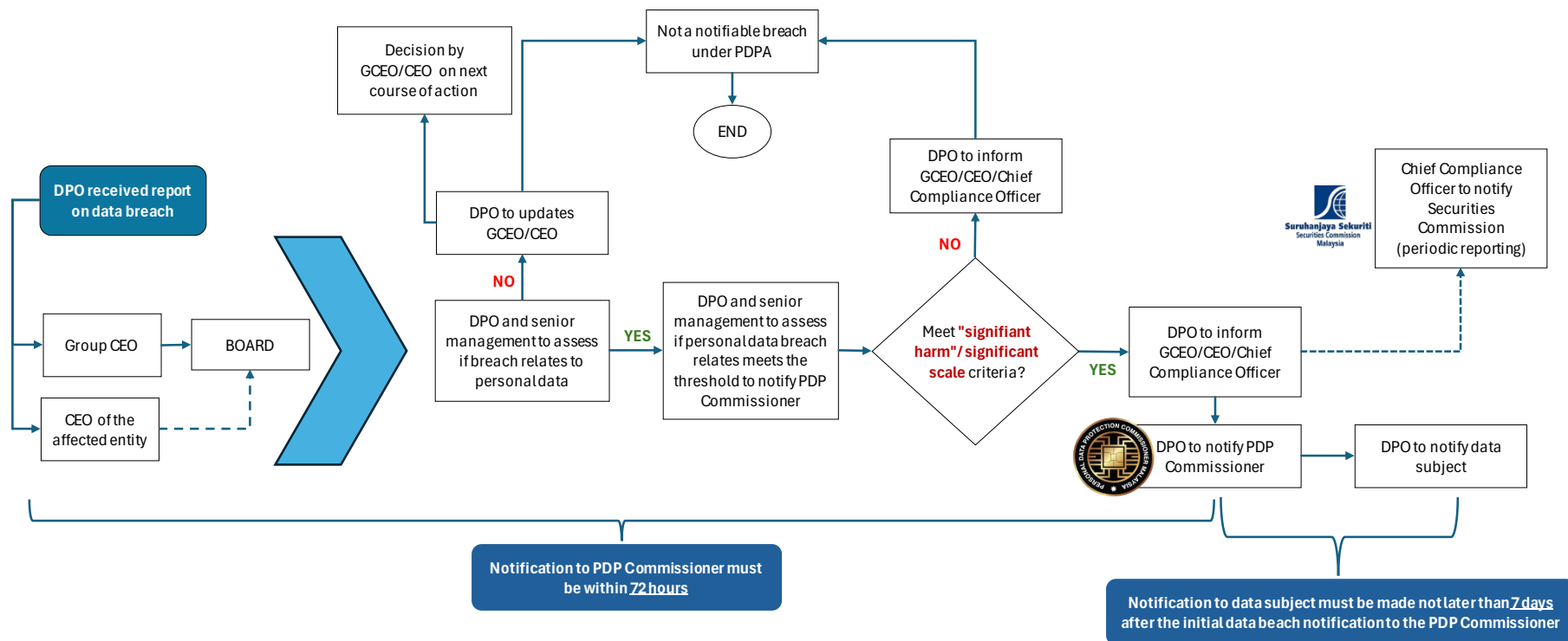
Email: .....

\*Data Subject can determine a reasonable stipulated time

---

<sup>15</sup> As adopted from Appendix 4 of the General Code of Practice of Personal Data Protection.

# PERSONAL DATA BREACH NOTIFICATION FLOWCHART



## ANNEX B: DATA BREACH NOTIFICATION FORM



<b>DATA BREACH NOTIFICATION</b>
---------------------------------

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 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**

8th Floor, Galeria PjH, Jalan P4W  
 Persiaran Perdana, Precinct 4  
 62100 W.P Putrajaya  
 or via email: [dbnpdp@pdp.gov.my](mailto:dbnpdp@pdp.gov.my)

<sup>16</sup> As adopted from Annex B of the Personal Data Protection Guidelines on Data Breach Notification.

**SECTION A: BASIC INFORMATION**

**1. Is this a new notification or an update to a previous notification that has been submitted to the Commissioner?**

<input type="checkbox"/> New notification <input type="checkbox"/> 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?**

<input type="checkbox"/> Yes <input type="checkbox"/> 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. 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?**

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 is 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?**

Published by RAM Holdings Berhad and its Group of Companies

Reproduction or transmission in any form is prohibited except by permission from RAM Holdings Berhad and its Group of Companies.

© Copyright 2025 by RAM Holdings Berhad and its Group of Companies

RAM Holdings Berhad  
Level 8 Mercu 2, KL Eco City  
No 3, Jalan Bangsar  
59200 Kuala Lumpur

T: (603) 2708 8288  
F: (603) 27088201  
E: [compliance@ram.com.my](mailto:compliance@ram.com.my)  
W: [www.ram.com.my](http://www.ram.com.my)